SEPTEMBER 2024
networkingplus.co.uk

NETWORK+

Stepping up public security

There's no time to waste in search of cyber resilience

Mark Jow, Gigamon, p6

Emptying the bins with IoT

How sensors, IoT and LPWAN join forces

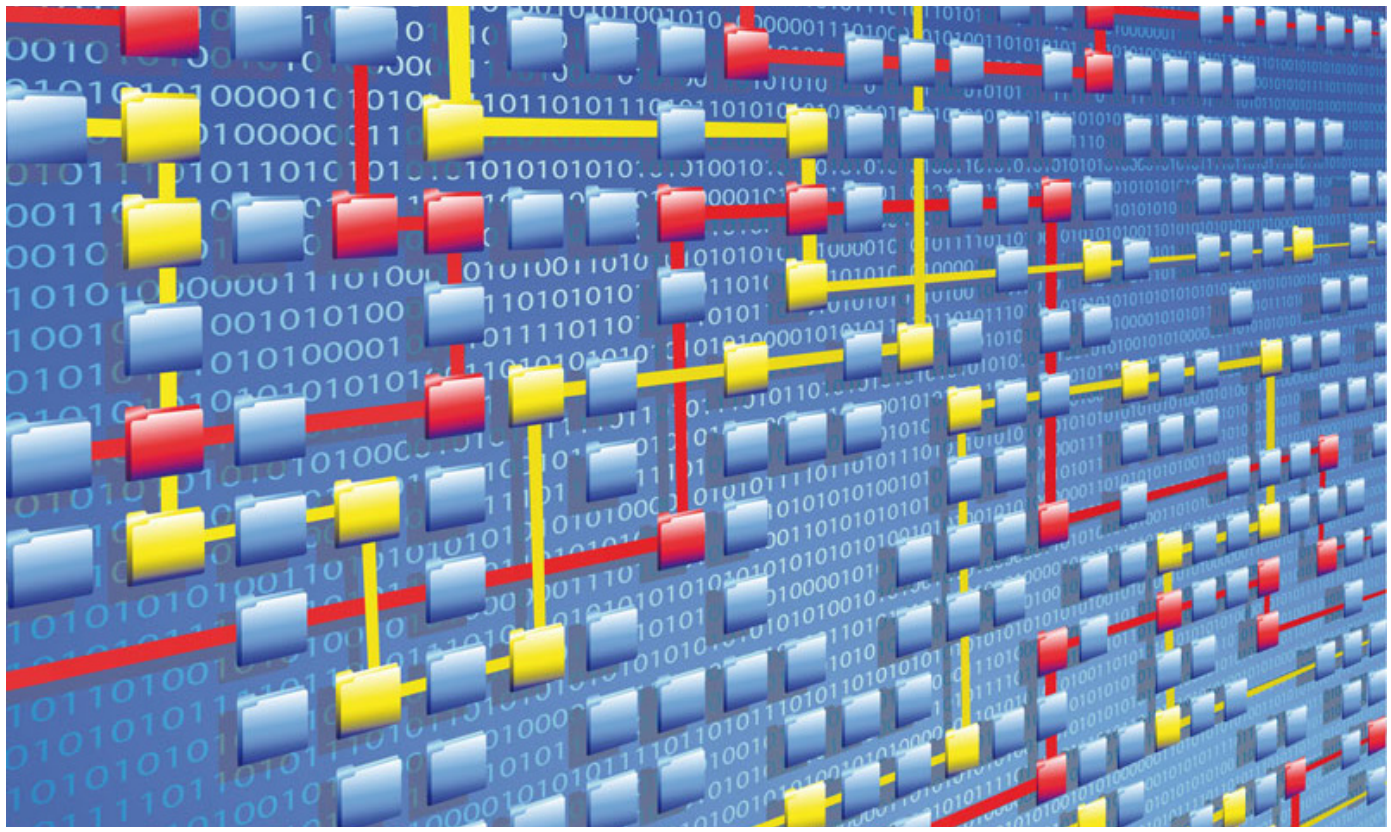
Gareth Mitchell, Heliot Europe, p11

Questions and answers

There are no pockets in a shroud...

Glen McCarty, Velocity Smart Consulting, p16

Data centres named Critical National Infrastructure – but is it enough?



The government has this month named UK data centres as Critical National Infrastructure (CNI) to protect the country's data against IT outages, cyber-attacks and environmental emergencies.

As the first Critical National Infrastructure designation since 2015, this move places data centres alongside water, energy and emergency services systems, giving them greater government support when recovering from critical incidents.

"Data centres are the engines of modern life - they power the digital economy and keep our most personal information safe. Bringing data centres into the Critical National Infrastructure regime will allow better coordination and cooperation with the government against cyber criminals and unexpected events," said Technology Secretary Peter Kyle.

As part of the designation, a dedicated CNI data infrastructure team of senior government officials will be formed to monitor for potential threats, working with the National Cyber Security Centre and emergency services to ensure data, from photos to NHS records, is protected. With the CNI designation, the government will work to build contingency plans to mitigate risks and damage caused in the event of an attack against a data centre.

"The move is long overdue and will hopefully pave the way for more countries to follow suit," reports Sylvain Cortes, VP Strategy at Hackuity. "Data is the foundation of trillions of annual transactions, to say nothing of the other CNI dependent on these very data centres. Coincidentally, that makes them a prime target for the $10 trillion cybercrime industry."

The decision is widely considered timely and strategic from a physical security standpoint, given that data centres comprise the backbone of the digital economy housing vast quantities of sensitive information.

"While data centres are better equipped than most businesses to secure data, this designation will give operators greater reassurance that the government will support them in recovering from and anticipating critical incidents, minimising the impact on the economy," explains Nick Smith, a data centre security expert and Business Development Manager at Genetec. "In terms of the implications for data centre operators and the wider supply chain, I expect this will further emphasise the importance of government product approvals such as CAPSS."

The CNI designation is a most welcome step in right direction for sure, but is it enough to truly safeguard our increasingly digital landscape, for commercial and public entities alike?

"As we move deeper into an era defined by AI and cloud services – not only for businesses, but for society as a whole – the need for robust security and resilience for data centres has become more pressing," says Thomas King, CTO, DE-CIX. "However, data centres on their own are of little value. Interconnection between data centres – therefore robust networks and interconnection platforms – is essential to enable the data and applications housed in data centres to create value for society and business, and these also require recognition as critical infrastructure. This is not just a local issue; it's a framework that can and should be replicated by other nations to safeguard their digital economies." ■

Inverclyde Council's Health and Social Care Partnership streamlines with Totalmobile

Totalmobile has announced a new partnership with Inverclyde Council's Health and Social Care Partnership (HSCP).

Totalmobile has been awarded the contract to manage the scheduling service for around 550 social care workers in Inverclyde. With Totalmobile's advanced technology, social care staff working in the community will now be equipped to handle on-day changes seamlessly, onboard new service users more quickly, and improve overall service efficiency.

The implementation of Totalmobile's solutions, which has just begun, is expected to enhance current processes and optimise resources across the HSCP. By utilising intelligent systems that can automatically react to unplanned changes such as staff sickness without requiring manual intervention, Inverclyde's social care workers can ensure that service continuity is maintained, and service users receive the support they need without delay or interruption.

"We anticipate the new service will allow social care staff, who are delivering vital services across the community, to work more efficiently and have less time sitting at their desk manually inputting data," said Councillor Robert Moran, chair of the Inverclyde Integrated Joint Board.

"We're proud to support Inverclyde Council in their mission to modernise their care services. By integrating our state-of-the-art solutions, Inverclyde will not only streamline their operations but also ensure that their carers have the tools they need to deliver exceptional care. This is a prime example of how technology can be leveraged to transform public sector services for the better," said Chris Hornung, Managing Director of Public Sector at Totalmobile. ■

Network Fire Service Partnership upgrades communications

The Network Fire Service Partnership (NFSP) has awarded NEC Software Solutions (NECSWS) a contract to deliver a new hosted Command, Control and Integrated Communication System.

Under the contract — which is for six years initially with a further four years' extension — staff and call handlers will be provided with the latest tools and real-time information they need to quickly dispatch fire appliances to incidents based on their proximity and capability, ensuring fast and effective responses to emergencies.

"Control firefighters are the start of the frontline. They play a key role in dealing with incidents – determining the scale of response and mobilising the most appropriate vehicles and equipment to tackle fires, animal rescue, chemical spills, road traffic collisions and more," said Tony Oliver, Assistant Director of Digital Systems and Information at Hampshire and Isle of Wight Fire and Rescue Service. It is therefore vital that the partnership makes the best use of technology to ensure our Control firefighters have the tools and information at their fingertips and can mobilise crews as quickly and effectively as possible."

The fully integrated, cloud-based system will provide users the latest in Control Room solutions, increased user functionality and an improved user interface. Hosted in NEC data centres, the system will also enable improved resilience and collaboration across the partnership in the delivery of response to incidents across the seven authorities. The system will also include a live video streaming facility and a mobile application for use by officers.

"The expansion of NFSP to include Kent FRS is testimony to the way that this partnership has developed over the years and it's great to see how our products continue to evolve and support the delivery of mission critical services across the region," said Andy Kerr, Principal Client Director, NECSWS.

The system is due to be fully rolled out in late 2026. ■

MLL Telecom connects classrooms in the southeast via LAN

MLL Telecom will provide schools in the Southeast of England with the latest local area network (LAN) and WiFi technology following a £2 million funding secured under the DfE Connect The Classroom scheme.

A total of 25 academies and schools in East Sussex, Essex, Kent, Hampshire and Surrey will benefit from upgraded fixed and wireless network connectivity supported by structured cabling infrastructure, ensuring higher connection speeds, safety, security and resilience.

"We are extremely satisfied with the work MLL and NCS have delivered in terms of improved network and WiFi infrastructure for our schools. We now have much more reliable connectivity for all our staff and pupils, wherever they are located across the school premises and are already seeing productivity gains and far fewer calls to the helpdesk for slow internet speeds," said Glenn Oakman, ICT Operations Manager at Brighton Academies Trust.

"We are delighted to be part of the DfE's initiative in equipping schools and academies with the secure and reliable high-speed network connectivity that teachers and students urgently need," said Mark Freeborough, MLL Client Manager, Public Sector – South. "Our network solutions will help to maximise the learning experience with the potential for lessons being disrupted by patchy internet connection or slow response times a thing of the past."

MLL is currently contracted by the South East Grid (SEG) to provide a range of full fibre wide area network (WAN) managed services throughout the region, including to schools, councils and other public sector organisations.

"We are very pleased to be making effective use of the DfE's Connect The Classroom initiative. With MLL's ongoing support we can now provide these schools and academies with the secure, fast and dependable network access they really need," said On behalf of South East Grid for Learning, Keith Renshaw, Service Design Manager, IT & Digital, East Sussex County Council. ■

Bridgestone EMEA migrates to SAP S/4HANA Cloud

Syniti has announced the completion of Bridgestone EMEA's transformation project, a migration to SAP S/4HANA Cloud.

The company's goal was to remove siloes across the organisation by consolidating business processes across its SAP ERP Central Component (SAP ECC) system into one SAP S/4HANA Cloud instance allowing the company to improve operational efficiency, data accuracy and set the stage for future growth, automation, and innovation in the tyre and mobility sectors.

A compressed timeline meant multiple data loads had to be fit into a shortened time frame. Outdated systems brought data quality and integration issues, resulting in Bridgestone's business experiencing continuous modifications during the migration process. Despite these challenges, Bridgestone achieved a 100% master data load, significantly enhancing their data accuracy, and achieved a 0.001% variance in inventory reconciliation — a critical component of their financial audits.

Syniti's Data First approach delivered significant results, including a 90% improvement in migrated master data accuracy. This accurate and reliable data became the cornerstone of Bridgestone's new business processes, allowing the company to more fully realise the benefits of its SAP S/4HANA Cloud investment.

"Our company is speeding up its transformation to be even more customer oriented, agile, efficient, data driven, sustainable and future-proof," said Bart Kerkhofs, CIO and Vice President of IT at Bridgestone EMEA. "This necessitates a comprehensive approach that encompasses all facets of our operations including upscaling our digital capabilities to elevate the overall stakeholder experience. Syniti was critical in helping us improve our approach to manage the data for our ambitious transformation effort. The Syniti team has proven they can do the hard things; their credibility was already established, and we knew we could trust their Data First approach to achieve excellent results."

"We are proud to have played a key role in Bridgestone EMEA's digital transformation. Our team's dedication to delivering high-quality data and seamless migration was central to the success of this ambitious project and underscores our commitment to handling the hardest work in data for the world's largest companies like Bridgestone. This collaboration highlights the power of trusted partnerships and the transformative impact of Syniti's software, methodology, and our skilled team of professionals — led by our Data First approach," said Kevin Campbell, CEO, Syniti. ■

EDITORIAL:
Editor: Amy Saunders
amys@kadiumpublishing.com
Designer: Ian Curtis
Sub-editor: Gerry Moynihan
Contributors: Nicola Pearce, Ruchir Brahmbhatt, Mark Jow, Andy Sheldon, Gareth Mitchell, Richard Petrie, Erik Hoeboer, Glen McCarty

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

Mobile phishing threatens enterprise stability

Zimperium's 2024 Global Mobile Threat Report highlights critical mobile threat trends, uncovering a significant rise in 'mishing' – also known as mobile targeted phishing – a technique that employs various tactics specifically designed to exploit vulnerabilities in mobile devices and users. 82% of phishing sites now target mobile devices.

As cybercriminals increasingly adopt a mobile-first attack strategy, they leverage a multitude of techniques to infiltrate enterprise systems by targeting weak, unsecured, and unmanaged mobile endpoints, recognizing mobile as a major entry point to corporate networks and sensitive data.

Cybercriminals are crafting their attacks to exploit the trust employees generally have in their mobile devices. The zLabs researchers found that 76% of phishing sites targeting enterprises are using HTTPS, a secure communication protocol that leads victims to believe the website on their device is legitimate. Employees are less likely to notice these phishing attempts because of their smaller screen sizes and less visible security indicators, such as hidden URL bars.

The success of mishing sites lies in their hit-and-run approach, where cybercriminals can launch deceptive domains rapidly, then have them disappear before they are ever detected, creating significant challenges for CISOs and their teams. The researchers found that around one-quarter of mobile phishing sites become operable less than 24 hours after their creation, launching malicious activities almost immediately.

"It is undeniable that mobile devices and applications have become the most critical digital channels to protect in our organizations," said Shridhar Mittal, Chief Executive Officer, Zimperium. "In today's digital age, where 71% of employees leverage smartphones for work tasks, enterprises must effectively protect their mobile endpoints by adopting a multi-layered security strategy including mobile threat defense and mobile app vetting. Our zLabs researchers meticulously analyzed the nature of mobile attacks, uncovering an attack surface within enterprises that requires a strategic and mobile-centered response."

Along with the rise in mishing, zLabs researchers unveiled the dangers of sideloading apps – the practice of installing mobile apps on a device that are not from the official app stores. Financial services organizations saw 68% of its mobile threats attributed to sideloaded apps. In fact, zLabs researchers found that mobile users who engage in sideloading are 200% more likely to have malware running on their devices than those who do not. Riskware and trojans, applications that disguise themselves as legitimate apps, are the most common malware families found.

Despite frequent updates, enterprises are finding it difficult to manage updates across all devices, highlighting the need for proactive mobile security strategies beyond platform updates. ■

Virgin Media O2 saves £1 million on DC cooling with EkkoSense

Virgin Media O2 has worked with EkkoSense to help achieve significant energy savings, cutting data centre cooling costs by over £1 million annually.

EkkoSense's AI-driven software has enabled a 15% reduction in cooling energy, equivalent to 760 tonnes of carbon dioxide emissions, according to location-based scope 2 accounting.

Virgin Media O2 utilised EkkoSense's solution, which combines IoT sensors with advanced machine learning, to gain real-time insights into thermal, power, and capacity performance across 20 UK data centres.

Virgin Media O2 is working to reduce its energy usage across operations by leveraging technology and innovation to enhance energy efficiency and by sourcing renewable energy to minimise its environmental impact.

"In partnership with EkkoSense, we've optimised our data centres so they operate efficiently, using real-time data so we can make airflow and cooling improvements, resulting in significant cooling energy savings," said Virgin Media O2 in a statement.

"With our software collecting thousands of data points every five minutes – adding to the millions of data points already collected, we're able to continually refine the effectiveness of our machine learning algorithms for Virgin Media O2," said EkkoSense. "Having access to this level of real-time insight means that Virgin Media O2's operations team are able to track how their data centres are performing from a cooling, power and capacity perspective. They are also able to identify further energy optimisation opportunities in terms of cooling energy usage and overall savings." ■

The 40th anniversary of the APC UPS: The journey of innovation continues

It's the piece of IT equipment that most of us take for granted, and it is sometimes forgotten in implementation plans. But it's also absolutely essential to bring reliability to IT operations by protecting everything from desktop PCs to servers to entire data centers.

Of course, we're talking about the uninterruptible power supply (UPS), and this year, we celebrate the 40th anniversary of the first UPS created by APC in 1984 – the 300PC. Now ubiquitous wherever you find IT equipment, UPS technology has grown in sophistication and capabilities thanks to numerous innovations along the way. It's a fundamental component of any new IT implementation or upgrade.

Over the decades, the UPS has grown in stature as IT teams and organizations have become increasingly dependent on data. Now, as the Internet of Things, Artificial Intelligence, and other data-intensive technologies infiltrate our lives, the UPS has never been more important

AI is powering an increasing array of mission-critical applications in every industry, from healthcare to education, manufacturing, logistics, and transportation.

APC started building a market 40 years ago with the 1984 introduction of our first UPS. Then, a few years later, in 1989, we revolutionized power management with the launch of PowerChute™ software, enabling the graceful shutdown of critical hardware and protecting the data on this hardware. The same year, we entered partnerships with two major IT distributors, which proved consequential in building our partner ecosystem.

Throughout the decades, we've continued to innovate. In 1990, we introduced the Smart-UPSTM brand of UPS, now considered the industry's premier network power protection solution. In 2004, we introduced the now industry-leading InfraStruXure architecture, the first scalable modular, energy-efficient, network-critical physical infrastructure (NCPI) architecture, which is an integral part of complete power and cooling systems. For a blast from the past, hop into the Way Back Machine to check out the original InfraStruXureTM offer.

The innovation journey continues

With our industry-leading EcoStruxure™ IT portfolio, our vendor-neutral data centre infrastructure management (DCIM) solutions enable our customers to operate the most resilient, secure, and sustainable IT infrastructure anywhere. We offer business continuity with secure monitoring, management, planning, and modeling from a single IT rack to hyper-scale IT, on-premises, in the cloud, and at the edge.

Other recent innovations include introducing products with recycled and recyclable materials to support your and your customers' sustainability strategies. We've also increased the use of lithium-ion batteries in UPS models, from small home office units to industrial-grade power-protection systems. Lithium-ion enables longer lifecycles and reduces footprint and maintenance costs, all of which contribute to the goal of decarbonization.

Building a sustainable future

Digitization and electrification are central to sustainability strategies across almost every industry. To support these efforts, we are investing in technologies such as the Smart-UPS™ Modular Ultra. The most sustainable UPS of its kind, it aligns with the growing demand for sustainable solutions and recycling programs.

We will continue to innovate as we look into the next 40 years and beyond. And we will continue to rely on you as trusted advisors to our customers to help us make an impact on the market. The journey continues. As in the past, we will walk it together. Please check out our 40th Anniversary website, 40 Years On, for the full innovation journey and see how we can help you evolve your business.

Vodafone and Three UK target the UK's roads and railways with 5G Standalone technology

As part of efforts to build support for a merger with Three UK, Vodafone UK has claimed that their joint plans for a nationwide roll-out of 5G Standalone technology could save regular road users £2 billion a year on fuel and boost productivity through remote working on trains by £1 billion (GVA) a year.

Most existing 5G networks in the UK are Non-Standalone (NSA), which means they're still partly reliant on some older 4G infrastructure. 5G SA, in contrast, reflects a pure end-to-end 5G network that can deliver improvements such as ultra-low latency times, faster mobile broadband upload speeds, network slicing capabilities, better support for IoT devices, increased reliability and security.

Vodafone has already made 5G SA technology available in the busy areas of 23 cities and more than 300 locations across the UK, although it's currently only accessible to customers with supporting devices on their Ultra plans.

But the operator has also pledged, as part of their merger with Three UK, to extend the service to more than 99% of the UK's population by 2034 and push fixed wireless access (home broadband) to 82% of homes by 2030.

As per new modelling by WPI Strategy, there could be up to 28.2 million train journeys every year in the UK where people want to work, but don't due to poor connectivity. Changing this could deliver £1 billion in extra productivity for the UK economy. In addition, the survey claims that 5G SA could help to reduce train delays, which would save £10 million in delay compensation that could be reinvested into critical infrastructure. Similarly, reduced congestion and journey delays for freight drivers thanks to 5G-connected devices on the UK's roads would equate to productivity savings of £140 million per year for businesses in the sector by reducing traffic, making journeys smarter, and deliveries more time efficient. ■

90% of local authorities focusing more on sustainability

Nine out of ten local authorities in the UK have increased their focus on sustainability in the last five years, according to research from OVHcloud.

However, despite this emphasis, 86% have found that cost concerns have impeded progress with projects aiming to improve the sustainability of their organization. Furthermore, 49% have found issues with staff resourcing and skills in realizing projects that will make themselves and their local area more sustainable.

"Many local authorities declared a climate emergency in 2019," said Emma Dennard, VP Northern Europe, OVHcloud. "Sustainability is high on their agenda and continues to rise in importance, but our local authorities need more support in terms of funding and skills to ensure that the UK has sustainability as part of its DNA. Sustainability is a key way to lower power bills, reduce carbon impact and meet the needs of today without compromising the world of tomorrow, so this isn't just a 'nice to have' – it's a business enabler."

With such pressing cost concerns, the report – carried out as an FOI request – also looked at other ways that local authorities are working to become more efficient and innovative.

According to the latest report from the Cloud Industry Forum, 29% of organisations in the UK are using cloud computing to reduce costs, and 96% of the local authorities surveyed reported that they had increased their use of cloud computing in the last five years.

"Cloud computing can significantly enhance the agility and processing power per pound of local government organisations," said Dennard. "But it's also a significant consumer of energy, so it is vital that councils assess the sustainability credentials of the cloud computing providers that they work with, ensuring that they are clear and transparent about their scope one, two and three emissions. This way, organisational drives to be leaner and more sustainable won't be obscured by technology supply chain issues." ■

Northumberland to home Europe's largest AI data centre

A new £10 billion investment will create Europe's biggest AI data centre in Cambois near Blyth, Northumberland, following a deal with private equity firm Blackstone.

Prime Minister Keir Starmer said that the investment, facilitated by the Office for Investment, showed the UK is "open for business."

Blackstone will also put £110 million into a fund for skills training and transport infrastructure in the area.

"The UK is a top investment market for Blackstone because of its powerful combination of talent and innovation along with a highly transparent legal system," said Blackstone's president Jon Gray. "We are making significant commitments to building social housing, facilitating the energy transition, growing life sciences companies and developing critical infrastructure needed to fuel the digital economy. This includes a projected £10 billion investment to build one of Europe's largest hyperscale data centres supporting 4,000 jobs. Blackstone is committed to Britain." ■

Word on the web...

Open source UC: empowering businesses

Ruchir Brahmbhatt, Co-Founder & CTO, Ecosmob Technologies Private Limited

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

Building a secure digital classroom

Nicola Pearce, head of education, BenQ

Digital infrastructures will continue to be a significant part of the classroom and school network. Every piece of technology must be completely secure to safeguard children from potential security risks and inappropriate online content, as well as protect teachers' data.

Schools already have significant experience with security and safeguarding tools and will need to amend these for the digital era. Education establishments can ensure they mitigate any possible security risks or data leaks within the school setting through security measures embedded within tools such as interactive displays, account and device management systems, and online cloud services or software.

The Online Safety Bill, designed to protect children online and tackle harmful material, came into force in early 2023. As technology continues to evolve, legislation will constantly change and be updated, but teachers require a consistently secure classroom in the meantime.

Securing assets for a school network

Both teachers and IT teams can implement a range of tools to secure assets within their classrooms and build a secure EdTech infrastructure. Multi-factor authentication, secure cloud services access, age-regulated or app restrictions, and secure single sign-on (SSO) capabilities enable teachers to safeguard children from inappropriate content and prevent unwarranted access to sensitive information.

The ongoing maintenance and security of devices within a school network is vital. Teachers must be educated on the latest best practices to follow whilst in the classroom, and IT teams must support teachers by leading the implementation of a secure network and technology infrastructure.

Remote management of displays through the cloud can ensure all interactive devices are up to date with the latest software patches to prevent security breaches. This means that central IT teams can manage the security of devices from one remote location, across multiple campuses or schools

How to build a secure digital classroom

Utilising the benefits of the cloud is just one important step towards building a safe and secure digital classroom. Firstly, ensuring lesson materials and documents are safely backed up to the cloud allows teachers to ensure that work is not lost when hardware fails or is stolen.

Secondly, tools like 'single sign on' can be extremely useful for teachers, saving time logging in and out of multiple devices or platforms, and remembering different logins or passwords. But this method can lead to potential security breaches meaning IT teams will need to manage and monitor carefully. IT departments must consider how secure their single sign-on practices are.

Multi-factor Authentication (MFA) and scanning via authenticator apps can also provide extra layers of protection against unauthorised access, especially when devices are shared across multiple classrooms in schools.

Auto-log out methods should be implemented to ensure all devices will automatically log out after periods of inactivity, to ensure students cannot use devices without a teacher present and any data stored on the device is protected from unauthorised users.

Proving that a device has secured the necessary governance guidance and international standards, such as the Product Security and Telecommunications Infrastructure (PSTI) guidelines or the GDPR is one way to ensure the chosen technology is secure. This guidance mandates that manufacturers of UK consumer connectable products comply with relevant obligations to meet minimum security requirements.

All technology should support end-to-end encryption for data transmitted between devices and servers. When shared devices are used, schools must ensure that each user account is compartmentalised, and has its own dedicated space, so that each user has access only to their designated files and data.

How technology can be used to help secure schools

As technology in schools continues to grow, so must the need for robust security. AI is now a fixture in day-to-day life and although many have concerns, it can play an integral part in managing security in schools. For example, many interactive classroom boards currently have two-way mirroring features, meaning students can share from their mobile devices without the need for cables interconnecting the devices.

There are multiple EdTech tools now at a school's disposal, and with this comes the need to ensure that robust security goes hand-in-hand. Practicing good safety measures not only builds a robust online environment but can also teach students the importance of security and embedding safety measures at an early stage, both in the digital classroom and across other corners of their daily lives. ■

No time to waste in stepping up public sector security

Mark Jow, technical evangelist, Gigamon

The UK public sector is failing in terms of its cyber resilience. Over the last few months, we have seen cyber-attacks of significant scale affect the MoD, Electoral Commission and the NHS.

The new UK government brings with it the hope of change. It must lead by example in the public sector and incentivise or regulate to get more organisations to follow best practices for enhanced cyber-resilience. It is encouraging to see that steps have already been taken in pushing forward The Cyber Security and Resilience Bill in the King's Speech on 17 July, which aims to build on the NIS regulations and 'strengthen our defences ensuring that more essential digital services than ever before are protected.'

Understanding the threat

Recent research revealed that 37% of recent breaches go completely undetected by organisations' security tools. This indicates a 20% rise in missed security breaches over the last year. While cyber criminals continue to innovate and find new ways to evade traditional security controls, ever more complex IT environments pose organisations' security stacks with a serious challenge.

For the public sector, the cloud offers optimised workflows, scalability, and more efficient use of resources. But, just as private organisations have experienced in their cloud adoption journeys, the hybrid cloud introduces a wider attack surface that conventional cloud or on-premises security tools might struggle to monitor accurately. In modern, hybrid cloud environments, network blind spots are proliferating, allowing criminals to hide out and launch attacks completely unseen.

Legacy hurdles and visibility

Unlike their private sector counterparts, public sector organisations still rely heavily on legacy systems. Earlier this year, a government report highlighted that 43 legacy IT systems across government are at a critical level of risk — 11 of which are in the MoD. Integrating these legacy systems with a hybrid cloud strategy only adds to complexity and according to research 83% of global IT and security leaders believe that cloud complexity increases cyber risk. The problem is that traditional on-premises monitoring tools lack the necessary visibility into cloud-based threats, while in turn, cloud-centric tools often have limited insight into on-premises traffic. This creates a significant 'visibility gap' that attackers are adept at exploiting.

Ultimately, cyber-resilience must start with improved visibility – you can't manage what you can't see. That means real-time, network-level intelligence that can spot suspicious activity even in encrypted traffic.

Reducing inherent trust

Public sector security teams must move beyond the common 'trust but verify' approach among internal stakeholders and employees, instead working towards a Zero Trust architecture. When passwords are easily stolen, phishing is rife, and unpatched home devices create security gaps, inherent trust introduces far too much risk. Multi-factor authentication (MFA) is key to this.

Architecturally, this should be paired with network segmentation and real-time, ongoing threat monitoring to detect and remediate any attackers moving laterally within the system. This offers 'defence in depth,' meaning that if one security barrier fails, bad actors cannot roam freely. Deep observability is vital to achieving this, combining real-time network intelligence with traditional logs, metrics, events and traces insights to give a complete 360-degree picture of all data in motion. Only then can IT teams prevent hidden threats.

Supporting tool investments

As threats continue to evolve and proliferate, organisations are tempted to throw more investment into security tools to mitigate the rising risks. But this ultimately leads to bloating tool stacks with no real security improvements. With 9 in 10 organisations reporting that they are regularly investing in new tools, but 69% of security leaders reporting that their teams are overwhelmed by tool sprawl, it's clear that this is not the answer.

Organisations need to turn their attention back to their existing tools to determine where they work well and where they create blind spots or need support. This means creating a stack of tools that work in a cohesive manner and improving tool efficiency by focusing on high-fidelity network data. By employing tactics like application filtering, security teams can separate high-risk traffic from low-risk, ensuring decryption efforts are focused where they matter most. Additionally, deduplication techniques prevent redundant decryption of the same data packets, significantly reducing processing load and saving valuable resources.

A data-driven approach to security stack optimisation ensures existing tools operate at peak efficiency. This frees security teams from the burden of managing a bloated toolset, allowing them to focus on real threats and streamlining security operations. When coupled with real-time network visibility and a Zero Trust strategy, this sets any public sector organisation on the right path to better cyber resilience. ■

"Recent research revealed that 37% of recent breaches go completely undetected by organisations' security tools. This indicates a 20% rise in missed security breaches over the last year."

Is every enterprise benefitting from business-quality broadband?

Maybe, maybe not - but as always, there's room for improvement...

Despite the widespread availability of gigabit connectivity, London's small and medium-sized businesses (SMEs) continue to struggle with slow and unreliable broadband, leaving many at a disadvantage in productivity, innovation and competitiveness.

New analysis from G.Network shows that SMEs are missing out on an estimated £28 billion in annual revenue due to slow and unreliable broadband. The annual lost output is estimated at £5.34 billion Gross Value Added (GVA). 25% of senior leaders and business owners of London SMEs admit that problems with slow or unreliable broadband have caused them to lose business; and 47% identified employee connectivity in the workplace as an area undermined by poor connectivity.

"Digital connectivity is at the heart of London's economy, but despite extensive availability, the SMEs we've spoken to recently are still suffering because connections are too costly and complicated," reports Kevin Murphy, CEO of G.Network. "Poor connectivity has pushed more than half of senior leaders and business owners of London SMEs to consider moving office location to get better access to faster and more reliable workplace internet, while four in 10 state they can't serve clients in the way they'd like due to problems with slow or unreliable office internet."

With this latest study direct from the nation's capital – and arguably, the best connected city the implications for UK-wide connectivity are stark…

Need for speed

With an average business broadband speed of just 73.21Mbps in the UK, there are significant implications for businesses.

Sectors like technology, media, and finance require higher speeds to handle large data transfers, video conferencing, and real-time analytics; 73.21Mbps is likely insufficient. As highlighted by G.Network, slow broadband speeds can impact productivity, especially if businesses rely on cloud services, video conferencing, or real-time data processing. Further, for businesses with online customer interactions or e-commerce operations, slow speeds can lead to poor user experiences and customer churn.

Rick Mur, CTO at GNX, however, reports that "much higher speeds are typically available in any part of the UK; it may involve installing fibre optic cabling which introduces a one-time cost, but after that the connectivity options are limitless. We also recommend businesses to not use typical broadband


Sam Hales, MS3 Networks


Rick Mur, GNX


Kevin Murphy, G.Network

or even business broadband circuits as they come with minimal to no SLAs and are based on the same network as consumer internet - which is highly oversubscribed, meaning no guarantees on bandwidth. Dedicated Internet Access (DIA) circuits are a much better option for any business."

"Although the UK's average broadband speed stands at 73.21Mbps, it's important to look at the progress that has been made in recent years," opines Sam Hales, Business Development Director (B2B), MS3 Networks. "According to Ofcom data, the nation's average upload speeds increased 73% between March 2022 and March 2023. During the same period, the gap in download speeds between urban and rural areas dropped from 58% to 26%, enabling more rural businesses to enjoy the benefits of ultrafast connectivity. Much of this progress can be attributed to the success of the UK's full fibre rollout."

According to Uswitch data, around 61% of UK premises now have access to full fibre, with the government aiming to make it available nationwide by 2030. However, Hales adds that some businesses are still in danger of being left behind: "currently, just over half of UK SMEs can access full fibre. Even when full fibre is available, uptake of the service is often low, standing at 28% of all UK premises where it is available."

Picking the right package

For a business to succeed in this digital era, having the right broadband can be make or break. When evaluating the most important features of a broadband package, it's crucial to consider the specific needs and priorities of the business.

"Before signing up for a business broadband package, it's important to consider how many employees use the internet simultaneously, what they use it for and the potential impact of any loss of service," suggests Hales. "The number of staff using the internet can help you decide the internet speeds you will need. You should also consider the types of activities employees carry out. For example, if you frequently make video calls, it's better to opt for a synchronous network. This means that upload and download speeds are the same, which is essential for tasks that require the upload of large amounts of data."

"We look at multiple factors to identify the right solution for a customer," agrees Mur. "How many users make use of the link at the same time? What profile of users does the company have (team calls, video editing, graphic designers, etc.)? Where are most of the resources hosted: in a private data centre, inside a public cloud or SaaS applications? Urgency of installation? SLA requirements? Growth trajectory of the location?" The answers to all these questions help outline the needs of each specific enterprise.

Reliability is, of course, crucial for any business to avoid disrupted business operations, lost productivity, and revenue impacts.

"Considering the potential impact of network failures on your business can guide you," says Hales. "Full fibre broadband that connects fibre cables straight to your premises is much more reliable than older services relying on copper wires, such as fibre to the cabinet (FTTC). Even so, if extended time without access to the internet would cause huge issues for your company, a business plan offering round-the-clock customer service, and a minimum service guarantee would be best."

Quality of Service (QoS), too, is key, enabling the prioritisation of certain types of traffic over others, and ensuring that critical applications receive the necessary bandwidth and performance; this is particularly important for businesses that use applications requiring real-time data or those with high demands on network performance.

Bandwidth and speed also have a huge impact on the success of a broadband network. Adequate bandwidth supports multiple users and devices, ensures smooth operation of cloud applications, and handles large file transfers, while faster speeds contribute to quicker download and upload times, and better performance for web-based applications. Moreover, with business success comes growth – the network must be scalable to support expansion.

Mur highlights that "latency is an often overlooked but absolute key requirement that has to be taken into consideration when deciding on a new internet connectivity solution. You can have a link with a huge amount of bandwidth, but when your destination is on the other side of the world, latency can cause transfers to be a lot slower than expected. Latency is caused by many different elements on the internet. Distance being the key factor, but a poorly designed network also contributes."

With cyber-attacks on a seemingly endless rising trajectory, security features like firewalls, anti-virus protection, and DDoS mitigation built into the business broadband package is becoming more common.

"It's essential that ISPs put the necessary measures in place to protect businesses from cyber risks. Although most employees know the dangers of choosing weak passwords or clicking links from unrecognised senders, the increasing volume and sophistication of cyber-attacks can leave businesses vulnerable. According to 2024 UK Government data, half of businesses have experienced a cyber security breach or attack in the last twelve months, with large and medium-sized businesses most at risk," opines Hales. "Many ISPs already offer security services such as firewalls and threat detection, but as the number of cyber-attacks continues to surge, we're likely to see business ISPs widen their security offering further."

Indeed, as cyber-threats become more sophisticated and widespread, many businesses now view security as a fundamental aspect of their internet service. But will security ever come as standard in business broadband services?

"For business usage: no. Security should be a part of the whole IT infrastructure of an enterprise network," opines Mur. "The internet provider (on a single location) should not be involved, and a third-party SD-WAN/SASE solution is a much more preferable solution. Transparency is key for business broadband or any type of internet connectivity for businesses."

Avoiding the pitfalls

Selecting a new business broadband provider is no easy feat; organisations should be aware of several potential pitfalls to ensure they make an informed decision.

"There are a number of elements that make it hard to compare apples to apples like different terminology used by various providers, and non-transparent models with companies buying from other companies where it is unclear who will deliver the actual service," explains Mur. "Looking for an honest, transparent partner that understands the business and technical requirements is key."

Inadequate bandwidth is a common challenge, with some providers overpromising on speeds, which it turns out aren't consistently achievable due to network congestion or infrastructure limitations. Business should thus check if the speeds are for peak times or average performance; these can be verified with customer reviews or a trial.

Hidden costs and fees are another concern. It's vital that the enterprise understands all terms and conditions, including early termination fees or penalties, and be clear about any extra charges for exceeding bandwidth limits or for services like static IP addresses or additional support.

Indeed, "failing to read the terms and conditions of your broadband plan can end up costing you in the long run," warns Hales. "Although business broadband packages are usually advertised with a single monthly cost, ISPs could increase their prices in line with inflation every April. This means that if you enter a 24-month contract, you could potentially face two price increases in that time. Ofcom has cracked down on this practise and will require ISPs to state these intended price increases in pounds and pence from 17 January 2025. However, with many providers applying a flat rate rise to all contracts, this change will disproportionately affect businesses on low-cost plans, which will see the biggest increases as a percentage of what they pay."

Preparing for the future

To future-proof business operations with a broadband package, it's important to consider factors that will support growth, evolving technology needs, and operational resilience.

With bandwidth demands increasing near-daily, many industry experts suggest opting for full fibre – even if the business need is not yet there. Fibre offers the highest speeds and reliability, which is crucial for handling increasing data demands, supporting high-definition video conferencing, and using cloud-based applications; and is generally more future-proof compared to DSL or cable.

"For small businesses, or those that don't rely heavily on the internet to undertake their daily activities, it can be tempting to stick with an older form of internet such as FTTC or an advanced digital subscriber line (ADSL) service. However, even for companies that don't need the high speeds of full fibre, opting for this form of connectivity helps to future-proof operations," advises Hales.

As well as prioritising today's demands – reliability, QoS, bandwidth, etc. – IT teams should plan for advanced technologies such as IoT, 5G, AI and ML which are becoming increasingly integral to business operations.

In 2024, future-proofing business broadband must naturally include considerations for hybrid working, which has placed further pressure on broadband speeds and bandwidth.

"With ONS data showing that around a quarter of UK employees worked on a hybrid model between 22 May and 2 June 2024, we're seeing many ISPs tailor their services to this adapted way of working," reports Hales. "Providers offering home office or hybrid worker plans highlight the benefits of business broadband, such as enhanced security, ideal for home workers who need to access confidential or highly sensitive data."

"We've seen the impact in that demand for internet-based connectivity options is rapidly growing for businesses," adds Mur. "Companies are moving away from traditional private connectivity options (like MPLS) as more applications are hosted and accessed from outside the customer premises."

To meet growing demand, there has been increased investment in broadband infrastructure, including the expansion of fibre-optic networks and improvements in 5G coverage. While urban areas are seeing faster improvements, rural areas still lag – raising questions about the longer-term viability of remote working from rural regions… ■

Uncovering the connectivity pain points for the UK's SMEs and sole traders amid the copper Switch-Off

Andy Sheldon, CTO, Everflow

The UK's telecoms landscape is on the cusp of a major transformation. The impending copper switch-off, which will see traditional copper-based landlines replaced by digital broadband connections, marks a significant step towards a fully connected, future-ready Britain. However, for many of the UK's small and medium-sized enterprises (SMEs) and sole traders, this transition presents a mix of opportunities and challenges.

The Switch-Off impact

Scheduled for completion by the end of 2025, the copper switch-off is a necessary evolution to modernise the UK's communications infrastructure. It promises faster, more reliable internet services and supports the growing demands of digital business operations. Yet, while large enterprises are generally well-prepared for such changes, the same cannot always be said for SMEs and sole traders.

For smaller businesses, the switch-off can be daunting. Many are still reliant on traditional phone lines for day-to-day operations, whether for customer communication, processing payments, or even for alarm systems. The transition to a fully digital system requires not just a shift in technology, but also a change in mindset and business processes.

Connectivity pain points

One of the most pressing issues facing SMEs and sole traders is the sheer pace of technological change. For businesses with limited resources, keeping up with the latest developments can be challenging. The copper switch-off is just one part of a broader digital transition.

1. Infrastructure gaps – many SMEs, particularly those in rural areas, face significant infrastructure challenges. Access to high-speed internet remains inconsistent, leaving some businesses struggling with inadequate connectivity.
2. Cost concerns – SMEs often operate on tight budgets, and the costs associated with new equipment, installation, and potential service disruptions can be significant. Moreover, the ongoing expense of higher-speed internet packages can add to their operational burdens.
3. Knowledge and expertise – for sole traders and smaller businesses without dedicated IT support, the technical aspects of the switch-off can be overwhelming. Understanding what is required, navigating contracts with providers, and ensuring a seamless transition without disrupting business operations are all potential pain points.
4. Reliability and security – with digital connectivity becoming the backbone of business operations, any downtime or service interruptions can have a series impact. Additionally, the shift to digital brings with it heightened concerns about cybersecurity, with smaller businesses often lacking the robust defences of larger corporations.

Actionable strategies

To navigate these challenges, SMEs and sole traders need to take proactive steps to ensure they are not left behind by the digital transition.

1. **Conduct a connectivity audit** - the first step is to assess current infrastructure and identify what changes are needed. This includes evaluating existing contracts, understanding the specific requirements for a digital setup, and identifying any potential barriers to implementation.
2. **Explore financial support options** - there are often grants, subsidies, or support packages available from both government and private entities designed to help smaller businesses with the cost of digital upgrades.
3. **Partner with the right providers** - businesses should look for partners who understand the unique needs of SMEs and can offer flexible, scalable solutions. This includes looking for providers who offer bundled services, combining telecoms with other utilities to simplify billing and reduce costs.
4. **Prioritise cybersecurity:** with the move to digital, cybersecurity must be a top priority. SMEs should seek advice on best practices for securing their networks and data.
5. **Engage in continuous learning:** the digital landscape is constantly evolving, and SMEs need to stay informed about the latest developments.

A final word

The copper switch-off is a pivotal moment for the UK's telecoms infrastructure, but it doesn't have to be a source of anxiety for SMEs and sole traders. By taking a proactive approach and leveraging available resources, small businesses can navigate the transition and thrive in the new digital landscape. As the digital future becomes the present, the time to prepare is now. ■

AI - bane or boon for business?

AI continues to plough through the IT sector, changing the networking world forever. What are the implications for IT teams; and is the governance where it needs to be?

Implementing AI into today's networks requires a structured approach with several essential building blocks, encompassing technology, strategy, infrastructure, and governance to ensure the AI implementation achieves both business goals and complies with safety standards.

First steps

"AI can dramatically improve and accelerate network planning, operation and monetisation. Realising that potential cost-effectively and in a safe manner requires four building blocks to be in place," says Abhishek Sandhir, Managing Director of Telecommunications for Sand Technologies.

First is a shared understanding of what success looks like and the problem the operator is trying to solve. Second up; the company needs a clear handle on its information journey: the data flows, exchanges, transformation and normalisation.

"Third is a dedication to compliance with GDPR, confidentiality and data sovereignty - which are important because they're required for any data handling, and because this dedication can help build trust among those stakeholders who are still sceptical about AI," shares Sandhir. "The fourth building block is a risk analysis of the decisions and activities that can be outsourced or automated versus left to human intervention, and the creation of any related guardrails that the enterprise deems necessary."

AI systems require large volumes of high-quality, clean and diverse data. Implementing mechanisms to collect, integrate, and manage data from various network sources is essential. Data governance policies to manage data ownership, security, and privacy, while also ensuring data consistency and accuracy, are required. With this data comes the responsibility to ensure security; implementing encryption (both in-transit and at-rest) ensures that sensitive data remains secure throughout the AI processing lifecycle.

"Data is the cornerstone," says Chris Gilmour, CTO at Axians UK. "AI systems often handle sensitive data, making security a top priority. Robust network infrastructure, data encryption, and access controls are essential to protect against unauthorised access and data breaches. Organisations must develop guidelines and frameworks to ensure that AI is used responsibly, avoiding biases, discrimination, and unintended consequences."

Implementing AI at scale requires specialised skills, including data science, machine learning, model management, and AI ethics. Companies need to assess whether they have in-house expertise, particularly since AI will impact the day-to-day responsibilities of IT staff.

"Scaling AI across the network is a worthy goal, but every great journey begins with a first step," opines Sandhir. "Before an enterprise can reach that target, they need to consider whether they have the capability in-house and/or with partners to understand, implement and manage a broad AI deployment. Scaling AI requires technical expertise of course, and partners bridge that gap effectively."

Chris Gilmour

Abhishek Sandhir

Likewise, businesses should evaluate whether their current infrastructure can handle the workloads. High bandwidth and low latency networks are required to support data-intensive operations, especially when dealing with IoT devices or cloud-based AI applications.

Then comes the choice of AI algorithms and models. Using pre-trained models or open-source repositories can reduce development time and costs. Fine-tuning these models for specific tasks within the network can further optimise performance. For domain-specific use cases, custom AI models must be built and optimised for tasks like anomaly detection, predictive maintenance, or traffic routing.

Indeed, "the choice of AI algorithm is crucial. Deep learning, machine learning, and other techniques each have their strengths and weaknesses," says Gilmour.

Rules and regulations

The UK's regulatory framework for AI and data-driven technologies is relatively advanced, but there are concerns about whether it extends far enough.

Indeed, several gaps could be better addressed to ensure AI and data-driven technologies are used safely and responsibly. These include a comprehensive, AI-specific regulatory framework akin to the EU AI Act; the absence of a legally binding, overarching AI regulation leaves organizations without clear, standardised rules governing the development, deployment, and accountability of AI systems across all industries.

"While there are general principles governing AI ethics, more concrete rules and standards are needed to ensure that algorithms are fair, transparent, and accountable," opines Gilmour. "Enforcement mechanisms should be strengthened to hold organisations accountable for any harmful or discriminatory AI applications."

"As is expected when working with any fast-evolving technology, there are opportunities to improve," shares Sandhir. "For example, more must be done to safeguard network vulnerabilities and mandate system resilience for major carriers, the recent Crowdstrike outage being just one recent example."

This holds true particularly for high-risk areas like healthcare, law enforcement and critical infrastructure, where safeguards might be considered insufficient. In healthcare, an AI-driven diagnostic system can have life-or-death consequences, and regulations don't sufficiently address the nuances of AI decision-making in these areas.

Bane or boon?

AI is both a boon and a potential bane for IT teams, depending on how it's implemented and the context of use. The impact of AI on IT teams varies based on factors like job roles, organisational culture, and preparedness for AI-driven transformation.

On the boon side, AI can automate repetitive tasks, perform predictive maintenance, and detect system anomalies. With improved efficiency and productivity, AI systems can provide insights and recommendations to IT teams by analysing vast amounts of data; help diagnose and resolve issues quickly; and optimise resource allocation. Moreover, AI-powered cybersecurity tools can continuously monitor network traffic, user behaviour, and system logs to detect anomalies, while evolving in real-time to new and unknown threats.

"The potential benefits of AI are significant. By automating repetitive tasks, IT teams can free up valuable time to focus on more strategic initiatives," confirms Gilmour. "AI can also help improve network performance, optimise resource allocation, and enhance security by detecting and responding to threats more effectively."

In the bane column comes challenges with the skills gap, increased complexity in system management, and difficult integration into legacy system, which can require significant investment in time and resources. Beyond the security and ethical concerns, there also comes the risk of opaque decision-making; this lack of transparency can be problematic for IT teams, especially in high-stakes environments where explainability is crucial.

"It's not hyperbole to say AI can, will and is revolutionising modern networks," says Sandhir. "IT teams must therefore not only embrace the technology but lead the AI revolution. It is incumbent upon us all to create a culture where the UK is leading the way in AI and adopts a mindset of driving success through innovation, regardless of the level of complexity." ■

Emptying the bins with IoT

Gareth Mitchell, UK partner manager, Heliot Europe discusses how sensors, IoT and LPWAN technology can minimise waste within manufacturing, and improve the refuse collection process

Manufacturers are increasingly burdened with rising energy and labour costs, regulatory demands, and growing environmental responsibilities. Among the common issues they share is inefficient waste management. Traditionally, industrial waste bins, particularly in vast setups like automotive production lines, are emptied on a fixed schedule, often before they are full, resulting in wasted resources. Internet of Things (IoT) technology presents a solution by equipping bins with sensors that are able to monitor fill levels. This enables real-time data collection to optimise waste collection processes, reduce unnecessary trips, and for the reallocation of human resources to more critical tasks. Gareth Mitchell, UK partner manager, Heliot Europe discusses how sensors, IoT and LPWAN technology can minimise waste within manufacturing, and improve the refuse collection process.

The hidden inefficiency in waste collection

To grasp the magnitude of the waste management problem in manufacturing, consider a typical example from the automotive manufacturing industry. In this industry, production lines can span to more than a kilometre in length, with individual disposal bins at each stage for different types of waste - standard, specialised, or recyclable. In an ideal situation, these bins should be emptied when they are full, but this is often not the case.

In many scenarios, subcontractors are used to collect waste from bins. When bins are not completely full, these trips are wasted. As well as this, the manual method of monitoring the fill level of a bin is often wasteful. In manufacturing environments, employees are generally pulled away from their typical work locations to manually inspect bins, depending on the manufacturer's process and type of waste, which reduces potential productivity and output for these workers. Moreover, in the absence of specific monitoring data or insights, the frequency and timing of collection often becomes incorrect and poorly coordinated. Is it truly efficient for staff to spend time inspecting fill levels of rubbish bins when they could be engaged in more productive activities?

As a result, the whole waste collection process can be inefficient for many manufacturers, both in terms of how the bins are filled and how resources and productivity are squandered in managing or collecting them. Should manufacturers really be paying subcontractors to collect bins when they aren't full? All these inefficiencies highlight the need for tracking of waste within bins and improved communication when bins need to be collected and replaced.

Automating waste management

A more effective alternative to collecting partially full bins or manually checking a waste disposal status is to utilise IoT technology. This can significantly enhance human productivity and efficiency, while streamlining the tracking and collection of bins. By equipping bins with IoT sensors connected to back-office IT systems, they can provide real-time or as near to 'real-time' data on waste levels. This kind of information could digitise the management of waste more effectively.

The sensors can measure the bin's volume or mass, providing data about how full the bin is. This information can be shared with manufacturers and third-party waste collection firms to determine the optimal time or day to collect waste. With sensors indicating fill level (e.g., by weight or fill level), manufacturers can reassign employees to other tasks within the organisation too, thus recovering this lost productivity.

Connecting bins to the internet via the sensors also allows manufacturers and sub-contractors to accurately track bin locations and assess any replacement needs at the same time too. Questions like whether the collection schedule with the subcontractor needs to change, or if there is a more sensible route within the factory itself to collect the waste can be addressed, for example. This data could significantly improve the waste management strategy for manufacturers.

In some scenarios, manufacturers use reusable packaging for storing or transporting goods. For instance, in glass production, where car windscreens are produced, the windscreen might be produced and loaded onto A-Frame Stillages (trolleys or racks) and transported to automotive manufacturers, who then return the racks to the glass manufacturer. In this example, IoT sensors can help to track and trace the location of these racks and other reusable packaging, ensuring they are returned and re-used effectively. And this approach is not unique to this example either - it also has applications and uses within other reusable packaging scenarios.

Connectivity and sensors

A major advantage of this technology is that these sensors can be retrofitted onto existing bins within manufacturing warehouses and locations. These sensors are also designed to be able to connect to various data networks in several ways too. In environments where WiFi and 4G struggle (cellular) to penetrate metal and large machinery, the most cost effective and reliable method of data connectivity comprises using a selection of appropriate forms of low powered wide area network (LPWAN) connectivity.

LPWAN connectivity is preferable in this scenario because LPWAN networks comprise wireless wide area network technologies that interconnect low-bandwidth, battery-powered devices with low bit rates over long ranges. This is key because it helps to bring down the cost of transmitting the data. Furthermore, because the transmission of more data often results in increased costs and power usage in sensors and IoT devices, it is important, where possible, to maximise their battery life. This is especially important because, once a device is in the field, frequent battery changes are expensive and challenging. LPWAN devices typically last around five or so years in these scenarios.

Another reason that many organisations opt for LPWAN connectivity over cellular is because LPWAN connectivity gateways can be easily set up across manufacturing sites or production facilities with ease. This capability allows for the connection of devices in challenging environments with limited signal, and even allows for installations underground. Moreover, it is also relatively straightforward and faster for an LPWAN provider to set up additional network connectivity than it is for a mobile phone company to expand their existing network. Moreover, LPWAN providers typically offer more robust service level agreements compared to cellular providers. These benefits make LPWAN technology an excellent choice for connectivity in smart waste management services, offering cost and time efficiencies in installation, operation and maintenance.

Conclusion

In manufacturing, efficient waste management is paramount, not just for cost saving reasons but also for enhancing productivity and sustainability. The integration of IoT and LPWAN technologies provides a robust solution for manufacturers, addressing inefficiencies inherent in traditional waste management processes. Moreover, the adoption of LPWAN connectivity ensures robust and reliable data transmission, even in challenging environments, further streamlining the waste management process. This connectivity promotes an effective use of resources, making the entire operation more efficient and sustainable.

As the manufacturing sector continues to grapple with rising energy costs, labour shortages, and increased regulatory pressures, embracing these technologies is an attractive solution for manufacturers across a broad range of industries. IoT enabled smart bins and LPWAN connectivity represent a way forward in waste management techniques, offering both economic and environmental benefits. ■

KOKO ushers in nightlife-as-a-service

Following a £70 million restoration, London's iconic KOKO reopened its doors, now offering a one-of-a-kind physical space and media facility that offers an unrivalled experience for live music fans. Launched in partnership with SISTER, the new KOKO marries historic buildings with state-of-the-art technology to build on a long cultural legacy and protect the city's nightlife for future generations.

However, KOKO's revitalisation goes beyond the realms of architecture and design. The team wanted a space where artists can create without limits, an all-encompassing location in which music can be performed, produced, and streamed around the globe. The entertainment world is going in new directions and this venue of the future needed the technology to match.

Redefining experiences

From an IT perspective, KOKO's complete metamorphosis presented exciting opportunities. Untethered by existing hardware, the team was free to define the experiences that they wanted to create and then select the tech to get them there.

Handling the extraordinary new broadcasting, recording and live streaming capabilities required a sophisticated new network with world class software and expertise in wireless technology was vital. After an extensive RFQ process, Qolcom was chosen as a natural fit with its leading-edge Network-as-a-Service offering.

Nightlife-as-a-Service

The KOKO team wanted an IT partner that could deliver impactful results. Network-as-a-Service (NaaS) was identified as an ideal solution, offering a modern, pay-as-you-go model, easing pressure and freeing up cash flow at a crunch time. With NaaS, network set-up and management are simplified, and KOKO could pre-empt and auto-fix issues and stay one step ahead of advancing technology.

As part of a 5-year NaaS plan, KOKO has underpinned its experiences with a network that is smart, secure, and scalable; and with round-the-clock support from Qolcom experts if ever they need it.

"By choosing NaaS, KOKO makes sure they keep their edge. The technology we've deployed for them is the absolute best in class right now. But technology iterates quickly, as do business requirements and customer expectations. Thanks to NaaS, KOKO has the agility to upgrade their tech in the future to stay ahead of the curve," said Stuart Pass, Chief Technology Officer at Qolcom.

Qolcom engineers set about mapping infrastructure to KOKO's high ambitions, alongside making sure that the technology was sympathetic to the building's heritage. Working closely with the leadership team, Qolcom plotted the design for a high-performance, wired and wireless IP infrastructure over which voice, data, and multi-media applications can operate over multiple buildings and floors. This works in tandem with an enterprise grade IP-based network solution that offers lightning-fast connectivity for all IT and Audio-Visual service requirements along with support for CCTV and Building Management Systems.

"At KOKO we had a special opportunity to start with a blank canvas. It was like song writing, in a way. It began with a creative vision – then it's about layering on all these instruments and locking them into step so that the whole piece works in harmony. The use of the Aruba Central platform in our Network Operations Centre is the key that binds the NaaS together," said Keith Reading, CEO at Qolcom.

No stone left unturned

KOKO is internationally renowned as an inclusive and eclectic space that welcomes music fans of all genres and eras. Proud of the new venue, the owners wanted to amplify the KOKO experience for people to enjoy wherever they are in the world.

Broadcasting in high definition to a diverse range of devices requires a network that securely manages a multi-tiered environment. The next-generation Aruba Edge Services Platform (ESP) gave Qolcom all the tools it needs to deliver NaaS. This full-stack, edge-to-cloud solution includes networking and security. Data from the edge drives real-time automation and actionable insights and built-in AI Ops help Qolcom analyse a vast body of information in new ways, so they deliver a quality NaaS to KOKO.

The Qolcom Network Operations Centre (NOC) utilises Aruba Central as the conductor that orchestrates Aruba ESP, a cloud-smart networking solution, so the Qolcom NaaS team have an unprecedented level of control. Wired and wireless infrastructure are unified in a holistic system that the NOC can manage from a single screen. The network also handles building management, security and CCTV systems as part of a 360-degree network strategy.

One notable feat was the successful delivery of a consistent Wi-Fi signal to all points in the building, from dome to loading bay. Starting with LAN infrastructure, Qolcom designed a resilient network of core routing services with sufficient bandwidth to scale and support future traffic. Network devices, including redundant power supplies, provide data connectivity and PoE/PoE+ (Power-over-Ethernet/Plus) and WLAN access points support AV equipment and CCTV cameras. Finally, all equipment is Wi-Fi 6E grade, which delivers greater capacity and performance, superior power efficiency and enhanced support for IoT devices. ■

Hydes navigates the path to PCI Compliance

Independent family pub, retailer and brewer, Hydes, was founded in 1863, and has remained an independent brewery in the Northwest of England and North Wales ever since.

Like other breweries, Hydes must comply with the Payment Card Industry Data Security Standard (PCI DSS), which exists to help keep sensitive financial information safe from theft, hacking, and other security threats.

Long-time partner Evolve has worked with Hydes for almost a decade, supporting its connectivity needs from point-of-sale and printers to CCTV and guest Wi-Fi. Evolve provides Hydes with a customised SD-WAN solution that boasts PCI Level 1 certification for payment security, and until recently, the business was able to complete a PCI self-assessment form to remain compliant. However, recent increases in payment card turnover meant an external audit was required, with a PCI assessor visiting sites to gather evidence that both Hydes and its third-party suppliers are PCI compliant. It would require not only additional resources but valuable hours for Hydes to gain external certification.

Safeguarding the business

Early in 2024, Evolve stepped in to oversee the entire external certification process. From working directly with Hydes POS provider and ensuring they have the right certification, to supporting site visits in-person, Evolve was able to complete the assessment on behalf of Hydes.

Although the process required extensive up-front work to prepare for the assessment questions and documentation requirements, this ultimately proved a time-saving exercise for Hydes. Not only did it negate the need for inhouse resource to be tied up by the process, but thanks to Evolve's long-standing relationship with Hydes, extensive knowledge of the PCI process and customisable boilerplates, Evolve's help in ensuring Hydes is fully PCI compliant has ensured the protection of card holder data, reduced the risk of data breaches, and safeguarded the business's reputation.

Working with the Evolve team has also brought a range of additional benefits. Hydes' 24/7/365 fully manned network operations centre has proven invaluable to businesses in the hospitality sector, which often operate outside core hours and require round-the-clock trouble-shooting support. Indeed, Hydes' managed network solution provides a complete and end-to-end network infrastructure, including hardware, software, as well as ongoing support, providing hospitality clients a consistent and secure internet connection, regardless of the size and complexity of their property.

Customised solutions

For merchants to thrive in these challenging times, it's vital that they remain PCI compliant. Evolve's customised solutions with PCI Level 1 certification for payment security as a Mako Network platinum partner help ensure success.

For Hydes, Evolve was able to reduce the length of the external PCI Compliance process significantly. Thanks to the expertise of the Evolve team, all the required documents and evidence of policies was gathered with minimal input from Hydes, and the business has now achieved external PCI certification. ■

How to protect data centres as Critical National Infrastructure

Richard Petrie, CTO, LINX (London Internet Exchange)

The recent announcement on 12th September saw the UK government officially designate data centres as critical national infrastructure (CNI), marking a significant recognition of their importance to our modern digital society.

This move highlights the evolving understanding of what constitutes essential infrastructure, and it brings to light the growing dependence on digital connectivity. As of March 2024, the UK had the third highest number of centres in the world, behind the USA and Germany, with 514. But what does this classification mean for the protection of data centres, and how can we safeguard such vital assets in a world increasingly prone to both cyber threats and environmental risks?

When protecting our digital infrastructure, the primary solutions fall to network resilience and network redundancy, both with the ultimate aim of minimising downtime. The recent CNI designation should form part of a wider digital protection strategy, creating protocols and fail-safes to reroute network traffic in the event of an outage.

Network resilience

Network resilience is a network's ability to withstand, absorb, and bounce back from unforeseen events that could impact its performance and availability. It is a wider strategy involving redundancy, diversity, flexibility, scalability and security.

"For critical services such as water supply, energy grids, transport and care systems, continuity is vital. These sectors depend heavily on communication networks to manage operations around the clock and respond to emergencies."

With important systems such as healthcare, transport and education reliant on digital connection, it's vital that networks are built with resilient infrastructure and protocols in place to ensure connections always remain online. Critical industries can't afford to have downtime.

Cyber-attacks and extreme weather pose significant risks to increasingly digitised CNI systems. As these systems become more vulnerable to cyber intrusions like hacking and ransomware, a successful attack on a data centre could disrupt vital communication networks and public services such as healthcare. Additionally, climate change exacerbates the threat of severe weather events, which can disrupt power supplies and damage infrastructure. Data centres, reliant on stable electricity and cooling, are particularly at risk from prolonged outages or flooding, potentially crippling essential services.

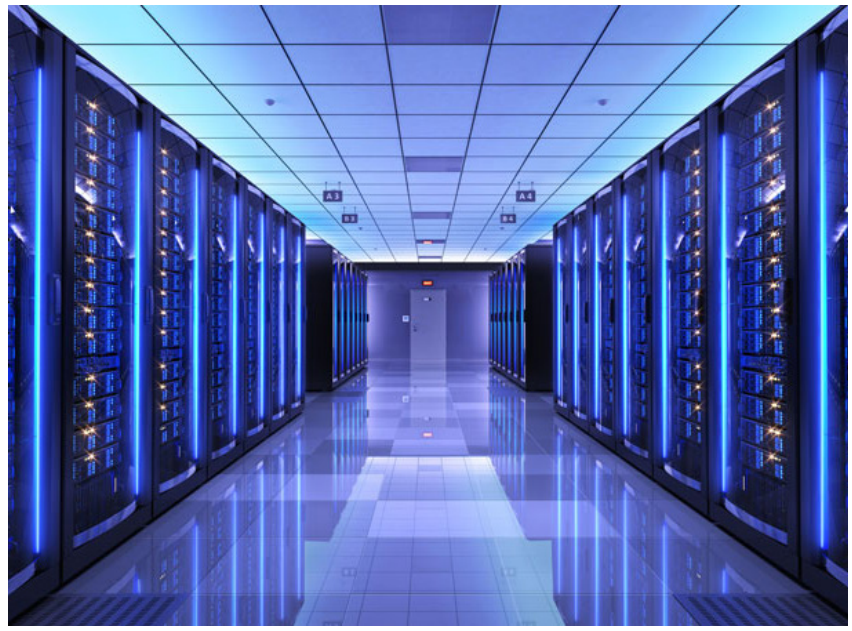
For critical services such as water supply, energy grids, transport and care systems, continuity is vital. These sectors depend heavily on communication networks to manage operations around the clock and respond to emergencies. For example, a hospital relying on digital records, diagnostic tools, and communication networks must have contingency plans in place to ensure that critical care can continue during a network outage or system failure.

The new designation of data centres demands strong resilience and preparedness against physical and digital threats, including robust strategies to mitigate cyberattacks and outages.

Network redundancy

Another key strategy for preventing or minimising damage is network redundancy. Network redundancy means creating backup systems that can take over if the primary system fails, i.e. in the case of a power outage caused by an extreme weather event. For data centres, this might involve setting up alternative pathways for data to travel in the event of a failure or having backup power supplies ready to kick in during an outage.

The principle is simple: if one part of the system goes down, another part takes over seamlessly. This helps prevent widespread disruption and ensures that critical services, such as emergency communications or hospital systems, remain online even in the worst-case scenario.



Redundancy isn't just about hardware — it's also about processes. Data centres need to have clear plans for how to respond to a failure, including how to communicate with the public and the organisations they serve. This level of preparedness is essential for ensuring that failures, when they inevitably occur, don't escalate into full-blown crises.

Why do we need to protect data centres?

Traditionally, CNI included physical infrastructure like power plants and water treatment facilities. However, as society becomes increasingly digital, the definition of CNI now extends to digital and cloud-based services, particularly data centres. These centres are crucial for storing, processing, and transmitting data that supports critical services across various sectors. As data continues to scale, resilient infrastructure becomes increasingly important to ensure uninterrupted data flow and protect against downtime, which can prove costly across many sectors.

Failures in critical national infrastructure can be caused by various factors, but two major threats stand out: cyber-attacks and extreme weather events. In both cases, it's not a matter of if but when. These threats are becoming more common, and CNI operators must be prepared to face them head-on.

The heightened protection afforded by the CNI classification, through the government's support in the event of a threat, should result in high availability and minimal downtime, which has a positive domino effect on disaster recovery and data protection.

By integrating continuity planning with robust IT infrastructure, organisations can ensure that essential services are not interrupted. This includes having backup power supplies, redundant data storage systems, and alternative communication channels in place.

The road going forward

As data centres become more central to everyday connectivity, their importance will only continue to grow. The classification of data centres as CNI should be seen as part of a broader strategy aimed at enhancing internet redundancy and resilience across the board. It will facilitate government support and funding to increase the speed of recovery when an inevitable threat hits.

By focusing on network resilience, continuity, and proactive threat management through a wider network redundancy strategy, we can protect critical national infrastructure — and the services that depend on it — from the inevitable challenges of the future. ■

Picking a winning wireless router

Erik Hoeboer, Marketing Manager for Business EMEA, Netgear

Robust and reliable digital infrastructure is the backbone of any successful business. Whether you're upgrading your existing setup or building a communications network from scratch, there are some essential considerations to ensure success.

1. Assess your business needs

Before diving into specific models or brands, consider the unique needs of your business, its size, the number of employees and the type of operations you run. Are you in one location or spread across several sites? Understanding the scale and complexity of your network will help you determine the necessary capacity and features of your routers and WiFi systems.

2. Prioritise scalability and flexibility

Businesses evolve, so when selecting WiFi systems, it's important to prioritise scalability. Choose equipment that can grow with your business, such as routers on which you can add additional modules or interfaces. A Mesh WiFi system will deliver seamless coverage across large areas and can easily be expanded by adding more nodes.

3. Security features are non-negotiable

Cyber-attacks are a constant threat, so security should be a top priority. Look for routers with advanced security features such as firewall protection, VPN support, and intrusion prevention systems (IPS). WiFi systems must support WPA3 encryption, the latest and most secure WiFi security protocol. Network segmentation, where different parts of the network are isolated, is another useful feature for protecting sensitive data. And be sure the latest security patches can be delivered to the router through automated firmware updates.

5. Evaluate performance and speed

When evaluating routers, consider their processing power, memory, and throughput capabilities. Pay attention to the WiFi standard they support. While WiFi 6 is the most widely adopted standard currently, WiFi 7 is fast on its heels and a huge number of devices and routers are being introduced to support it.

6. Futureproofing with WiFi 7

WiFi 7 deserves its own top tip; such are the performance and security benefits it delivers. WiFi7 is backwards compatible, so you can upgrade your existing WiFi5 or WiFi6 network. What WiFi7 provides are speeds of up to 30Gbps, four times faster in throughput than WiFi6E, significantly reduced latency, and better support for dense environments. If your enterprise relies on bandwidth-intensive applications like video conferencing, AR/VR or cloud computing, investing in WiFi 7-compatible equipment, which supports channels up to 320MHz wide, could be a strategic move. The standard is also helping to drive the use of an enhanced authentication mechanism which means advanced exploit prevention and AI heuristic techniques to detect and block unknown threats.

7. Interoperability and compatibility

Most enterprises will opt for a combination of routers and WiFi Access Points or a Mesh system to ensure the signal extends across multiple rooms, floors and even buildings and to multiple users. All WiFi7 access points use IEEE 802.11be Extremely High Throughput (EHT) making their data transmission interoperable. Ensure the new WiFi system is backwards compatible with your existing WiFi infrastructure to combine these access points in one network.

8. Vendor support and warranty

Choose products from reputable vendors with strong 24/7 customer support and warranties. Look for manufacturers that provide regular firmware updates to maintain security and performance.

9. Total Cost of Ownership (TCO)

While upfront costs are important, it's essential to consider TCO. To save time and money, you can manage your network remotely using a cloud management platform and select a network supplier who does not require your engineers to be fully certified and trained. Investing in energy-efficient equipment can also save your organisation money in the long run, especially if you operate a large network.

10. Watch out for overkill

If you purchase the latest cutting-edge technology to ensure your network is futureproof, consider how you will utilise all the additional features, e.g. do you need Bluetooth for localisation? Research the available WiFi systems to decide how to strike a balance between performance, features and cost.

Choosing the right WiFi system for your enterprise is a critical decision that can impact your operations for years to come. By carefully considering your needs, the emerging technologies you might want to take advantage of later, and prioritising security, you can build a robust network that supports your organisation's success. ■

PRODUCTS

For a dual-purpose business router, the Zyxel SCR 50AXE router is equipped with best-in-class threat management features, detecting and preventing common threats like ransomware and malware – with no ongoing annual costs.

The enterprise can monitor internet traffic and applications to help identify how connected devices behave on the network, and easily identify and filter internet traffic based on its country of origin (examining its IP address) to add an extra layer of protection.

Delivering superior speeds and reliability in wireless connectivity by leveraging the SCR 50AXE's WiFi 6E Tri-band radio, super low latency and speeds up to 5.4Gbps are up for grabs. The SCR 50AXE allows the business to quickly build secure connectivity (VPN tunnels) with a few simple steps making it easier for companies to extend their reach for remote working environments like work-from-home staff or teleworkers who often require secure remote access to their head office networks. Moreover, with the SCR 50AXE, it's simple to create easy secure guest access to the network by creating up to four separate networks; keeping your corporate or local networks private and secure away from the guests, while allowing them to surf the internet and enjoy the benefits of the network protection.

Finally, the SCR 50AXE leverages Zyxel's Cloud Management platform, Nebula, to streamline the process of managing not only the SCR 50AXE but all Nebula enabled Zyxel networking products in a single platform without the need for any additional software or hardware.

The **DrayTek Vigor 3912** series is a premium next generation multi-WAN router designed for the most demanding and complex networks.

The most anticipated new feature is the ability to install Linux applications with a 256GB SSD card. Boost security, management and overall efficiency with this new feature that supports Suricata, Ubuntu, VigorConnect or any compatible docker based application.

The new router brings a focus on reliability throughout its core functions, with total throughput of over 12Gbps and VPN Concentrator (500 VPN tunnels, up to 5Gbps). Featuring 12 LAN and WAN interfaces in total, 4 dedicated LAN ports and 8 switchable ports that can operate as LAN or WAN ports to fit network requirements. With up to 12Gbps of NAT

& Firewall throughput, the Vigor 3912S is suitable for the most demanding and bandwidth intensive SME applications. Each of the WAN ports on the Vigor 3912S can be grouped together to provide Load Balancing or operate as Failover or Backup WAN connections.

For multi-tenant or departmental flexibility, the Vigor 3912 series supports multiple LAN IP subnets, together with VLAN capabilities and user management, providing access to WAN resources only to the appropriate users or departments, as well as maintaining infrastructure efficiency.

Aircove is ExpressVPN's range of Wi-Fi 6 routers with built-in VPN. While any router can provide internet access, the Aircove range instantly brings all the benefits of ExpressVPN to everything on the network. If it's connected, it's protected.

Suitable for small and medium sized businesses (SMEs) Key features include WPA3 Wi-Fi security, dynamic DNS, port forwarding, and Lightway Passthrough.

Devices can be sorted into up to five groups, each with its own location and settings based on network conditions. Trackers, malicious sites, and display ads can all be blocked. Every device can be protected, including those that can't normally run a VPN.

Aircove Wi-Fi 6 routers come with dual-band Wi-Fi 6, up to 5Gb ports, impressive coverage of up to 1,600 sq. ft., and a maximum VPN speed of 180Mbps.

The **Synology RT6600ax**, a tri-band Wi-Fi 6 router, delivers ultrafast and secure wireless connectivity to the office. With easy distribution of devices between radios, RT6600ax optimises range and performance while avoiding bottlenecks.

The quad-core 1.8 GHz processor enables fast management and connection speeds, even with multiple devices connected and all features enabled.

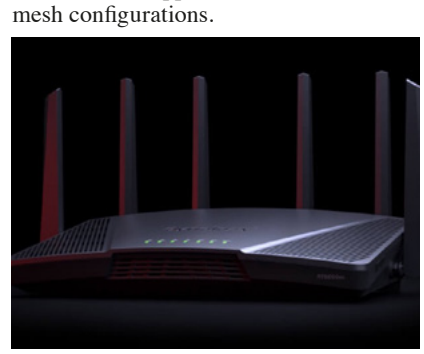
Supporting the new 5.9 GHz band, resulting in more dependable high-speed networks using clearer 80MHz and 160MHz channels, the router offers throughput up to 4x higher concurrent connections and up to 2x faster VPN server performance. Meanwhile, the 2.5GbE port, configurable for WAN or LAN use, supports superfast internet plans or high-performance devices.

With the Synology RT6600ax, the enterprise can create up to 5 separate networks and 15 Wi-Fi SSIDs to distribute devices based on their role or purpose. Networks can be isolated or set one-way access rules to limit connectivity to and from vulnerable devices. The router can be integrated into existing networks with full VLAN support in router, AP, and mesh configurations.

The **Archer AXE7800** tri-band Wi-Fi 6E router offers 7800Mbps tri-band WiFi for ultra-fast browsing, 8K streaming, online gaming, and large file downloading, all at the same time. The brand new 6GHz band brings more bandwidth, faster speeds, and near-zero latency.

Delivering 'ultra connectivity,' the AXE7800 offers one 2.5Gbps WAN/LAN port, one 1Gbps WAN/LAN port, three Gigabit LAN ports, and two USB ports to ensure max flexibility and boosted throughput. Armed with a 1.7GHz Quad-Core CPU, the small business router enables the creation of a mesh network when connected with a TP-Link OneMesh Extender for seamless coverage.

Eight antennas and beamforming ensure broad coverage deliver extensive coverage, while improved vents offer a more efficient experience.



Please meet...

Glen McCarty, consulting director, Velocity Smart Consulting

Who was your hero when you were growing up?

My father. From a very young age he taught me the value of education and personally tutored me to a high school level of education before I finished primary school; being one step ahead has always been an enormous advantage (although freaked out a lot of my teachers who had no idea what to do with me), and I credit my father fully for the man I am today, both vocationally and personally.

What was your big career break?

My promotion to transition director in the early 2000s was a seminal moment. Until that point, I had worked extensively in several industries and had been focusing on call centres (working initially as an agent, then as supervisor and manager, and eventually setting up new ones), but in my TD position, I not only gained budget line authority which raised me from being task-driven to business outcome-orientated but also moved very much into setting up IT outsourced services which not only included service desks (which was where I came from) but also all other IT services for delivery, which opened a door to my IT consulting career.

A second career break came when I met Velocity in 2013. I consider myself very lucky to have met my now business partners at such an early stage in my career, and my early role with Velocity as a consultant expanded and grew to first director and then partner. I will be forever grateful to Stuart, Anthony and Lyubo for taking me in and giving me the space and support to grow.

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

When I was 14 I attended an appointment with a careers advisor who asked me that very question. I told her that I wanted to design microchips in Silicon Valley. She looked at me blankly and handed me a leaflet on how to become a pharmacist. Clearly in the 1980s most adults had never heard of 'IT' but I knew it was the future even then.

I have no idea what happened to the careers advisor, or if she ever came to know what a microchip was, but I felt I had come full circle when I performed some consultancy work for Arm; the world's leading microchip designer. I worked for them in Cambridge rather than Silicon Valley, and I wasn't a designer, but it was close enough for me.

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

Alan Turing. He had the most brilliant mind, decades ahead of his time, and I would love to understand if he knew what his work would eventually become.

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

The saying 'work smarter not harder' is an excuse to be lazy; there is no compensation for hard work, however smart you are. If you want to succeed, put in the hard work and do it before anyone else – that's how you win.

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

My mother always thought I would make a great hairdresser, but I suspect it was mostly because she wanted free haircuts. If I hadn't moved into IT I would probably still be working in large customer service call centers which is where I started my career.

If I could do the whole thing again I would probably choose medicine and train to be a doctor as I think I would make an excellent diagnostician, as I have an encyclopedic memory and am a highly logical thinker. I suspect my bedside manner and the fact I get queasy at the sight of blood would have been an issue, but nobody is perfect.

The Rolling Stones or the Beatles?

The Stones; they're more edgy, and I think have stayed relevant longer than the Beatles. (Don't tell my father – he's a huge Beatles fan).

What would you do with £1 million?

Although I'd love to think I'd be smart and invest it wisely, I would probably spend most of it on ill-advised luxuries and treating my friends. My grandad always told me that there are no pockets in a shroud, so to enjoy money when I have it, and I've always held to that – the things we buy with money are far more important than the money itself. We always remember the smile on someone's face when they get a great gift but forget how much it cost almost immediately.

Where would you live if money was no object?

I already live in central London – I think 'money is no object' was one of the questions the estate agent asked me before I moved in.

What's the greatest technological advancement in your lifetime?

Personal computing. The move in the 1970s and 1980s away from large mainframes which were only accessible to a few large businesses to a commoditised product within the grasp of almost anyone was a seismic shift in technology. ■