JUNE 2024
networkingplus.co.uk

NETWORK+

It's the office of 2024

But not as we know it with today's wireless networks

Ian Wharton, Principle Networks, p5

Connected thinking

Smarter decision-making and improved outcomes

Amit Mehrotra, Tata Communications, p11

Questions and answers

I am an avid consumer of travel content

Kanwar Loyal, Cato Networks, p16

Dark skies on the horizon for the UK's public cloud service providers

Bringing good news for the UK's IT sector, Whitelane Research's recently published '2024 UK IT Sourcing Study' reports that IT budget spending with external providers is up; business transformation is high on the agenda; and access to resources and talent is the top driver for using external IT providers - reflecting the challenges in finding/hiring the right IT talent.

However, while satisfaction in IT sourcing relationships is up three-percentage points from 2023, cloud platform relationship satisfaction has taken a significant 11% decrease on 2023; and the 'very satisfied' category experienced a hefty drop from 21% to 11%.

"As more and more services move to the cloud, the number of people experiencing issues with the cloud will increase," explains Danel Turk, solution portfolio manager, data centers, ABB. "Implementing new solutions or systems for the first time can lead to bottlenecks in support, or for other technical issues raised during implementation – therefore some drop in the satisfaction index will occur."

It's true that starting out with public cloud is not without its challenges: "these often arise as a result of an organisation not being fully aware of the complexity of the change. That's often due to the business not undertaking a thorough evaluation and assessing the feasibility of migrating their existing IT infrastructure to a public cloud environment," adds Cathal Griffin, CRO, Asanti.

Many enterprises might find it challenging to manage and predict costs effectively with public cloud services, and unexpected expenses and complex pricing models can lead to budget overruns, says Don Valentine, vice president of sales and client services, Absoft: "additionally, the level of customisation available in public cloud environments can be restrictive, and the lack of control over infrastructure can be a significant drawback. And sometimes, the level of support provided does not always meet the enterprise's expectations."

"The pay-as-you-go approach to subscriptions taken by most providers can prove problematic in the long term-particularly for internet-based start-ups using cloud technologies who have yet to reach a stable client baseline," warns Courtney Evans, security consultant, Prism Infosec. "While it will be cheaper initially, it means that an increase in clients will lead to an increase in service costs. This is reflected in the 2024 UK IT Sourcing study, in which 27% of organisations expected nearshore growth but stated that capacity may be an issue."

"The other concern is that some businesses risk getting locked into a long-term relationship with their public cloud vendor, with little or no room for negotiation on terms and conditions, as well as concerns around control and internet connectivity. We find that this often raises the inevitable question: 'Is there is a better way to use public cloud?'" asks Griffin.

Expanded cybersecurity concerns stemming from external service providers is also a growing concern, particularly when it comes to public cloud provision.

"Relying heavily on external service providers can pose risks to enterprises, such as loss of control, insufficient support, dependency, and hidden costs," opines Valentine. "However, these risks can be mitigated through careful preparation and thorough research when selecting a provider. Asking the right questions, maintaining transparency, and ensuring consistency are key to finding the right partner. The enterprises should be looking for a partner who provides a clear framework, with detailed breakdown of services and defined service levels, the deliverables and how these are managed. Additionally, effective communication and regular audits are essential for successful cloud adoption." ■

Scottish Courts upgrades to SD-WAN with MLL Telecom

MLL Telecom has been awarded a £1.8 million three-year contract by the Scottish Courts and Tribunal Service (SCTS) for the provision of a new managed software defined wide area network (SD-WAN). The nationwide network deployment is replacing a Virgin Media solution which is due for completion by August.

MLL's managed SD-WAN solution will ensure secure and seamless connection to key administrative applications while also facilitating, for example, virtual hearings, remote juries, and livestreaming of court proceedings.

MLL's integrated mixed carrier WAN solution is being rolled out across all 54 SCTS sites including those in remote highland and islands areas. The SD-WAN includes dual rather than single circuits and the implementation of Fortinet firewalls. The network will be monitored and supported 24/7 by MLL's Network Operations Centre (NOC).

"We are delighted to be providing SCTS with a modern high quality SD-WAN solution which is aligned to their requirements for ensuring a highly efficient, secure and reliable administrative services to the judiciaries of Scotland," said James Stamford, senior project manager at MLL. "This project brings the additional challenges of connecting many older, often listed buildings along with the remoteness of certain highland and island locations. MLL is therefore working very closely with our chosen carrier partners to ensure the smooth delivery of our proposed solution within a short timeframe."

"MLL's provision of a secure, reliable and highspeed SD-WAN, matched the SCTS technical roadmap and design and will maximise our ability to support the courts and members of the public. The provision of this flexible and highly responsive service is designed to support the introduction of emerging digital capabilities that will benefit the entire justice system," said Mike Milligan, SCTS executive director of change and digital innovation. ■

North to make Port of Aberdeen smarter with £1 million contract

North has been awarded contracts to the value of £1 million by Port of Aberdeen to improve the safety, connectivity and sustainability of Scotland's largest berthing port.

The contract includes the upgrade and expansion of the port's CCTV and security systems and the deployment of a private 5G, public WiFi and IoT networks to support a range of solutions to improve operations and customer experience.

The partnership follows the transformational £420 million expansion of the port's South Harbour which represented the largest marine infrastructure project in Trust history and officially opened in September 2023.

North has designed and deployed an expansive CCTV and security system across the port's North Harbour and South Harbour. This includes integrated video management systems, automatic number plate recognition (ANPR) and access control.

Robust 4K marine-grade cameras with video analytics now provide visibility as vessels approach the port, enabling a smarter approach to security management. Upgrades to control barriers and ANPR integration has strengthened real-time event detection and traffic management, ultimately helping to better safeguard people and resources across the Port.

The 5G investment will allow Port of Aberdeen to install a high performing private 5G network, providing better connectivity at the new South Port. The 5G network will enhance communications while support applications such as drone technology, smart bollards and 5G cameras.

With 6,948 vessels utilising the port in 2023, the introduction of 5G infrastructure will advance data gathering using new technologies and importantly, support the Port of Aberdeen's goal of becoming the UK's first net zero port by 2040.

The technology will allow Port of Aberdeen to provide a safe, secure and connected environment that can further their growth and sustainability targets through their newly secured contracts with cruise operators and shipping companies that will be responsible for building renewable energy sources in the North Sea.

"Port of Aberdeen is focused on using cutting edge technology to achieve its aspirations, both in maintaining operations at the port and delivering our award-winning, industry-leading 2040 net zero strategy. The additional data available through the installation of these systems will allow our team to make more informed decisions that will continue to enable us to offer the operational excellence that our customers expect," said Jon Oakey, chief financial officer at Port of Aberdeen. "We look forward to continuing the journey with North following these awards."

The introduction of IoT solutions will allow Port of Aberdeen to monitor environmental factors through sensor technology. This will provide it with data-led insight on applications such as waste management, air quality, parking, waste, flooding and occupancy across the site.

"North is focussed on delivering stronger networks and smarter places, and we are proud to help Port of Aberdeen realise this. Its transformational expansion and mission to become Scotland's first premier net zero port will be accelerated through its prioritisation of and investment into smart solutions," said Julie Hutchison, business development manager at North. "North is uniquely placed to offer end-to-end technology solutions and we are looking forward to continuing our partnership with the Port of Aberdeen as we embark on the next phase of the project. As part of this, we will work closely with the team to explore how data and trends are accessible through the technology which can drive operational efficiencies and support the Port's digital transformation ambitions." ■

Kingsland Drinks employs new network, increases productivity

Kingsland Drinks has significantly increased productivity and is meeting its efficiency targets thanks to a new wireless network providing comprehensive, always-on, connectivity over its 18-acre site.

Following a site survey, the solution was designed and supplied by Allied Telesis and its channel partner Holker IT.

Kingsland Drinks is an employee-owned business with approximately 480 staff. It has been based in Manchester since 1995 on a hybrid indoor/outdoor site that dates from 1895 and so has some buildings with 4ft thick walls. As a 24/7 bottling production and warehousing environment, the challenge for a wireless network includes lots of fluids, cardboard, and fluctuations in temperature between areas. The company has a high reliance on its IT infrastructure, and the ability to remotely monitor, manage and trouble-shoot the network is vital. Based on Allied Telesis' Channel Blanket single-channel wireless architecture, the new network solved Kingland's problem of black-spots and unreliable coverage in its existing WiFi network, which is often a challenge in manufacturing environments.

"We work in a very agile warehouse and production environment where we need to be able to monitor and manage the continuous movement of stock. Our forklift truck drivers move stock around the site and use a hand-terminal to scan it in from location to location, but our old WiFi did not work because it had patches (of low/no coverage). Every time the signal dropped, drivers had to dismount and walk to a PC to enter the information manually, which caused delays with booking in stock, movement of stock and the booking out of goods ready for distribution to customers around the UK. It was extremely frustrating and was costing our business a lot of time and money," said Brian Polkinghorne, IT manager at Kingland Drinks. "We now have a highly resilient WLAN that covers us like a blanket with stable performance everywhere including the drivers' handheld terminals. It is perfect for our complex site with its various warehouses, production halls, and outdoor loading/unloading areas, as well as our offices and meeting rooms where we need high speed connections for laptops, phones, and other devices. Holker supported me through the entire process and it's a partnership that I know works."

Deployed within two months, the new wireless network at Kingsland Drinks comprises AWC Channel Blanket licensing for hybrid wireless architecture; Allied Telesis TQ5403 Wireless Access Points for indoor areas and Allied Telesis TQ5403e Wireless Access Points for outdoor areas and areas requiring external, directional antennas. The new network provides Kingsland Drinks with significantly improved coverage across the site, with no black spots being reported by users and monitoring software showing good coverage in all required areas. The onsite IT team are now able to use Allied Telesis' Vista Manager EX & AWC for monitoring via a visual representation of the network, allowing them to see in-depth traffic management, performance of the WLAN and the devices which were connected at any given time.

"Our Channel Blanket solution is ideal for designing and deploying wireless networks in dispersed manufacturing and warehousing locations. It solves the major problems of these environments by using only one wireless channel to create a single 'blanket' of wireless coverage, thereby eliminating interference. In this way, a manufacturing business can not only optimise network performance, but also reduce the consumption of mobile devices, ensuring uninterrupted productivity combined with an agile and fast experience," said Chris Dyke, sales director UK & Ireland at Allied Telesis. ■

EDITORIAL:
Editor: Amy Saunders
amys@kadiumpublishing.com
Designer: Ian Curtis
Sub-editor: Gerry Moynihan
Contributors: Vikram Sinha, Ben Schein, Amit Mehrotra, Brian Martin, Tamblyn Calman, Kanwar Loyal, Ian Wharton, Rob Smith,

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

Three goes green with Ericsson's AI

Three UK has hit a new milestone in its network sustainability journey with the deployment of next-generation AI-powered hardware and software solutions from Ericsson.

As part of an ongoing network modernisation initiative over the last 18 months, Three UK has worked with Ericsson on improving network energy performance thanks to a combination of industry leading energy efficient radios and the use of AI and data analytics.

Late in 2023, Three UK became one of the first major operators in the UK to deploy Ericsson's award-winning dual-band Radio 4490, which consumes less power and is 25% lighter than previous models, simplifying site access and speeding up site upgrades.

Combined with the deployment of more energy efficient radios, Three UK has also implemented a series of software features that consume less power per radio during low traffic hours. Thanks to advanced machine learning, passive cooling and power-saving features, the new generation of radio works autonomously across 4G and 5G networks to switch off radio components when not active, while having the capability to switch on again in microseconds for the next service request.

So far, the partnership between Three UK and Ericsson has resulted in an improvement of network energy efficiency of up to 70% at selected sites, all completed while improving network performance but reducing site footprint and lowering CO_2 emissions.

"Three UK's collaboration with Ericsson marks a milestone in our commitment to sustainability. We've achieved excellent improvements in energy efficiency while expanding network capabilities for our customers. We plan to take these learnings on board for future projects, ensuring that we continue to improve the environmental impact of our network," said Iain Milligan, chief network officer, Three UK.

"Together with Three UK, we are redefining the network of the future and making it both smarter and more energy efficient. To increase network availability and performance while reducing network energy consumption is a testament to the technology and expertise of our two great teams. I am both excited and proud to know that we are building a modern digital infrastructure together that brings not only superior performance for Three customers, but also helps to make the future more promising and sustainable," said Evangelia Tzifa, chief technology officer, networks & managed services, Ericsson UK and Ireland. ■

IOM installs MPLS solution

Spitfire Network Services Ltd has designed and delivered a MPLS solution for The Institute of Occupational Medicine (IOM) to significantly enhance business readiness and operational efficiency.

The Institute of Occupational Medicine is a UK leader in occupational health risk management, identified the need for greater agility and enhanced security in response to evolving customer demands for real-time monitoring and routine workplace audits, while simultaneously meeting stringent regulatory requirements.

IOM approached Spitfire to provide a comprehensive roadmap to reduce costs, improve IT management, tighten security, and deliver a market-leading product. The result is a complete connectivity solution based on the Spitfire One Network solution, delivering a 40% cost reduction through optimised network connectivity and transition to a CAPEX-free firewall model; enhanced network management and visibility with customised firewall settings and comprehensive monitoring; secure, direct connections for remote sensor gateways via Spitfire's Mobile IoT SIMs, simplifying deployment and management, crucial for expanding IOM's capabilities in cost-sensitive scenarios; and meeting stringent data security demands from public and government clientele by keeping data within a private network and utilising two-factor authentication for remote access, simplifying compliance and securing client contracts.

"Our work with The Institute of Occupational Medicine is an excellent example of our Spitfire One Network solution delivering operational excellence and cost savings while maintaining data security needs. We take care of modern-day workplace connectivity complexities and give cost effective flexibility to our clients," said Harry Bowlby, managing director, Spitfire Network Services Ltd.

"Our aim was to reassess our Wide Area Connectivity with an aim of right-sizing connectivity, reviewing security management, simplifying IT management, and providing a network that would underpin our business for years to come. Spitfire's simple yet powerful One Network solution did it all. I would have no hesitation in recommending Spitfire to anyone embarking on any level of fixed line, mobile, or cloud connectivity project," said Alan Boyd, group head of technology at the Institute of Occupational Medicine. ■

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

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

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

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

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

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

For further information visit:
www.zpesystems.com

AI could save public sector 23 million hours per week

Adopting AI tools in the public sector could save up to 23 million hours of administrative tasks each week according to a new report from Microsoft, Goldsmiths University and Symmetry.

The key findings offer significant time saving benefits for workers, especially high impact professionals like doctors and teachers, saving approximately four hours per week.

45% of public sector workers report being overwhelmed by unnecessary administrative tasks, impacting their mental health and job satisfaction.

"The incoming government needs to emphasise boosting public sector efficiency, streamlining the day-to-day work of staff and cutting down on the average of eight hours of admin each week to allow them to focus on higher value projects. Adopting AI tools to automate data collection, management and analysis, for example, is a great way to relieve the admin burden on staff and optimise their productivity," said Michael Thornton, senior director of public sector at Investigo, part of The IN Group. "When looking to implement AI tools, departments should take a smarter approach to interim versus consultancy staff. Bringing in staff with specialised AI skill sets can streamline the delivery of AI adoption projects, while also keeping costs down."

Half said that high admin workloads are compromising the quality of service they provide and limiting the time they can spend with the public and more than half said the volume of admin work is having a negative impact on their ability to actually do their job.

"AI should be central to enhancing efficiency, and investment is crucial for successful tech projects that boost productivity and growth nationwide," said Libero Rapsa, director of adesso UK. ■

Buckinghamshire Council deploys AI

Buckinghamshire Council has deployed Copilot for Microsoft 365 to improve operational efficiency.

With Microsoft's artificial intelligence (AI) tool, the council has been able to save up to 90 minutes a day on routine tasks, while also improving accessibility.

The new technology has been a game-changer in improving efficiency, making its resources stretch further. The council hopes Copilot will drive further efficiencies and transform working practices.

"Local authorities are seeing this technology as a partial silver bullet," said Peter Parfitt, head of digital at Buckinghamshire Council. "No council is swimming in cash. But we wanted to deploy Copilot, not because we had to do it, but because it was the right thing to do."

The council believes even bigger wins will follow when it employs Copilot to enhance frontline services, such as social care and housing, which account for the bulk of its budget. "If we can be more efficient, that's fantastic," said Parfitt, "But if we can trim just 1% off the cost of social care, that's where the real pressures are."

According to Marie White, head of customer experience at Buckinghamshire Council, the AI Copilot tool has enabled the council to improve its quality and complaints procedures, as well as streamline response drafting and call summarising. ■

180 Oxford public service sites connected

Utilising its high-capacity fibre network and solutions, and aggregating local fibre networks from Openreach, Virgin Media Business and Gigaclear, Neos Networks has now provided full fibre connectivity to 180 out of 193 public buildings contracted for Oxfordshire County Council under the GigaHubs project.

The initial project, delivered by the end of 2023, saw 175 GP practices, schools, libraries and community centres connected to full fibre. However once deployed, Neos was engaged to extend connectivity to a further 18 rural sites in the county that were previously only connected via copper-based services. The fibre networks are now enabling faster provisioning of public services at a fraction of the cost due to Neos' network rationalisation of services and ability to access an extremely competitive supply chain. ■

AlphaSights picks LogRhythm for SIEM platform

LogRhythm has been selected by AlphaSights to deploy its Axon cloud-native SaaS security and information event management (SIEM) platform.

"We are excited to collaborate with LogRhythm," said Kelvin Leung, senior technical operations manager at AlphaSights, when reflecting on the deal. "We were looking for a tool that would allow us to secure our environment and a company that would partner with us on that journey. LogRhythm Axon and their team met those requirements."

"Axon provides AlphaSights with a powerful threat hunting tool delivered with flexibility and an easy-to-use interface. It empowers security teams and gives them a model that is built to scale," Kev Eley, VP UKI & Europe at LogRhythm. ■

BT Group implements 'cell sleep' across EE mobile sites

BT Group has implemented energy-saving 'cell sleep' technology across its EE mobile sites nationwide, following successful trials in each of the UK's home nations.

'Cell sleep' software works by putting certain 4G LTE capacity carriers to sleep when the capacity is not needed, based on predicted periods of low traffic which have been established for each site through machine learning.

The system then automatically wakes up during busy periods and is also configured to react to unexpected surges which might occur during scheduled sleep modes – in which event, the carriers wake up within a matter of seconds to serve demand without any interruption to customers.

An even lower power state, 'deep sleep', can also be activated if required, for example during overnight periods of extremely low demand.

Both the 'cell sleep' and 'deep sleep' functionality is provided by the respective RAN equipment supplier on each of EE's sites. BT Group's site data is used to inform the statistical algorithms which then autonomously inform the functionality.

"There is huge potential for energy savings across our networks by dynamically matching power consumption against network usage. The optimisation and roll-out of cell sleep technology to over 19,500 sites across the UK is a significant milestone in achieving this, and an important development in countering the massive growth in data consumption we're seeing across our networks," said Greg McCall, chief networks officer, BT Group.

It is expected that the technology will deliver energy savings of up to 2KWh per site per day, or 4.5 million KWh per year across EE's estate, reducing BT Group's demand on the local Grid.

As the largest provider of fixed-line broadband and mobile services in the UK, BT Group's networks account for around 89% of its total energy consumption. As such, increasing network energy-efficiency is integral to the group's ambition to become a net zero carbon emissions business by the end of March 2031. ■

Word on the web...

Navigating towards sustainable IT: a practical path

Rob Smith, CTO, Creative ITC

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

The future of the wireless network: it's the office, but not as we know it

Ian Wharton, technical architect, Principle Networks

The office as we know it no longer exists. The modern workspace has become a multifunctional hub, blending work with client interactions and social events and at its core is a fast, reliable and secure wireless network.

However, the shift to the modern office isn't as simple as updating old systems. It's a comprehensive overhaul which demands a fundamental reimagining of existing infrastructure and all that underpins it. The density of traffic travelling through today's networks is no longer akin to those of the past, which means on-premise Local Area Networks (LAN) and clunky, standard guest WiFi connections are no longer fit for purpose.

Why is there a desire for change?

For many organisations, the office wireless network hasn't been a priority. Incorporating guest WiFi into existing infrastructure was considered enough. Fast-forward ten years, those same businesses are attempting to transition to the cloud and using the same network connection to host multiple users. Almost immediately, they found it had limited bandwidth and couldn't cope with the density of devices trying to connect.

This approach is hindering innovation. A recent survey of over 500 IT decision-makers found that organisations spent an estimated 40% of their annual IT budget on maintaining legacy technology. Furthermore, 69% of respondents acknowledged that technical debt is hindering their ability to innovate.

There has been a shift in what organisations need, want, and expect from a wireless network. Why? Hybrid working is one reason, but another is the fact consumer brands have transformed our experiences as technology users.

Hybrid working has made it possible for us to use public spaces such as coffee shops as a place to work. They offer instant, fast, and secure internet access, which can be more appealing than going into the office. It has highlighted flexibility as the cornerstone of modern network infrastructure. Organisations need to match this with a network that seamlessly adapts to the dynamic nature of the current working environment. When a new starter joins your organisation, they or any visitors must connect to your network. It's a benchmark of a modern business.

Transitioning to the future

The Department for Science, Innovation and Technology's (DSIT) Wireless Infrastructure Strategy details the government's plan to deliver world-class wireless infrastructure across the UK by 2030. But how do we get there?

Organisations need to move away from simplistic, standard networks and embrace more secure, user-friendly and cloud-based infrastructure that reflects the needs of the modern office. This shift should be a necessity and is driven by several key factors.

Firstly, modern security concerns require a more robust network. Standard solutions often lack the required security measures to safeguard against a potential cyber-attack. Any attack could prove extremely costly, whether financially or reputationally. The rise of hybrid working and the handling of sensitive data across dispersed environments means security protocols are imperative to maintain data integrity and minimise the threat of unauthorised access to a network.

Secondly, scalability and flexibility are central to organisations' operations. Traditional networks can struggle to adapt to the evolving needs of multiple devices and a fluctuating workforce. Cloud-based infrastructure provides the required adaptability, scaling up or down to meet the changing needs without compromising network performance. They also ensure a hassle-free connection across various devices and locations, driving productivity and collaboration, and delivering a user experience that surpasses physical boundaries.

Optimised performance is another crucial factor when it comes to upgrading wireless networks. Cloud-based infrastructure can manage dense environments well. It ensures speed, latency, and reliability are not compromised, no matter how busy the network is. Transitioning to the cloud also facilitates ongoing innovation. It supports new technologies and enables the deployment of updated security measures. This is essential to businesses trying to stay ahead in a competitive marketplace.

The office we once knew no longer exists

IT decision-makers can mould what the office of the future looks like.

By prioritising network upgrades and designing a network infrastructure that aligns with their business objectives, they will be able to create a modern workspace that enables their business to thrive.

It's about implementing networks that facilitate change rather than hinder it. The need to embrace future-ready infrastructure is imperative.

It's long past time to overhaul legacy systems, transition to the cloud and build a secure, reliable and scalable network that drives success. ■

Indosat Pioneering AI Development in Indonesia through Democratization and Innovation

Vikram Sinha, president director and chief executive officer, Indosat Ooredoo Hutchison

When we started our journey in the merger to form Indosat Ooredoo Hutchison some 28 months ago, we agreed that it would be good for our customers, good for our country, and good for our employees. Today, the numbers speak for themselves. Coverage is up, consistency and experience are improved, and we truly have benefited Indonesia as a whole.

It's become clear in a post-COVID world that the telecommunications sector plays a vital role in the digital economy and has a significant impact on GDP growth. In the last two years, the industry has been growing at 5%, but I believe it has the potential to expand by 8-10%.

AI is democratising innovation at a phenomenal pace. Back in 2008, Apple launched their Apple Store with just 500 applications, and in 2012, Google did the same, but with 16,000. ChatGPT, meanwhile, launched last year with 3 million – imagine the democratisation and innovation to come in the next few years!

We believe that AI is linked to our larger purpose of empowering every Indonesian and has the potential to help GDP grow faster.

Growth mindset

Looking to the future and our goals, we have built ourselves on three pillars.

The first pillar is becoming an AI-native telco. Embedding AI in our core business starts with virtualisation around customer offerings, managing our CapEx and productivity, into procurement, HR, sales and marketing – every business function. The second pillar is to become an AI-native techco, which talks about creating new businesses; our focus will be content like sovereign cloud security, and we are focusing on verticals like financial institutions and energy companies. The third pillar is in creating an AI nation shaper; we are working on our AI Centre of Excellence and are also putting disproportionate focus on human capital development. Technology without investment is destined to fail. If we don't invest in human capital, how can we create skills?

When we talk about moving from telco to techco, this reflects the market and the new business opportunities we're seeing. Today, banks are approaching us for help with sovereign cloud and sovereign infrastructure – the focus is not on connectivity anymore. They want to know how we can help solve money laundering or Know Your Customer (KYC) problems.

And it's not just urban centres and big city users - one of the things which is often underestimated is how even the most rural of communities are adapting to technology. Farmers in Indonesia are using AI to increase their crop yields, for example, despite their many years of knowledge. For the country to advance, it must use technology as an enabler, and democratise not only on tier one and tier two, but also on the most rural.

With our growth mindset, we want to double our EBITDA to $3 billion by 2028. There is so much opportunity in Indonesia - 21 million new customers coming from rural regions are first time internet users. There are very few countries in the world like it, and with growing ARPU and GDP spend, whichever way you look at it, GB per user is under indexed.

There's a clear opportunity to enhance ARPU from its current $2.8 to $4-5. By offering our customers data and connectivity, we're helping people achieve productive work at a fraction of a cost. Delivering a 'marvellous experience' is one of our priorities, and rationalising our prices to remain sustainable is part of that.

FTTH home broadband is another growth engine in Indonesia. Only 15% of homes today are connected, but there are 80 million homes in the country. FTTH home broadband connectivity will expand to 30-35% in the next 3-4 years.

Each year, we spend some $700 million. Part of planning for the future and evolving from telco to AI-native techco is to talk about how we're personalising things, how we're managing CapEx in a more productive manner. Our CapEx intensity today is close to 24% of revenue, but going forwards, we're not looking to save money – we're in a growth mindset. We want to spend the same and make it more productive; and AI is going to help us in that.

Intelligent networks

Everyone is so excited about AI, but first, we must establish the horizontal platform. If you don't get the basic steps right, you will not be able to scale things up. It took us a year to do with our partners, but we're there now with our unified data platform on Google Cloud. On top of that horizontal platform, we must also have vertical expertise.

Incorporating AI into the network helps us bring our operating maturity level up a notch. To do this, we must understand our ecosystem in totality, so that we can exponentially grow our customer base.

When you look at AI, you start with efficiency and productivity, but you don't stop there if you really want to unlock the full potential of AI. It is so important to look at growth. Growth will only happen when the leadership teams spend time on growth. In our case, we grew our revenues by 15% year-on-year last quarter, but EBITDA was up just 1% - this shows just how big an impact AI is having on driving core growth via ARPU increase.

We are seeing new opportunities that never existed before AI cloud, and things are moving very fast. We must be there when opportunity knocks.

One of the first successes which we saw was on our capacity planning – if our capacity is over places where nobody is using it, it's not generating revenue. Previously, this planning was done manually, and we'd achieve 75-80% accuracy. With AI, we have gotten close to 98%. We spend $300-400 million on capacity, so using AI for planning in the first quarter has saved us almost $10 million.

Another success where AI has really helped us is home broadband. Today, we've changed our approach to a building-by-building case; our platform analyses socioeconomic data, and we deliver FTTH accordingly. With this application, we've increased uptake from 13-14% to 15-16% in just six months.

Harmonising collaboration

Ensure effective collaboration and harmony among the various level partners in our ecosystem and considering potential conflicts that may arise is complex.

In my ecosystem, I have 960 vendors - out of that we have classified 66 as partners, of whom 22 are strategic partners. There is a clear difference between vendor, partner, and strategic partner. First, we must align the culture within the organisation – I don't call my partners 'vendors,' I call them partner or strategic partner. It's more than just a name; it's an operating model that starts with me and my team, how we behave, how we talk, and how we operate.

There are difficult times of course, when you work with sovereign cloud. When working with a partner, sometimes there are conflicting messages, and the only solution is to be more open and transparent.

What I ask of the big tech companies is that they align their values first. Our actions must be good for our country, and fair for the partners on the ground, including us. Previously, there has been a trend where the big tech companies will say: "no, this cannot be done." It's not an easy thing, and we must work on a case-by-case basis to ensure our principles are aligned. We want to make money with our partner, not from our partner.

History shows us that telcos like us have been very inward looking. We used to complain about OTT operators to the regulator, but the reality was, the issues were more self-inflicted. We were not building trust with our customer, and we were not open.

For me personally COVID-19 was a pivot moment for the ecosystem - but AI is a much bigger pivot moment. Today, we must bring that learning mindset, let go of old ideas, and embrace the new. ■

Securing the election of a generation

With the 4th July election almost upon us, threats to democracy lie in wait. From ransomware to AI, which are the most significant dangers to a fair and open election – and how will they be addressed?

As the UK heads towards the polls on – auspiciously – 4th July, the cyber threat landscape has become front and centre to those who seek to attack and expose weaknesses and those tasked with defending and ensuring the integrity of our democracy.

"Bad actors may use combinations of simple and sophisticated methods, including social engineering, phishing and malware approaches with the intent to gain unauthorised access to online services. If successful, this may lead to the spreading of false information and the possibility of gaining a strong foothold to execute potentially more disruptive cyber-attacks," says Christian Reilly, field CTO EMEA, Cloudflare.

In the most exciting General Election of a generation, the chips are down, and the pressure is well and truly on.

The cyber threat

Daniel Schwalbe, CISO & VP IT, DomainTools reports the welcome news that the UK's Election System is largely immune to network-based attacks or attempts to manipulate vote counts electronically, as all governmental elections are still conducted entirely using traditional paper ballots.

"Elections in the UK rely on a mixture of citizen volunteers and government employees to manage voting locations and to conduct counts after the polls have closed," reports Schwalbe. "Vote counts are done by hand, under the oversight of independent observers and party representatives. This system creates checks and balances that makes vote count manipulation at scale impractical."

Back in 2020, President Donald Trump infamously claimed that the 2020 United States presidential election was rigged by means of tampered voting machines, electoral fraud, and an international communist conspiracy. However, experts like Schwalbe assert that this kind of tampering is rare across the developed world; much larger threats exist with the power to truly sway an election.

Political interference, whether domestic actors engaging in unethical practices such as voter suppression or the dissemination of false information; or foreign governments and/or entities using cyber-attacks or heavily funding specific parties, are a particular concern this year, especially with ongoing geopolitical tensions and the threat of World War III.

"The UK government has previously indicated that hostile nation states including China Iran, Russia and North Korea offer a significant threat to election integrity due to their advanced cyber warfare capabilities, however, when considering the threat landscape and how to defend against it, there should also be consideration given to the potential threat from organised crime groups and 'lone wolf' hackers whose motivations may be different but may still cause disruption if their attacks are successful," adds Reilly.

Cybersecurity threats will be another major problem. Attackers could target

Guiding political candidates

Ahead of the local elections, European Parliament elections and General Election taking place over the 12 months from May 2024, the National Cyber Security Centre (NCSC) has published an updated guide on cyber-attacks that target election candidates or political party they represent.

The publication includes guidance on identity and access management policies; enhancing website security; prevent digital impersonation; educating constituents about misinformation; and preparing for ransomware and deepfake attacks.

"We work closely on an ongoing basis with the local authorities who have responsibility for the running of the elections, as well as the Electoral Commission, however we are also conscious of the impacts of any potential cyber-attack on the candidates themselves, or the parties they represent. It is vital that we guard against the potential for an attack at any point within the electoral cycle, and that we continue to raise awareness amongst those taking part in elections of the importance of strengthening the security and resilience of the ICT systems and devices they are using," states NCSC Director Richard Browne.

election infrastructure, such as voter registration databases and election management systems, disrupting the election process, stealing sensitive data, and manipulating results. Meanwhile, ransomware attacks could lock election officials out of crucial systems or data, demanding a ransom to restore access, which could cause significant delays and disruptions.

"The UK's National Cyber Security Centre (NCSC) has repeatedly stated that, in their opinion, ransomware is the largest single threat facing the public and private sector alike," says Reilly. "Therefore, we should consider the possibility and impact of a ransomware event to be a strong one for the forthcoming elections. Recently, a number of local authorities in the UK have been subject to successful ransomware attacks which have affected various critical services including voter registration and validation."

"Ransomware is a considerable threat to the upcoming UK general election, largely due to the evolving sophistication of cyberattacks, which are increasingly powered by AI," agrees Srinivas Mukkamala, AI leader and CPO, Ivanti. "Generative AI technologies might amplify cybersecurity risks by making sophisticated attacks more accessible. The potential attacks could range from those targeting essential infrastructure like voter databases and result reporting systems to those affecting a wide array of individuals including MPs and civil servants, all aimed at creating chaos. The implications of such disruptions could be severe."

Richard Hummel, threat intelligence lead at NETSCOUT, warns that the rise of politically motivated DDoS hacktivism is a major concern: "The months leading up to the UK general election have seen a shift in the global cybersecurity landscape towards a trend of politically motivated DDoS attacks. An unprecedented number of attacks were launched by hacktivist groups such as NoName057(016) and Anonymous Sudan, targeting opponents for geopolitical causes, as well as waging political and religious war against any nation or official that stands in the way of their ideals. In terms of election-related DDoS attacks, cybercriminals can impede voting processes in several ways, such as overwhelming voter information and registration sites, disrupting campaign websites and targeting official results reporting. The outcomes of these votes can also lead to an uptick in cyberattacks. For example, Poland experienced a surge in DDoS attack activity at the hands of NoName057(016) in late December 2023 after the swearing-in of its new Prime Minister, Donald Tusk, who expressed the nation's support for Ukraine, which stands in direct opposition to the threat actors' interests."

AI: influencing an election

For the first time in UK history, AI may well play a significant role in deciding the outcome of the General Election, possibly influencing voters or even interfering with results.

"AI tools can be used to interfere with the UK's upcoming General Election in several ways such as disinformation campaigns with deepfakes and social media manipulations, bots and fake accounts, cyber-attacks on voting infrastructure by assisting cybercriminals in hacking by exploiting vulnerabilities in the infrastructure and DDoS attacks to disable websites and online services related to the election such as voter registration portals or election result reporting sites," reports Reilly.

Industry experts warn that AI can be used to create and spread false information rapidly. Deepfakes, fake news, and misleading social media posts can sway public opinion or create confusion among voters.

"The biggest opportunity for hostile actors to attempt to influence the election would likely be through disinformation campaigns using social media and other electronic communications channels such as Telegram, for example," asserts Schwalbe.

"While there's currently no evidence that AI can directly disrupt the electoral process, its role in influencing public opinion through misinformation is a significant concern," shares Mukkamala. "For instance, a BBC investigation revealed that young voters in critical electoral regions are being targeted with AI-generated fake videos. Given this, it's vital for voters to be aware of and carefully consider potential shortcomings of AI, such as unintended bias, erroneous baseline data, and/or ethical considerations."

The general public should be aware that AI algorithms can analyse vast amounts of data to create targeted political advertisements, which can be tailored to specific groups or individuals based on their online behaviour, potentially influencing voting decisions. Moreover, automated bots can amplify political messages or disrupt online discourse by spamming, trolling, or manipulating social media trends. Media manipulation is another pressing concern where AI tools can generate convincing fake content, making it harder for voters to distinguish between genuine and false information.

"Media has influenced people's political opinions since the print press was born, but we have seen a huge increase in polarisation and partisanship since the advent of the internet and especially social media," says John Smith, Veracode EMEA CTO. "The danger comes when people use social media as their news source. Many platforms are rife with misinformation and malicious actors use targeted ads to skew voters' opinions in one or another. Influencing votes and misleading voters has become even easier with generative AI being not only very widespread, but also so easy to use to create fake audio and video clips of prominent political figures."

Indeed, "fears around AI interfering with the upcoming election have only grown in recent months as political figures, including Prime Minister Rishi Sunak, have had their identities spoofed in deepfake videos or audio clips, falsely portraying them as saying politically damaging things," says Stuart Wells, chief technology officer, Jumio. "As deepfakes have caused havoc during other elections, UK electoral candidates have since been warned that anyone involved in the election process could be targeted by online disinformation and offered guidance on reducing the likelihood of a deepfake attack. It's clear that deepfakes and disinformation have the power to undermine trust in our democratic system."

In the immediate term, organisations providing media platforms must remain vigilant and proactive, working in tandem with government efforts to safeguard the electoral process from the misuse of AI-generated content.

"They can also look to collaborate with vendors who offer state-of-the-art deepfake detection pipelines that can detect and prevent deepfake-based disinformation," adds Wells.

Maintaining democracy

The integrity of the UK's general election is under threat and requires a coordinated

Daniel Schwalbe

Christian Reilly

effort from government agencies, election officials, cybersecurity experts, and the general public to ensure a secure, fair, and transparent electoral process.

The UK's IT sector can play a crucial role in supporting elections, leveraging their expertise to ensure the process is efficient, transparent, and secure. From protecting election infrastructure and monitoring threats to maintaining systems and software and providing infrastructure support through the cloud, there is a great deal to do in a very limited time, given the short notice provided.

"The UK's IT sector is pivotal in enhancing election security, from providing essential IT infrastructure for ballot processing to safeguarding critical data. With the rise of AI and associated risks, there is a growing need for robust IT support," says Mukkamala. "By establishing clear guidelines and a flexible regulatory framework, the IT sector can empower the public sector to use AI responsibly, maximising its benefits while ensuring electoral integrity."

"Ahead of the election, government organisations, service providers, and enterprises should be prepared for DDoS attacks to increase significantly," asserts Hummel. "This necessitates organisations implementing industry best current practices (BCPs) in conjunction with ensuring their DDoS protection solutions are up to standard and ready to take on the threat that hacktivist groups pose."

As an industry, the UK's IT sector has a collective opportunity to continue to guard and protect the democratic elections by combining technologies, skills and experiences to help defend, identify and fact check systems and sources that are used to provide critical online services throughout the timeline of the election, says Reilly. Education and targeted training, specifically to help combat the threat of social engineering, or phishing, against candidates, prospective candidates and those involved in political campaigning can significantly reduce the risk of an attack being successful.

Additionally, while AI has the capability to interfere with elections, installing proactive measures can make all the difference to its impact. Governments can establish regulations to monitor and control the use of AI in political campaigns and adverts, while platforms can improve transparency around political ads and the sources of information. Implementing robust cybersecurity measures and using AI to detect and counteract malicious activities.

"It is important to put in place mitigation measures starting with audits, fast-checking and identification, and using AI to increase the level of protection across all security areas, ranging from application security to email security and a robust Zero Trust platform," says Reilly. "This includes creating customised protection for every customer for API or email security, or using our huge amount of attack data to train models to detect application attacks that haven't been discovered yet."

The UK's IT sector possesses the tools and expertise necessary to support and enhance the election process, fulfilling a critical role in safeguarding democracy, ensuring fair access to voting, and protecting the integrity of electoral outcomes. Some believe it is their moral duty to contribute to these efforts – and may even come under CSR commitments promoting good governance and ethical practices - reflecting a broader commitment to societal good and national security.

"It is in the best interest of the UK and our democracy for tech companies to openly share threat intelligence and to provide services for protecting and mitigating risk free at the point of use for government organisations involved in the election process," asserts Reilly.

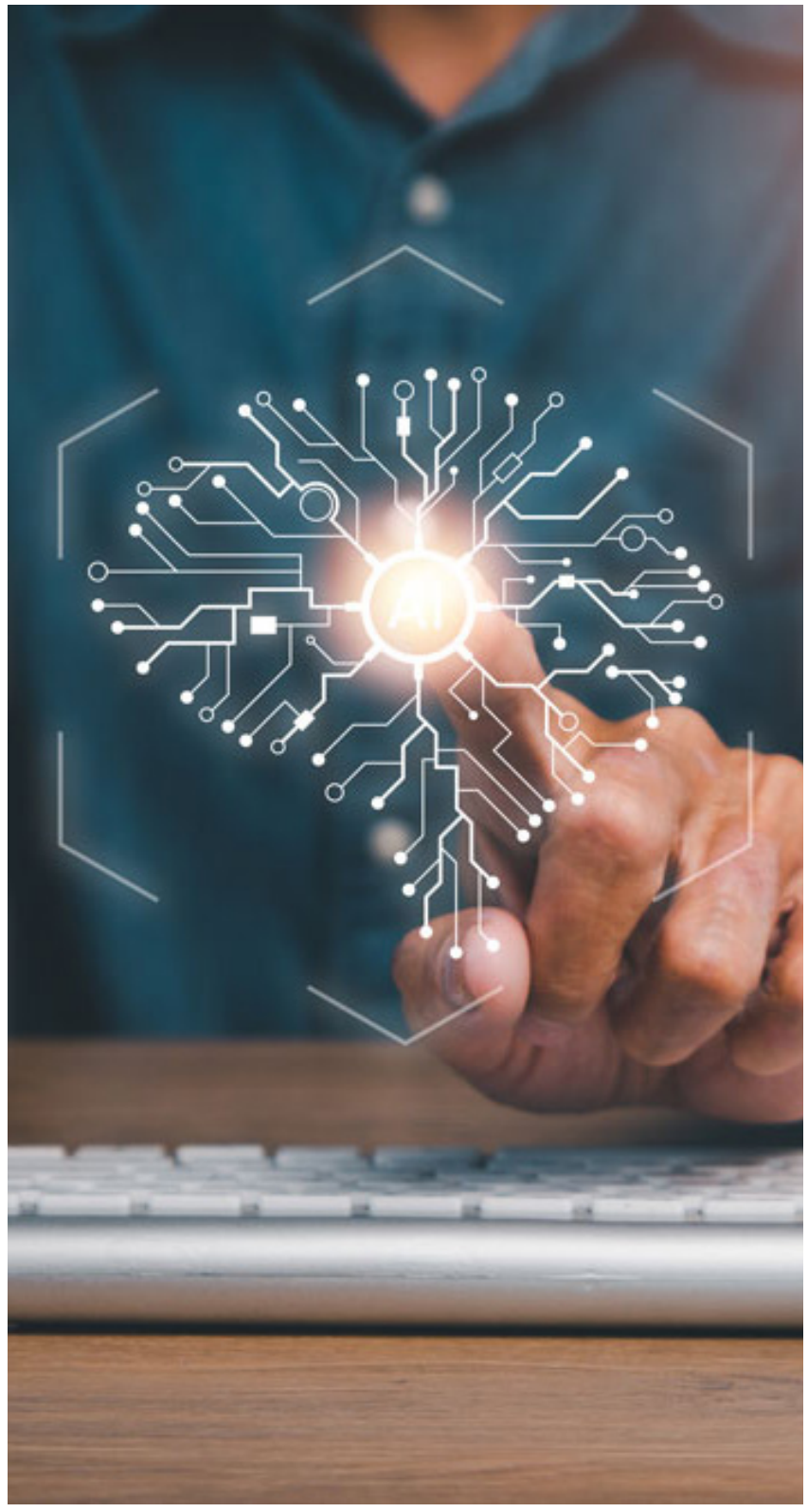
Future voting systems

As threats evolve, the networks supporting the elections and voting infrastructure must too evolve to become more sophisticated, secure, and resilient.

Built on networks that prioritise security, resilience, and user accessibility, future voting networks are expected to incorporate blockchain, AI, and cloud computing. Adhering to stringent cybersecurity measures and open standards, these networks will support robust, transparent, and trustworthy electoral processes, to ensure that every vote is counted accurately and securely while maintaining the public's confidence in the integrity of the electoral system.

Reilly believes that future networks will ensure that the critical services that are delivered across them are increasingly protected against being overloaded, taken off-line completely, or compromised by the types of attacks that allow malware and ransomware to infiltrate an organisation.

"Providing built-in resiliency, where voting systems are distributed across multiple physical locations, will also be a key feature of future networks ensuring that even if an attack is initially successful, there is sufficient redundancy within the network to ensure continuity of service," says Reilly. ■



Beware the deepfakes

Jumio's '2024 Online Identity Study' reveals fear and concern among the British public on the political influence AI and deepfakes may have on the General Election set for 4 July.

The study examined the views of more than 2,000 adults from across the UK. The results suggest that 60% of Britons are worried about the potential for AI and deepfakes to influence upcoming elections, and only 33% think they could easily spot a deepfake of a politician.

The data also reveals a changing relationship between the public and online media. 64% of Britons are more sceptical of the political content they see online, compared to the last election in 2019.

The arrival of generative AI and deepfakes has not significantly changed Britons' trust in traditional news — 56% of Britons said nothing has changed in their level of trust in print or broadcast news, while 25% said they trust print and broadcast news less. However, four in 10 Britons say they trust what they see on social media less than they did before the arrival of generative AI.

As such, the populace has an appetite for increased regulation of AI: over half (53%) think UK laws around AI don't go far enough, while only 26% trust the government's ability to regulate the technology.

"With the UK heading to the polls, it's vital that we have an open conversation about the role that generative AI and deepfakes could play in the national debate," said Stuart Wells, Jumio's chief technology officer. "The public's lack of confidence in their ability to identify fraudulent content online is concerning, and more needs to be done to educate consumers on how to spot deepfaked content, and how to report it should they see it. Online organisations also have a responsibility and should implement multimodal, biometric-based verification systems or other deepfake detection mechanisms to keep deepfakes from influencing voters in the days leading up to the election and beyond."

Data never sleeps… AI and the enterprise network in focus

Ben Schein, senior vice president of product, Domo

Understanding the profound impact of the ever-expanding internet population and the evolving ways in which people engage with the digital world is pivotal. According to Domo's latest Data Never Sleeps (DNS) report, which offers a big-picture glimpse into the immense volume of data generated on the internet every minute, as of November 2023, 5.2 billion people around the globe are on the internet - around 64% of the entire world population.

Notably, the frequency of internet usage is on the rise, with 6.3 million Google searches occurring every minute. This is a 215% increase on searches compared to a decade ago when Domo first launched its annual Data Never Sleeps report. This surge in internet activity is mirrored in the data landscape, with predicted global data creation reaching 120 zettabytes in 2023 and predicted to grow to 181 zettabytes by 2025.

However, beyond sending emails, browsing recipes, and shopping online, the influence of data extends far beyond consumer dynamics and the evolving use of internet and user behaviour is particularly relevant to enterprise networks.

In this transformative era, data has transcended its role in shaping individual routines to become the driving force behind the operations of businesses and industries. This evolution is particularly evident in the realm of enterprise networks and networking technologies. The significance of data is not confined to individual preferences but extends to the fabric of how organisations operate, innovate, and leverage connectivity, marking a pivotal change in the broader spectrum of internet utilisation.

AI, cybersecurity and enterprise networks

Unsurprisingly, as internet use has increased, so has the volume of crime. Attacks by cybercriminals are becoming more and more sophisticated and complex. Showing this, since the inaugural Domo Data Never Sleeps research was conducted in 2013, 2 million emails were sent every minute; this figure climbed to a staggering 241 million in 2023. Intertwined with this, is also the fact that there were 30 Distributed Denial of Service (DDoS) attacks launched by cybercriminals each minute in 2023.

The landscape of cyber attacks is vast and costly - with UK cybercrime costing the economy an estimated £27 billion per year. The importance of heightened awareness and implementing robust protective measures to prevent potential cyberattacks and breaches on businesses and individuals has never been more vital.

An additional dynamic at play that is important to understanding the broader cyber landscape is the rapid rise in the prominence and adoption of AI - marked by its use among ordinary people. Showing this, Domo's data reveals that ChatGPT users sent 6,944 prompts per minute in 2023. Meaning that a staggering 416,640 prompts were sent every hour and over 9.9 million every day.

In this dynamic landscape, the rise of Artificial Intelligence (AI) emerges as a double-edged sword. On one hand, AI offers transformative benefits and productivity gains for enterprise networks. It empowers organisations to proactively address network issues, enhance reliability, and optimise performance. AI-driven user behaviour analytics ensure a secure and efficient user experience, identifying potential issues and security threats. Network automation streamlines routine tasks, allowing IT teams to focus on strategic aspects of network management. Similarly, self-healing networks, powered by AI, automatically identify and rectify issues, minimising downtime and optimising performance - a game-changer for operational efficiency.

However, the same AI capabilities that benefit enterprise networks can be harnessed for cybercrime. AI becomes a potent tool for malicious actors, enabling stealthy navigation through networks, automating, and scaling attacks, and adapting to counteract security measures. The key lies in navigating this technological paradox — leveraging AI for innovation while fortifying defences against potential misuse.

Beyond prioritising advanced digital security measures, predicting the precise evolution of internet use over the next year will also be key, as companies begin to anticipate technological and societal shifts. As organisations collect increasing amounts of data, ensuring its security becomes paramount. AI plays a crucial role in providing secure solutions by automating processes like records management and ensuring compliance with industry protocols. For customers, AI aids in fraud detection by analysing records and transactions, learning normal behaviours, and identifying outliers.

In the realm of security and compliance, AI holds immense potential. It can detect intrusion and malware, respond to data breaches, predict user behaviour, and prevent phishing. While AI promises increased security and compliance, ethical considerations are paramount. The evolving field of AI ethics raises concerns about its potential misuse for security breaches and exposure of private information.

AI's future evolution in the cybersecurity domain is promising. As cyber-attacks and data breaches pose significant risks, AI will continue to automate processes, enhance fraud detection, and fortify security measures. Industries heavily reliant on personal data, such as healthcare and finance, are expected to experience a surge in AI adoption, further amplifying compliance and security measures across sectors. ■

Embracing connected thinking: smarter decision-making and improved outcomes

Amit Mehrotra, vice president and head of UK & Ireland, Tata Communications

The last few years have seen organisations and industries make impressive progress towards a hyperconnected world; one where billions of interconnected things communicate seamlessly with each other, people, and systems.

As a result, the IoT market has seen impressive growth, driven by the rise of connected devices and the increasing demand for smart solutions by organisations in every industry. Businesses are keen to take advantage of the array of potential benefits, particularly those operating in highly competitive industries.

From gathering behavioural data on customer preferences for personalised products and services to real-time insights for predictive maintenance, there are a wealth of benefits to be found. By leveraging IoT technology, companies can stand out from their peers, as well as set new standards for efficiency, safety, and customer satisfaction.

According to projections by IDC, IoT ecosystem investments are expected to surpass $1 trillion in 2026. Nearly 60% of organisations are already engaged in IoT projects, according to Accenture. But that doesn't mean they're all getting it right: deploying and managing an IoT solution can present significant challenges, and many of these projects are not delivering the promised benefits.

There are several common obstacles that prevent companies from harnessing the power of IoT, but by understanding, approaching and addressing these head on, every organisation can ensure a smooth transition and long-term success.

Setting the foundations

The first challenge to overcome is connectivity – without this, any IoT project will struggle to get off the ground.

Strong connectivity is all about ensuring that different devices spread across multiple regions can be connected in the most optimal and cost-effective manner. When organisations are connected to a large number of vendors, OEMs, and service providers, ensuring interoperability between different devices, including legacy assets, is a priority.

For example, a manufacturer operating worldwide may need to connect thousands of sensors, machines, and vehicles across different plants, warehouses, and transport routes. A retailer may need to link their inventory, point-of-sale, and online systems across different stores and regions. City councils may want to integrate their traffic, parking, lighting, and waste management services across different areas and platforms. All of these solutions help companies be more efficient, cost-effective and sustainable.

To achieve these goals, organisations need a connectivity solution that can support their specific requirements, scale with their needs, and adapt to their changing environments. This is where partnering with a trusted service provider can make a difference. With platform-based IoT offerings, service providers can help organisations streamline their connectivity, customise their solutions, and manage their devices and data more effectively.

"There are several common obstacles that prevent companies from harnessing the power of IoT, but by understanding, approaching and addressing these head on, every organisation can ensure a smooth transition and long-term success."

Safeguarding against threats

IoT solutions generate and transmit massive amounts of data, which can expose them to cyberattacks, breaches, or theft. Moreover, IoT devices can increase the attack surface for cyber threats, as they can be compromised or exploited by hackers to access sensitive information or disrupt operations.

For instance, a cyberattack on a smart grid could cause a power outage, affecting millions of customers and businesses. A breach of a smart healthcare system could expose confidential patient records, violating privacy and compliance regulations. A theft of a smart vehicle could enable criminals to track its location, endangering the driver and the cargo.

But in many IoT use cases, these endpoints are not adequately secured, making the whole ecosystem vulnerable. Securing these different devices across the entire IoT estate is a big challenge. So is leveraging the vast amount of data generated to make more informed business decisions.

To mitigate risk in an ever-evolving threat landscape, it's critical that businesses create a broad cybersecurity strategy that covers their devices, networks, and data. This means implementing robust encryption, authentication, and monitoring capabilities, as well as complying with relevant standards and regulations, across borders. Partnering with an experienced cybersecurity provider can help organisations achieve this, as they can offer advanced threat management solutions that can detect, contain, and respond to security incidents effectively.

Enabling integration

A third challenge of IoT deployment is integrating the solutions with other technologies, such as analytics, automation, and artificial intelligence. While IoT offers significant benefits on its own, combining it with these technologies can unlock more opportunities to optimise performance, enhance decision-making and achieve sustainable growth.

For example, employees in a smart factory can use analytics to analyse data from sensors and machines, and identify patterns, trends, and anomalies. Teams can then enable automation to adjust processes and parameters in real-time, improving efficiency and quality. AI can also be used in tandem, to help teams earn from data and feedback, and generate insights and recommendations for improvement.

However, integrating these technologies can also introduce more complexity and challenges, such as data management, technology compatibility, and network performance. To address these, organisations need a flexible and secure network solution that can support their diverse and dynamic needs. This is where SD-WAN can help. By combining multiple connectivity options into one hybrid network, SD-WAN can enable an intelligent, automated, and adaptable approach to network management. It can also isolate IoT devices from the rest of the network, enhancing security and preventing attackers from accessing critical assets.

Demonstrating ROI

A final challenge of IoT deployment is demonstrating a return on investment. IoT solutions require significant upfront and ongoing costs, such as hardware, software, connectivity, security, and maintenance. To justify these costs, organisations need to show tangible benefits, such as cost savings, efficiency gains, and customer satisfaction.

For example, a smart energy system can provide real-time insights into energy consumption patterns for residential, commercial, and industrial users, improving energy conservation, optimizing tariffs, and promoting sustainable practices. IoT-enabled supply chain management can track the movement of food products from farm to market, ensuring timely delivery, reducing spoilage, and improving overall efficiency. A smart healthcare system can improve patient outcomes, staff productivity, and regulatory compliance, leading to better quality and reputation.

To achieve these benefits, organisations need to define clear and measurable objectives, monitor and evaluate their performance, and communicate their results. They also need to align their IoT strategy with their business strategy and adopt a digital fabric of solutions that addresses their specific challenges and opportunities. By doing so, they can maximise the value of their IoT investments and drive innovation and growth.

The future of IoT

In a world driven by data and connectivity, businesses that wait to take advantage of IoT solutions risk being left behind. By not investing, businesses will sacrifice their chance to get ahead of the competition – and inevitably deal with greater inefficiencies, difficultly adapting to market shifts and a limited potential for growth. ■

Full steam ahead for NOC's ocean research fleet

The National Oceanography Centre (NOC) is at the forefront of research in large-scale oceanography and ocean measurement technology innovation. The UK-based NOC is one of the world's top oceanographic institutions employing around 650 staff. The NOC supports scientists in universities and research institutes with facilities, research infrastructure and irreplaceable data assets; and additionally manages Europe's largest fleet of autonomous and robotic vehicles, and two state-of-the-art research ships - RRS Discovery and RRS James Cook.

Refurbish and upgrade

The NOC had planned to refurbish RRS Discovery and RRS James Cook and identified an opportunity to install a robust and secure IT infrastructure solution onboard both vessels. Connectivity is an essential aspect aboard a research vessel amidst the vast ocean, and given the rarity of such refits, this presented a unique opportunity to establish modern levels of connectivity and state-of-the-art security onboard each vessel.

The primary objective was to provide an up-to-date, high speed, and secure network and IT infrastructure. Emphasis was placed on security, especially considering the prevalent challenges posed by malicious attacks, ransomware, and data breaches. Considering that the vessels continuously amass substantial volumes of research data, which serves as the foundation for scientists' research papers and academic degrees, the pivotal task was to efficiently store, secure, and provide seamless accessibility to this data across the vessels' various devices.

Pre-staging equipment

Logicalis was tasked with installing both indoor and outdoor elements, including access points mounted on masts. Upon embarking on their journey, the outdoor components would be subjected to extreme weather conditions from Equatorial to Arctic and the Antarctic. Therefore, Logicalis was required to design a solution that could withstand the harshest of weather conditions.

The RRS Discovery and RRS James Cook pose significant architectural obstacles to the installation of IT infrastructure. Despite their considerable size, the vessels' limited space is primarily allocated to research equipment and the storage of provisions necessary for sustained periods at sea.

Consequently, the implementation of any IT solution had to be executed within highly constrained physical parameters and be appropriately sized to fit into the available space. Additionally, the metallic composition of the research vessels poses a significant challenge to the design of any wireless solution.

The refit completion date was fixed, as RRS Discovery and RRS James Cook were scheduled to depart on a specific date. Accordingly, updating the onboard network had to be started and completed within a narrow window of opportunity.

Given the time constraints, a pre-staging process became imperative. Over three months, Logicalis pre-staged all wireless networking equipment at the NOC building in Southampton. The project team tested and ensured the functionality of every component whilst overcoming any challenges during the testing phase. Once the customer approved the solution, the equipment was swiftly transferred onto the ship, which then continued on its journey to Scotland, where a team of Logicalis engineers undertook the physical installation of the network.

While testing is important for every project, this one added a distinct dimension of urgency, as all challenges had to be successfully addressed and resolved within an immovable deadline. The timeline for delivering the solution was initially constrained by manufacturer supply times. The process began with the design and sign-off, which took approximately 12 weeks, followed by the pre-build, equipment staging, and off-board testing on both ships, spanning 14 weeks. The installation and testing on each vessel required 2 weeks, while the final knowledge transfer preparation and sessions for the operations team took an additional 2 weeks. Overall, the entire elapsed time accounted for 11 months, primarily due to equipment dependencies. The physical progress, from kick-off to operational handover, extended over 32 weeks.

All aboard

The partnership successfully delivered on the deployment of an advanced and all-encompassing wireless infrastructure solution that ensures improved levels of security to keep research data safe and in the right hands. As a result of the success of this partnership, the NOC has entered into a 12-month managed service agreement with Logicalis.

In adherence to Logicalis' proposed strategy, the project executed its outlined objectives:

1. High speed and highly available server and storage solution with up to four times more capacity than the ships previous solution in a smaller footprint.
2. High-speed data backup and recovery.
3. Multi-gigabit network backbone.
4. Network segmentation and software defined access control.
5. Centralised user authentication and role-based access.
6. Wired and wireless network access throughout the ships.
7. Software Defined Wide Area Network connectivity through satellite, 4G and point-to-point networks.
8. High speed ship-to-shore connectivity in the home port.
9. Guest WiFi internet access.

The individuals onboard now experience enhanced WiFi coverage encompassing the entire vessel. From the IT administrators' standpoint, the primary advantage lies in the significantly enhanced cybersecurity on board, along with an integrated solution that facilitates seamless wireless connectivity between the vessel and the NOC headquarters upon arrival at port.

"Resilient and robust IT systems are fundamental to supporting the work and research we do at sea," says Juan Ward, head of the ships scientific system team, National Oceanography Centre. "The Logicalis team worked tirelessly to deliver the project against a complex set of requirements and the backdrop of global supply chain issues. We are pleased that their solution significantly increases the security of the onboard IT infrastructure, decreasing risks to research data, scientific systems and marine business systems, whilst at the same time enhancing the user experience with WiFi throughout the ship and high-speed connectivity when alongside in Southampton." ■

Wellcome Genome Campus expands connectivity

The Wellcome Genome Campus (WGC), located on the Hinxton Hall Estate, is home to world-leading genomics and biodata research institutes, innovative companies, scientific facilities, and a state-of-the-art conference centre.

WGC needed to quickly replace its previous radio system and equipment, as, within a short timeframe, the incumbent provider was no longer able to offer support, maintenance, or repairs. As well as nearing its end of life, the WGC required a radio system with a higher level of resilience and security, which could be expandable for future campus expansion.

Resilient decision-making

WGC approached long-time partner Radiocoms Systems looking for an easy-to-deploy, scalable system that could provide improved site- wide coverage, both now and moving forward, as there are plans in place for further campus development. Additional requirements included a high level of resilience and security, the need for ongoing support and maintenance, and the flexibility for multi-layered integration (for flexible radio usage and management data, for example.)

Following meetings with stakeholders and site surveys, Radiocoms recommended a Motorola Solutions DIMETRA Express system to WGC. DIMETRA Express has been specifically designed so that smaller-scale commercial customers like WGC can benefit from the TETRA technology usually associated with large public safety organisations. WGC opted for an MTS4 system, with web-based applications for configuration (and system management), which is a complete TETRA solution in one box, having the core server integrated alongside the base radios; this meant, following the Factory Acceptance Tests, the Radiocoms engineers were able to set up the system in a very short turnaround.

"We rely on radio communications to manage operations on campus. Therefore, it was a great relief when our partner Radiocoms stepped up to quickly deliver a Motorola Solutions TETRA radio system, when our previous system suddenly went end-of-life. We did look at alternatives, but DIMETRA Express met all our requirements. Plus, lots of public safety organisations work with Motorola Solutions and use DIMETRA TETRA technology, so we know we will have the security, reliability, and flexibility we need, both now and well into the future. This is a long-term investment for us," said Jenny Rees, head of soft services, WGC.

To ensure the required coverage, two separate base radios were installed at opposite ends of the campus. Radiocoms also organised the Ofcom licences and initial trainer training, followed by a series of follow-on meetings to ensure all areas of the system were working optimally.

In conjunction with Motorola Solutions TETRA Support Services, Radiocoms will continue to provide 24/7 ongoing support and maintenance, for both the software and hardware, with upgrades, repairs or replacements (with courtesy equipment), as well as licence management. Talk groups have been established and the system and radios have been configured to meet both the wider team requirements and the specific operational needs of several different user groups, including Grounds, Cleaning, Security, Estates & Facilities Management, Health & Safety and Engineering. Should a member of the grounds team press the emergency button or not respond to a lone worker notification, this will be received not only by the 24/7 control room and members of the grounds group but also the security team, so groups can easily interact when necessary.

The system is also compatible with WGC's existing IT infrastructure and security patrol system. The IT team particularly appreciates the significantly easier system management, as well as the fact that, via iTM, it can now centrally programme, maintain and upgrade its radio fleet on-site; this saves time and cost, compared to the previous system, when radios had to be sent back to Radiocoms for any changes. The radios can also be ramped to 2.8W transmission power, giving long range coverage, essential for such an extensive site.

Expansion and functionality

WGC is now benefiting from fully supported, more secure, high performance and flexible radio communications.

Users are particularly enjoying the improved audio and coverage, as well as the latest handsets; the IT team, meanwhile, is appreciating the ease and autonomy of management of both the system and the radio fleet; and, finally, senior stakeholders are pleased with the cost and time savings the system is delivering, specifically regarding the speed of procurement and installation, the ability to programme and manage radios on-site and the reduction in licensing fees.

"My teams love the new MXP600 radios. They are compact, lightweight and offer much better audio quality everywhere on campus. They are also packed with extra features, like the Lone Worker app and emergency button, and many more we haven't started using yet, so my teams can work more safely and efficiently. And being able to now manage our radio fleet here on-site is a huge plus," said Richard Figgins, security manager, Wellcome Genome Campus.

Moving forward, there are plans to both grow the system, in line with planned campus expansion, and introduce new functionality and features, such as dispatch software.

"Radiocoms is proud to have been selected as the supplier for this upgrade project by Wellcome Genome Campus, building on our long-standing partnership. By leveraging the advanced capabilities of Motorola Solutions DIMETRA technology, we have deployed a resilient and bespoke system that will significantly enhance safety, insight, and efficiency across the entire campus. Radiocoms are excited to be supporting them as they embark on a journey of expansion," Simon Bingham, senior account manager, Radiocoms, told *Networking+*. ■

The impact of AI on security: advocacy vs apprehension in a time of uncertainty

Brian Martin, head of product development, innovation and strategy, Integrity360

The debate over whether AI is friend or foe continues to rumble away in cybersecurity spheres, further fuelled by the recent rise of generative AI tools such as ChatGPT.

On the one hand, many security professionals have heaped praise upon natural language processing platforms, proclaiming their potential to transform security for the better. From streamlining SOC operations to predicting potential threat and intrusion scenarios and fine-tuning security configurations, many organisations are already exploring the application and potential benefits of AI in security.

On the other, however, extreme concerns are being cited around the threat that AI could be used to democratise cybercrime, enabling attackers to develop and carry out sophisticated attacks more easily and effectively.

Such concerns are only natural. Time and time again we've witnessed the relentless exploits of attackers who continue to evolve their attack strategies to bypass or overcome target defences.

Between these two opposing seas of advocacy and apprehension, it's hard to know which side is right in relation to AI's use in security.

With the aim of better understanding industry sentiment and ascertaining key arguments from either side of the fence, we explored the debate further through surveying 205 IT security decision makers.

Three key AI concerns among security professionals

In conducting this analysis, three clear key concerns emerged regarding the use of AI in security…

#1 – Worries over deepfake attacks

More than two thirds (68%) of respondents to the survey highlighted their worries about cybercriminals' use of deepfakes in targeting organisations.

Interestingly, this aligns similarly to a 2022 survey from VMWare, where 66% of respondents revealed that they had seen malicious deepfakes used as part of phishing attacks in the previous 12 months.

The impact of this novel technology being used for nefarious purposes has already been demonstrated, perhaps most famously in a video impersonating Ukrainian President Volodymyr Zelensky falsely requesting that the country's forces lay down their arms and surrender.

While this example was politically motivated, organisations must be aware of and prepared for similar threats. Indeed, back in 2020, one cybercriminal stole $35 million after using AI to successfully clone a company director's voice and trick a bank manager.

With AI on the rise, sophisticated attacks such as this will only continue to become increasingly prominent in the coming months.

#2 - Heightening attack volumes

59% also agreed that AI is serving to increase the volume of cyberattacks facing organisations.

Indeed, we've already seen instances in which AI is being used offensively. Check Point Research, for example, identified instances where cybercriminals were using ChatGPT to create social engineering attacks and even develop malware code.

At present, the ability of natural language processing tools to create phishing messages is perhaps the area of greatest concern, with threat actors able to accurately mimic the language, tone, and design of legitimate emails to trick their victims.

#3 - Poor understanding of AI

Thirdly, we found that 46% of organisations disagreed with the statement that they do not understand the impact of AI on cybersecurity. Further, the survey also revealed that CIOs appear to have even less comprehension of AI's impact on cybersecurity, with 42% indicating disagreement with the statement.

This potential gap in knowledge and understanding among key executives is likely to be responsible for much of the stress relating to AI in security, with 61% of respondents having expressed apprehension over the increase in AI.

Similar concerns have been raised in relation to AI taking people's jobs. However, it's become clearer that technologies are largely being introduced to help workers, enhancing their efficiency and productivity, rather than replace them.

People are naturally wary of what they don't understand. Therefore, these figures highlight the importance of education in relation to AI in security to ease potential anxieties.

AI is becoming an increasingly important security tool

From the threat of deepfakes and phishing, to the sheer novelty of AI tools, it's easy to see where AI-related concerns are stemming from in a security context. However, despite these, much of the industry is already showing recognition of AI's potential to enhance security practices.

"73% of security decision makers agree that AI is becoming an increasingly important tool for security operations and incident response, highlighting the belief that AI can be used in both a defensive and offensive manner as a force for good."

According to our survey, 73% of security decision makers agree that AI is becoming an increasingly important tool for security operations and incident response, highlighting the belief that AI can be used in both a defensive and offensive manner as a force for good.

More than 71% of respondents also agree that AI is improving the speed and accuracy of incident response, with key technologies able to analyse vast amounts of data and identify threats in real-time. And 67% also believe that using AI improves the efficiency of cyber security operations – something that can be particularly useful in relation to routine tasks, with automation freeing up staff to focus on more complex and strategic aspects of their work.

Of course, it's essential to ensure businesses are considering how AI can be used against them and putting processes in place to protect against these growing threats. Without question, threat actors will look to leverage such tools in whatever way they can to get an edge.

However, at the same time, there are clear benefits to be obtained in proactively embracing AI. Indeed, those organisations that do so will be well placed to defend against both traditional and novel attack methods moving forward. ■

Support your operations with the right NAS

Tamblyn Calman, sales & marketing director, QNAP

Choosing the right NAS for an enterprise environment requires careful consideration of several critical factors to ensure it meets the specific needs of the business. These factors include connectivity options, types of drives, and intended usage scenarios.

Connectivity options: 10GbE, 25GbE, and 100GbE

One of the foremost considerations is the network connectivity of the NAS. These devices come with various Ethernet options, including 110GbE, 25GbE, and even 100GbE. The choice of connectivity can significantly impact the performance and future scalability of the storage solution.

10GbE: For many enterprises, 10GbE provides a substantial improvement over traditional 1GbE networks, offering up to 10 times the bandwidth. This is particularly beneficial for environments where multiple users or applications access large files simultaneously, such as in media production or data analysis scenarios.

25GbE: Enterprises with more demanding performance requirements might consider 25GbE. This option offers greater bandwidth than 10GbE and can handle more intensive workloads, making it suitable for businesses that deal with large volumes of data or require real-time data processing.

100GbE: For the highest performance needs, 100GbE is the pinnacle of network connectivity. This is ideal for data centres, large enterprises, or organisations involved in high-frequency trading, scientific research, or any application requiring ultra-low latency and maximum throughput.

Selecting the right network connectivity ensures that the NAS can deliver the performance needed both now and in the future as the business grows and demands increase.

Types of drives

Another critical decision revolves around the types of drives to be used within the NAS. NAS devices support a variety of drive types, including high-capacity SATA HDDs and high-speed SSDs. The choice between these largely depends on the specific use case of the NAS.

High-capacity SATA HDDs: These drives are typically the go-to choice for large data stores. SATA HDDs provide high storage capacities at a lower cost per gigabyte compared to SSDs, making them ideal for applications that require storing vast amounts of data but do not necessarily demand high-speed access. Examples include archival storage, backup solutions, and content libraries where the volume of data is more critical than the speed of access.

SSDs: Solid State Drives offer significantly faster read/write speeds and lower latency compared to traditional HDDs. This makes SSDs ideal for applications that require high-speed access to data. Use cases include virtualisation environments, high-performance databases, and real-time analytics where performance is a critical factor. Additionally, SSDs are more reliable in environments with high I/O operations due to their lack of moving parts.

Hybrid storage solutions

For many enterprises, a hybrid approach that combines both HDDs and SSDs can offer the best of both worlds. NAS devices often support tiered storage, where frequently accessed data is stored on high-speed SSDs while less frequently accessed data resides on larger capacity HDDs. This setup can provide a balanced solution that optimises both performance and cost efficiency.

Additional considerations

When selecting a NAS, enterprises should also consider other factors that can impact the overall effectiveness of the solution:

Scalability: Ensure that the NAS can scale with your business needs. Look for devices that support expansion units or additional drive bays to accommodate future growth.

Redundancy and data protection: Features such as RAID, backup solutions, and snapshot capabilities are crucial for protecting data integrity and ensuring business continuity.

Management and software: There exists a comprehensive suite of management tools and software applications that enhance the functionality of their NAS devices. Some include operating systems that offer intuitive management, virtualisation support, and advanced networking capabilities.

Encryption: Ensure that the NAS supports robust encryption protocols to protect data at rest and in transit. This includes full-disk encryption and secure data transfer protocols such as SSL/TLS.

Choosing the right NAS for an enterprise involves evaluating the specific needs related to connectivity, storage types, and additional features. By carefully considering these factors, businesses can ensure they select a NAS solution that provides the necessary performance, scalability, and reliability to support their operations both now and in the future. ■

PRODUCTS

Buffalo's TeraStation 51210RH is a high performance 12-bay NAS solution ideal for businesses requiring a reliable RAID-based network storage solution for business critical applications.

Increased speed and reliability are achieved with a 10GbE connection and enterprise class hard drives. With the powerful Annapurna Labs® Alpine AL314 1.7Ghz Quad-Core processor and 8GB of fast DDR3 ECC memory, TeraStation 51210RH provides exceptional performance during file transfers and everyday NAS functions.

The TS51210RH model is available in partially-populated units with 8TB or 16TB, and fully-populated units with 24, 48, 96, 120TB or 144TB. Partially populated models are ideal for users needing a small start with less initial investment.

The Asustor Lockerstor 10 AS6510T is a 10-bay NAS appliance that supports both hard disk drives (HDDs) and solid-state drives (SSDs), including NVMe-based drives.

The AS6510T is particularly focused on cybersecurity. Key features include a virtual private network (VPN) connection, two-step access verification, and antivirus software integration.

With Intel Denverton-based Atom C3538 Quad-Core CPU, 8GB DDR4-2133 SO-DIMM (30% faster than DDR3), and dual Intel 10-Gigabit Ethernet ports, supporting up to 20Gbps under link aggregation, the AS6510T is an excellent choice for the enterprise. The NAS also features dual Realtek 2.5-Gigabit Ethernet ports, supporting up to 5Gbps under link aggregation, dual M.2 NVMe SSD ports for fast caching, and supports Wake on LAN and Wake on WAN.

The new **TerraMaster F4-424 Pro** – reportedly the most powerful 4-bay NAS available to date - is suitable for SMB users who need high-performance storage solutions.

It features the Intel Core i3 8-core 8-thread processor with a maximum turbo frequency of 3.8GHz, integrated Intel UHD Graphics card with a maximum dynamic frequency of 1.25GHz and supports AES NI hardware encryption. Equipped with 32GB DDR5 4800MHz memory, two 2.5G Ethernet ports, and built-in dual M.2 NVMe slots for SSD caching, it significantly boosts the storage efficiency of the disk array.

Featuring a more powerful CPU and DDR5 memory, the F4-424 Pro represents a performance improvement of more than 150% on the previous generation. Application load times have increased by 100%, file and photo retrieval speed by 45%, database response speed by 55%, and the PHP response for web pages has seen a 65% improvement.

The F4-424 Pro is configured with two 2.5 GbE interfaces, supporting a 2.5 GbE high-speed network bandwidth. The linear data transmission speed can reach 283 MB/s (Seagate IronWolf 18TB x 4, RAID 0). Link Aggregation offers a network bandwidth up to 5Gb, thereby providing a cost-effective solution for multi-user and high-concurrent file access.

Synology DiskStation 1621+ is a powerful and compact 6-bay NAS – expandable to 16-bay - designed to store and protect critical data assets.

Today's growing amount of unstructured data requires smarter and increasingly higher performance methods of storing, accessing, and collaborating. Designed for scalability, the DS1621+ enables the user to start small, then expand as data grows. The enterprise can reduce transfer times with the DS1621+ and achieve faster networking and NVMe drives to further boost performance.

Synology iSCSI storage fully supports most virtualization solutions to enhance work efficiency with easy management interface. VMware vSphere 6 and VAAI integration helps offload storage operations and optimizes computation efficiency. Windows Offloaded Data Transfer (ODX) speeds up data transfer and migration rate. OpenStack Cinder support turns your Synology NAS into a block-based storage component.

DS1621+ integrates various backup applications into an intuitive user interface, offering durable storage technologies to safeguard valuable data on any device. Active backup, hyper backup, and drive backup are among the options.

Western Digital's My Cloud Pro 4100 is a four-bay high-capacity NAS which enables the enterprise to back up content from all computers in one place, on a private network, and without monthly subscriptions. Combined with a quad core Intel Pentium N3710 processor and 4GB of RAM, the user can seamlessly stream HD videos or share content with multiple users.

The available Acronis True Image for Western Digital software delivers easy, efficient, secure cyber protection, integrating backup with an AI-based defence against ransomware and cryptojacking attacks. The Acronis True Image for Western Digital software backs up everything from operating systems and applications to settings and individual files.

Multiple RAID options help protect the digital library, while password protection and 256-bit AES volume encryption helps safeguard files from prying eyes. Along with two power ports in case of a power supply failure, the My Cloud PR4100 helps keep data safe.

Data is always protected with remote off-site backup to another My Cloud NAS device or with an integrated cloud backup solution. My Cloud Pro Series also provide LAN/WAN backup options with centrally managed backup, or basic file backup. Remote off-site backup to another My Cloud NAS device will help ensure that critical data is always protected and available in the instance that one NAS fails or is destroyed by a catastrophic event.

Please meet...

Kanwar Loyal, VP for Northern Europe & MEA, Cato Networks

Who was your hero when you were growing up?

Growing up, my heroes were quite diverse, ranging from Liverpool players like Jan Mølby and the legendary Bruce Grobbelaar, to the iconic Bruce Lee. I was so enamoured with the football world and martial arts that I even asked my parents if I could change my name to Bruce, inspired by both Grobbelaar and Lee. It's funny how my enthusiasm for martial arts blended seamlessly with my passion for football, and these two Bruces became my idols during my formative years.

What was your big career break?

My significant career breakthrough occurred during the early days of my time at Imperva. It wasn't so much a break, but rather the influence of an exceptional manager who wholeheartedly believed in my capabilities. This endorsement proved to be a game-changer, providing me with the freedom and inspiration I needed to thrive. In an industry often characterised by micromanagement, having someone who genuinely believed in me, demonstrated that support and encouragement makes a profound impact. I believe there's a distinct contrast between management and leadership in our industry. It seems that we're surrounded by many managers but only a handful of true leaders. Since that moment, my career has been on an upward trajectory, fuelled by the confidence and opportunities that stemmed from that important encouragement and guidance.

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

The best advice isn't something explicitly given to me, but more of a philosophy I've embraced. One mantra that has become a guiding principle for me is - 'win the morning, win the day.' I try to accomplish as much as possible before noon, whether it's personal, work, or family. I firmly believe in maintaining a balance across these aspects of life to create fulfilment.

Additionally, another piece of advice I've adopted is to 'lead with gratitude.' This approach has significantly altered my perspective on life and career. Resentment and unhappiness seem prevalent in many people's lives, gratitude has become a powerful lens through which I view the world. Understanding that different parts of the world find happiness in varied expectations has been eye-opening. In the cyber industry, I recognize the privileged position we hold, given the high demand for our skills. This perspective is a result of leading with gratitude each day, acknowledging the fortunate choices we've made in our career paths.

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

Given my love for travel and belief it has the power to make the world feel either expensive or intimate, I would choose to work in the travel industry. I've always been fascinated by the idea that travel can broaden the mind and expose us to countless cultures and experiences. The world is vast, and there's so much happening beyond our immediate knowledge.

Personally, I am an avid consumer of travel content, and it's the one thing I consistently watch on television. Whether it's exploring different destinations or understanding unique cultures, travel programming has a special place in my heart. If I were to venture into a different industry, I would want to contribute to the world of travel, helping others explore and appreciate the diverse wonders our planet has to offer.

Where would you live if money was no object?

I would undoubtedly choose to live along the Mediterranean. The appeal lies not only in the warm climate but also in the rich culture of the region. My friends who reside in Continental Europe have shared stories of casually driving down to Portugal for the day, highlighting the ease of exploring different countries in the area. While I appreciate the allure of living in various places, particularly in Asia, the convenience and charm of Europe, especially along the Mediterranean, resonate with me. Whether it's Portugal or the southern coast of Italy, the Mediterranean offers a perfect blend of climate, culture, and accessibility that I find immensely appealing.

What's the greatest technological advancement in your lifetime?

The most remarkable technological advancement in my lifetime has undoubtedly been the internet. Considering that individuals in their twenties nowadays may not have experienced a childhood without it, the impact is profound. It's not just about the Internet itself but how it has seamlessly interconnected every aspect of our lives. From shaping our identities to influencing how we connect and stay connected, this interconnectivity is the hallmark of our era, all rooted in the inception of the Internet.

While this has brought about incredible benefits, such as better communication and accessibility to information, it has also created issues, notably the proliferation of disinformation. Despite the drawbacks, the pros of this technology are numerous, making it a transformative force that has reshaped the way we live and interact. ■