MARCH 2023
networkingplus.co.uk

NETWORKING+

Endpoint backup

Effective data recovery is essential for maintaining security

André Schindler, NinjaOne, p6

Smart food storage

IoT sensors provide peace of mind and reduce costs

Chris Potts, ANT Telecom, p13

Questions and answers

I'd love to have met Alan Turing

Martin Saunders, Highlight, p16

Spring Budget: making the UK a science and tech superpower

The UK Government announced in its Spring Budget 2023 a £370 million Science and Technology Framework to make the UK a 'science and technology superpower.'

Most notably for those in the networking and IT space is the promise that, although corporation tax has been increased to 25%, every pound invested in IT equipment, plant or machinery can be deducted in full and immediately from taxable profits.

"It is positive the chancellor stuck to the decision of increasing corporation tax to 25%," commented Claire Trachet, CEO/founder, Trachet. "Measures such as the implementation of 'full expensing' are critical for growth in curbing the impacts of this. This will help to support businesses, particularly in the tech sector, where investment in equipment and infrastructure is critical to growth and innovation."

The news is good for research-intensive technology companies (defined as those spending more than 40% of their outgoings on R&D) too, with additional financial support of up to 27p/£ announced to help drive innovation.

"The significance of this update is clear and follows from the rate cuts to SME R&D credits announced in the disastrous Autumn budget statement, which had far-reaching implications for many high-growth early-stage companies," said Richard Turner, senior managing director, FTI Consulting's UK Tax Practice. "We are hopeful that the current consultation results in a new regime that puts the UK unquestionably ahead in its competitiveness for being the location of choice for ground-breaking and lifesaving R&D."

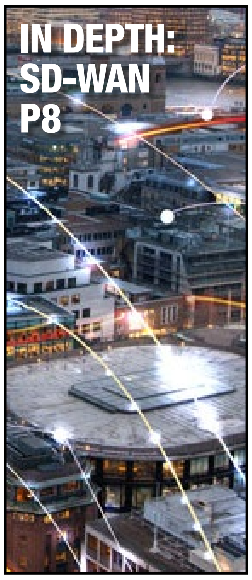
The budget specifies that £900 million will be invested to build an exascale supercomputer and to establish a new AI Research Resource. Further, a £1 million prize will be awarded annually for the next 10 years to researchers driving progress in critical areas of AI, and a whopping £2.5 billion will be invested over 10 years in quantum computing.

"The government's commitment to strengthening the country's position in AI through the AI sandbox and the clarity on IP rules for generative AI companies will enable us to bring cutting-edge products to market faster," said Trachet. "Additionally, the £900 million funding for an exascale computer and the £2.5 billion for quantum computing will position the UK as a world leader in this field."

Also announced in the budget is an £80 million funding pot to support the development of open network solutions, aiming to target high demand density (HDD) use cases; RIC and other RAN software automation; and processors, RF, and other RAN hardware.

"As it [the government] has correctly pointed out, blueprints to develop, demonstrate and test approaches that are commercially ready for operators to deploy is vital to the success of open networks," said Kristian Toivo, executive director, Telecom Infra Project (TIP). "The UK is looking to become a leader in telecoms diversification, and incubate home-grown innovations, particularly for the RIC, that will bring about new use cases that ultimately benefit consumers and businesses."

Following the headlines into the rest of the year, we can expect to see an uptick in spending as companies make hay while the sun shines. "There is a growing number of investors who are sat on a dry powder pile having paused investments due to uncertainty in 2022. This means there are significant opportunities on the horizon, and now is the moment to prepare and get deal ready as optionality will increase in H2 of this year," said Trachet. ■



IN DEPTH:
SD-WAN
P8

44% of hospital trusts not ready for PSTN switch off

A Freedom of Information (FOI) request by Maintel reveals that out of the 105 hospital trusts across England and Wales that responded (44%) have no strategy for the Wholesale Line Rental (WLR) withdrawal of Public Switch Telephone Network (PSTN) and Integrated Services Digital Network (ISDN) services.

The size of the issue facing the UK healthcare sector is revealed, as the FOI also found that among the 56 NHS trusts which could respond, there is a staggering amount of PSTN / ISDN lines installed – up to 10,315 in total.

Maintel states, if the switchover is not done in time, it could lead to widespread disruption of healthcare services. Services such as pagers, alarm lines, payment terminals, payphone lines, medical devices and external connectivity to telephony systems could all be impacted.

"Healthcare has a strong reliance on PSTN lines, not only for communication systems like the pagers used by doctors and other hospital staff but also for actual medical devices. The lack of strategy for the WLR withdrawal among some hospital trusts is worrying, as the deadline is fast approaching and those that don't change course face major disruption," said Dan Davies, CTO at Maintel. "Hospitals may not be able to meet safety standards and could be left in a position needing urgent and expensive workarounds to adhere to safety or insurance requirements. Telephony systems that connect to the outside world via ISDN could also be cut-off, potentially impacting critical services."

While BT will switch off the PSTN and ISDN in 2025, all WLR products will be removed from sale by September 2023. Organisations using ISDN, PSTN or xDSL broadband services will need to migrate to new digital alternatives.

Supply chain delays lasting over 12 months mean those hospitals that try to wait until the last minute could be caught out. As a consequence, installing the new technologies across their historic hospital buildings could cause major issues. Hospital trusts need to act this year if they are to ensure that any technology upgrades needed can be ordered to be delivered and installed in time for 2025. They, therefore, need to start comprehensive audits of their estates to identify any affected services.

New services will be almost exclusively fully fibre based and completely digital. This means they are highly resilient and integrate seamlessly with other next-generation services.

"Migrating all lines ahead of the 2025 WLR withdrawal is no small feat. Hospital decision-makers cannot wait any longer. Understanding the problem is the first step. A rapid audit of networks is a must to understand how many connections there are and what type they are being used for," said Davies. "Hospital IT teams who leave it to the last minute, do not just face widespread disruption to services, but it could result in increased installation costs and delays. Whatever existing WLR ISDN/PSTN services you have, there are a number of easy migration paths to ensure the normal running of the organisation is uninterrupted. Hospitals must act now to ensure services can continue to function." ■

HS1 gains upgraded communications systems

Essential work to upgrade communications systems across the HS1 rail network has been completed with minimal disruption at some of the UK's busiest international rail stations.

Telent was contracted by High Speed 1 (HS1) to upgrade all critical systems from legacy analogue to modern IP solutions at St Pancras, Stratford, Ebbsfleet and Ashford international stations. These improvements better protect the station and assets, grow the business through better management of station operators and provide the ability to meet future system demand.

Around 176 thousand hours were spent on this project overall and, thanks to early detailed planning, no unplanned operational impact was experienced. There was a 50/50 split between time spent on design/planning and on-site work.

Telent designed a new core station data network (SDN) and, using an industry leading approach, drew on best in class practices and the very latest tools and standards. This helped ensure the assessment and mitigation of any identified cyber threats and vulnerabilities across the estate. Telent also designed and installed CCTV, public address, public help points, electronic access control and IP telephony systems. The building management system which controls and monitors the station environment was updated as part of the project.

As part of the project a Station Management System (MICA) was designed and installed. MICA allows the station operation team to efficiently manage all refreshed systems from a central location during both normal operations and disruption.

"This was a unique and complex project, as can be imagined on such a large-scale project at international stations including the iconic grade 1 listed St Pancras station" said Telent's programme manager station comms, Dean Clarke. "There were a significant number of stakeholders to liaise with, and ensuring their individual needs and requirements were addressed as part of the of project was crucial. We also had to deal with the complexities and disruptions caused by the coronavirus pandemic."

As well as the train operating companies that were involved, Telent worked with security agencies within the international terminals at the stations alongside local councils, and heritage advisors due to the historical significance of St Pancras station. Other challenges included working in a live rail environment, with passengers needing access for 24 hours a day, the works had to be well planned and carried out with minimal disruption.

"We're very proud to have renewed critical communications systems with minimal impact to station operations during an already difficult time, ensuring passengers continued to receive timely and accurate information. This is key to an enhanced experience, and to ensure that passengers and staff stay safe and informed during their travels," said Clarke.

"The stations on the HS1 route welcome thousands of passengers every day. Making sure our security and communications systems are of the highest quality and reliability is of maximum importance to us. Designing and delivering the renewals across all four stations with minimal interruption to our passengers and customers has been key to its overall success," said head of programmes and sponsorship at HS1, Owen Virrill. ■

Maintel to update NHS telephony system for hybrid work environment

Argyll & Bute Health & Social Care has selected Maintel to deliver a new and improved telephony system. In a new hybrid working environment, 2,500 staff across eight community hospitals and selected GP practices now benefit from Maintel's cutting edge, reliable and resilient telephony solution with patients being able to enjoy accessible, user-friendly phone contact.

Argyll and Bute Health and Social Care Partnership (HSCP) provides all health and social care services across a large area in the west of Scotland. The legacy telephony system had been in place for many years and had developed known issues. Not only was it a significant financial overhead, but it was unable to support the integration of new technologies and was no longer providing value for money.

Maintel was chosen to design a comprehensive yet cost-effective telephony solution that would introduce new features and applications to enhance call routing and handling and enable Argyll and Bute HSCP to achieve their future integration goals with ease. The system was designed to be scaled and expanded as necessary to cover more GP practices, and encourage, support, and facilitate the close collaboration that their mixed management team need to help improve patient care.

The Argyll and Bute HSCP team were also looking for a close partner relationship with easy regular access to specialists so that any issues could be dealt with quickly. Maintel's reputation as a trusted advisor with teams that take time to understand current issues, restrictions and requirements fitted with their vision perfectly.

Maintel's customer success manager worked closely with the Argyll & Bute HSCP team to provide a state-of-the-art, industry leading, future-ready telephony solution within the eight hospital environments, which also went on to benefit a small collection of GPs in the Oban area. The modernised system has already begun to revolutionise how Argyle & Bude HSCP operate and is a solid foundation for them to take further advantage of existing and emerging technologies in the future.

"The entire Maintel team were so easy to work with. Complete professionalism and constant support - it's all really good from a customer's perspective," said Stephen Morrow, deputy head of e-health HSCP, NHS Highland.

"We are thrilled to have delivered a smooth transition to the new platform," said Fraser Sutherland, head of government and education at Maintel said. "We also look forward to the potential for Argyle & Bute HSCP to reap more benefits from the system with additional integrations, which will help them to achieve maximum value from their investment, while also improving the lives of the local community."

"Having one system across all four remote sites that is flexible enough to work independently of, and collaboratively with one another is brilliant," said Mark Dixon, practice manager, Lorn Medical Centre and Mull and Ioana Medical Group. ■

EDITORIAL:

Editor: Amy Saunders
amys@kadiumpublishing.com

Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Kate Fulkert, Chris Potts, Scott Goodwin, Duncan Swann, André Schindler, Sergei Serdyuk, Martin Saunders, Dene Lewis

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

Cognizant to deliver digital transformation for VWG Ireland

Cognizant has been selected by Volkswagen Group Ireland (VWG Ireland) to transform its digital customer service landscape. Cognizant will re-engineer VWG Ireland's existing siloed contact centre platform into an omni-channel customer experience (CX) platform, based on Salesforce service cloud voice and Amazon Connect.

VWG Ireland needed to unify its legacy contact centre functionalities and streamline its customer service to reduce maintenance costs and improve efficiency, while gaining a holistic customer 360-degree view. Due to its siloed customer engagement processes and channels, VWG Ireland was also faced with a lack of customer insight and time-consuming manual customer data aggregation. As part of the agreement, Cognizant will implement a fully digital, cloud-based omni-channel CX platform to modernize customer engagements, as well as provide an easy-to-use, web-based, and unified user interface for the agents combining customer data, context, journeys, and interaction channels.

Cognizant will also provide VWG Ireland with advanced insights into customer journeys and conversations. This is intended to improve reporting, advance business decisions, and drive next best actions to provide a personalized experience to customers and recommend next steps, services or products. In addition, Cognizant will work together with VWG Ireland for continuous improvement, feature enhancements and process innovation of the CX platform. The introduction of the CX platform allows for improved efficiencies for both end users and their supervisors, freeing up time for the provision of an optimized level of service to VWG Ireland's customers.

"The automotive industry has been transformed from the bottom up over the past decade, not least with the accelerated uptake of electric vehicles. In addition, customer expectations on service levels and how to engage with various organisations has also shifted, accelerated by the necessity of remote access, service provision and support during the pandemic," said Tom Murphy, CIO, VWG Ireland. "In particular, the car industry has seen a shift in how customers wish to communicate with us. To be able to interact with our customers in a more meaningful and direct manner, we needed a trusted IT partner to help us in our mission to improve our systems and engage with our customer base more efficiently." ■

Gigaclear selects Aiimi Insight Engine for privacy

Gigaclear has adopted the Aiimi Insight Engine to deliver advanced data privacy and compliance capabilities.

With the Aiimi Insight Engine, Gigaclear will greatly enhance its risk mitigation capabilities and increase operational efficiency at scale. As a purpose-built AI-powered compliance platform, the Aiimi Insight Engine reduces data privacy risk exposure by bringing unstructured data under control through advanced enrichment and classification. This will enable Gigaclear to quickly identify high risk items for action and enable proactive monitoring and management of high-risk data across the business.

"With more than 300,000 rural homes and businesses now connected to our full fibre network and that number growing every day, the delivery of an efficient and scalable data risk mitigation posture is absolutely essential for the business," said Gordon Perry, CIO, Gigaclear. "The capabilities of the Aiimi Insight Engine clearly aligned with our data management needs and will future-proof Gigaclear as our growth journey continues to accelerate."

Further to the advanced day-to-day management of data, the Aiimi Insight Engine also delivers a fast and efficient process for responding to data subject access requests (DSAR). The platform's advanced search and discovery capabilities, along with automated redaction technology, removes extensive manual processes and streamlines the delivery of information pertinent to DSARs.

"Organisations that operationalise and manage a significant amount of customer data on a daily basis are increasingly exposed to falling foul of data privacy laws and regulations. With costly repercussions, both reputational and financial, advanced data management platforms and technologies that mitigate risk and drive data efficiency are rightly being implemented across industries. As Gigaclear's growth accelerates, we are pleased that the Aiimi Insight Engine will provide the scalable solution needed to enable a complete data vision and match the business's growing data management requirements," said Steve Salvin, Aiimi. ■

27% of decision-makers confused about cloud provider responsibilities

Arcserve has announced key findings from its annual independent global research. The study found that 27% of IT decision-makers (ITDMs) from UK organisations falsely believe that cloud providers are responsible for protecting and recovering data in the public cloud. This misconception of data protection responsibility can lead to increased vulnerability, especially amid a growing cloud investment trend for the cloud.

The Arcserve annual survey uncovers a consistent misperception regarding the responsibility for data stored in public clouds. In 2019, 47% of ITDMs believed it was the cloud provider's responsibility. The misconception persisted in 2020, with 40% believing the same, and now stands at 27% in the latest research. The research highlights several additional factors that reveal a concerning lag in data protection, including that nearly two-thirds of ITDMs surveyed believe cloud backups are safer than on-premises backups; almost one-third reported poorly documented disaster recovery plans; and 27% reported that their organisation's disaster recovery plans were not updated.

"Organizations need to understand that data protection and recovery responsibility lies with them, not with the cloud provider," said Florian Malecki, executive vice president of marketing, Arcserve. "The time to act is now, particularly amid growing hybrid and multi-cloud adoption as proven by our annual research with some 85% of ITDMs expecting to increase hybrid cloud investments and 77% expecting to increase multi-cloud investment." ■

Blue Tahiti relocates to Proximity's Bristol Edge 9 DC

Blue Tahiti has relocated its IT operations to Proximity's Bristol-based Edge 9 colocation data centre.

Following an extensive review of its immediate and future IT and infrastructure requirements, Blue Tahiti made the decision to move to Proximity Edge 9 from its previous Surrey-based colocation facility. The move was prompted by Blue Tahiti's planned significant expansion with the launch of a new range of products, including an ecommerce platform which has the potential to service the data analysis requirements of thousands of online traders.

Key data centre decision criteria included available space and forward power, on-site engineering support, a strategic location, high level of physical security, diverse fibre connectivity options and price-competitiveness.

"In Proximity Edge 9 we have found a very secure and conveniently located facility with access to further rack space and power as and when we need it," said Nathan Collins, CTO, Blue Tahiti. "Their competitive fixed pricing is an additional bonus. These factors along with experienced on-site engineering personnel is very reassuring as we continue to expand."

Network services provider ICONIC Networks managed the necessary fibre to rack network connections at Proximity's site including a VPN connection between Blue Tahiti's UK and US offices. ■

Virgin Media O2 upgrades to 4G and 5G RAN

Virgin Media O2 will invest millions of pounds to install the latest Ericsson 4G and 5G RAN hardware, software, and service enhancements.

Under the new contract, Virgin Media O2 will deploy the latest Ericsson quad-technology baseband, multiband and 5G Massive MIMO radio AIR 3258 technology - Ericsson's new lightweight antenna radio - in England, Scotland, and Northern Ireland.

Additional service upgrades and small cell solutions will improve connectivity in Birmingham, Manchester, Liverpool, Leeds, Sheffield, Glasgow, Edinburgh and Belfast with enhanced mobile capacity, improved coverage, and faster speeds.

A reduction of up to 30% in energy use is expected compared with the previous generation of cell technology.

A 40% reduction in weight and volume will minimise the impact of installing infrastructure and help accelerate network deployment.

"This investment means customers can benefit from more reliable and faster services and reduce overall carbon emissions. Our relationship with Ericsson allows us to deliver improvements quickly and efficiently, helping us move towards future-proof networks," said Virgin Media O2, chief technology officer Jeanie York.

"We are building a network that will help to transform new industries and pave the way to a more connected digital society," said Ericsson UK and Ireland CEO Katherine Ainley. ■

Oxfordshire gains gigabit capable full fibre broadband

Neos Networks has built infrastructure to more than 90 public sector and local authority sites in Oxfordshire to access gigabit capable full fibre broadband. This milestone is part of the GigaHubs project to upgrade connectivity infrastructure across Oxfordshire in partnership with Oxfordshire County Council with additional funding from Building Digital UK.

The project is on track for completion by the end of 2023. The project began in 2021 with four of the eight delivery milestones having been completed to date. Sites including community centres, village halls, schools, libraries, GP surgeries, leisure centres, fire stations and museums, are already benefiting from gigabit connectivity, improving service quality for end users, and allowing public spaces to better fulfil their roles as community hubs.

The GigaHubs project has a primary aim of bringing fibre right into the heart of communities, improving service efficiency whilst providing fibre 'hubs' from which industry can additionally connect other businesses and homes.

Following the council's Better Broadband for Oxfordshire and Businesses in Rural Oxfordshire projects, the addition of the GigaHubs project will mean over 1,500km of fibre has been provisioned to lay the foundations for a 'smart county.' This improved connectivity is a key component in enabling future innovation such as drone corridors, connected autonomous vehicles, and other IoT services for residents and businesses. ■

Word on the web...

Why is automation crucial for digital transformation?

Dene Lewis, head of technical strategy and direction, CAE Technology Services Ltd

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

Building a solid DC business continuity strategy

Kate Fulkert, global business continuity and disaster recovery manager, Vertiv

Anything can happen at any time. Organisations need to be ready to pivot operations quickly and efficiently when needed. Business continuity has never been more important, and a company's DC strategy is paramount in keeping operations running and businesses open. So, what do we see as the most pressing risks to businesses today - more than two years after we first started grappling with the pandemic?

Dealing with civil unrest

One year ago, the fallout of COVID-19 continuing to rock businesses of all sizes. But today we are spending more time on civil unrest and extreme weather conditions than any other threat.

In addition to the devastating destruction and for those in the country and in nearby regions, the war in Ukraine has dramatic implications globally. Further strain has been put on supply chains, severely restricting commerce.

The war is taxing systems and creating an environment that attracts bad actors. It's an ongoing and increasingly volatile situation, and will be for the foreseeable future. Organisations should develop business continuity and disaster recovery plans for employee communication, transportation, supply chain and workflow, whilst increasing cybersecurity training.

Protecting organisations

The shift to hybrid models continues to cause challenges, not least a significant increase to the threat of cyber attacks. A distributed workforce means more endpoints, each representing a risk. Businesses must increase attention on network security and ramp up employee training on IT and operational security.

Organisations must also consider how they will track and communicate with employees in an emergency. They should invest in platforms that can enable critical communications, even when traditional channels are down, and update crisis management training so employees know how to react independently.

A twelve-point plan for success

1. **Risk assessment and the Business Impact Analysis (BIA):** Perform the BIA to determine critical business functions and a risk assessment to identify potential mitigations or controls that should be implemented.
2. **Weatherproof the data centre:** Create a severe weather checklist and train employees how to prepare for extreme weather conditions.
3. **Network redundancy:** Build network redundancy into your data centre; ensure you have redundant core and edge infrastructures along with multiple fibre vendors to reroute traffic in the event of an interruption in the network path. Conduct a network system check two times each year.
4. **Backup data:** Automatic backups on-site may need to be initiated manually, and the mechanics should be hardened against cyber threats.
5. **Preparation for communication breakdowns:** Develop lists with all means of communication for all employees and reach out early with instructions in the event of communication interruptions.
6. **Emergency staffing:** The preference for many companies today is to shift work virtually, but staff on site may still be required, and needed immediately; have an emergency staffing plan in place.
7. **Contact vendors:** As supply chains continue to lag, businesses should consider adding vendors and suppliers to their mass notification systems to ensure critical communications are maintained.
8. **Move away from a single vendor approach:** Critical business functions should have more than one vendor in place in the event that vendor has a supply chain issue.
9. **Build team redundancy and train on emergency response:** Along with team redundancy, train team members for various types of crisis events at work, home or out in the field. Conduct training so they can react to a crisis independently. Employees should take advantage of weather and emergency phone apps too.
10. **Inform and work with first responders:** Taking photographs of the data centre prior to a disaster event is good practice; before and after pictures make it easier to work with insurance providers.
11. **Consider the opportunists:** Training employees on cybersecurity best practices is more critical than ever.
12. **Test your plans:** Testing is the best means to get recovery plans communicated.

Whilst the threats to businesses are changing, the need to prepare adequately with robust business continuity strategies is not. Processes, policies and plans must begin with protecting the critical infrastructure which keeps businesses up and running – not least in the DC. ■

Endpoint backup – essential for modern enterprise

André Schindler, general manager EMEA, NinjaOne

An effective data recovery solution is essential when it comes to maintaining security and business continuity. Backups give you important survival options when ransomware hits, a laptop is lost, or someone accidentally deletes a folder full of important files.

What is an endpoint and endpoint backup?

An endpoint is any device used for producing, sharing, accessing, and saving information and connected to a network. It can be a laptop, desktop, tablet, mobile phone, point-of-sale (POS) device, manufacturing machine, IoT device, etc. The safety and security of endpoints is extremely important because they can create vulnerabilities if they're not properly managed.

One part of effective endpoint management is maintaining remote, secure backups of the files and other mission critical data on those devices. Endpoint backup tools make this possible by sending copies of data to remote, secure file storage where it can be later recalled in the event of a disaster or deletion.

Endpoint backup vs. cloud

Cloud-syncing services (like OneDrive, Dropbox, or Google Drive) can't protect data from the wide range of potential threats that true backup solutions address. Data corruption, ransomware, and other types of malware will simply 'sync' right from the infected device to the remote storage location. Even if a user accidentally deletes a file, it will usually sync that deletion right into the cloud and remove all copies of the file.

Endpoint vs. datacentre backup

Many data centre backup solutions offer endpoint security coverage, but not all do. Some endpoint backup software can also provide comprehensive data centre backup coverage.

So, what is the difference? Data centre backup refers to solutions that are used as part of an organisation's disaster recovery efforts. These are large-scale backup solutions that you might associate with making backups of a company's entire operational database.

Endpoint backup refers specifically to the safe storage of backup copies made from 'endpoints' like laptops, desktops, phones, and tablets.

How does it work?

Endpoint backup solutions can range greatly in functionality but will generally pull data from a local hard drive or device and send secured, most likely encrypted, copies of that data to a remote storage location. What data is copied and how often is configured through the software itself.

The most effective endpoint backup plan would involve protecting every file on every device. In most cases this is possible without too much demand on resources, although large files (think media production) could put a strain on network stability if backed up frequently and in full.

The integrity of backups is a key factor to consider. Advanced endpoint protection tools will conduct automatic backup checks to ensure backups are verified for a reliable recovery, validating every backup, and providing a notification to IT if there are any issues.

Features of endpoint backup

There are many options when it comes to endpoint backup solutions. The right fit will depend on budget, resource needs, and how much freedom you need in configuration.

Self-service: because the modern workforce operates from different locations, a variety of devices and in multiple time zones, it can be difficult to offer responsive IT support around the clock. A great deal of strain can be removed even for larger organisations by incorporating self-service whenever possible.

Flexibility: effective protection often hinges on how well the software can be adapted to your unique needs, integrations, and technical specs.

Automation: process automation is essential to productivity and operational maturity. The more automation can be fit into a solution, the more effective your IT environment will ultimately be.

Resource optimisation: backups take storage space and bandwidth, regardless of what tool you use. Take notice of the options that offer bandwidth throttling, deduplication, network acceleration, compression, and other ways of minimising bandwidth usage and storage.

Do I need endpoint backup?

In a word, yes. In a recent State of Endpoint Security Risk report by Ponemon, 68% of IT/security professionals said that the frequency of attacks against endpoints had increased over the past 12 months. In addition, 51% of respondents considered endpoint attacks to be successful because their endpoint security solutions don't accurately detect threats.

Unfortunately, today's threat actors have developed numerous means for bypassing these traditional AV solutions, driving the need for more advanced endpoint security solutions.

Along with endpoint backups, other defensive measures should be put into place, such as:

- A means of application whitelisting
- Multi-factor authentication wherever possible
- Network access control
- Patch management software to ensure all assets are updated quickly
- Advanced anti-malware software

Even with all these solutions in place, endpoint management is not complete without an endpoint backup solution.

Conclusion

How we work has changed forever, and it has become routine for organisations to have employees and collaborators all over the world, compounding security challenges.

As such, endpoints are now one of the weakest parts of an organisation's network with over 70% of breaches originating from endpoints. That's why endpoint backup must be a key component of any security stack and choosing the best endpoint backup provider can make all the difference. ■

What would energy blackouts mean for cybersecurity?

Scott Goodwin, COO and co-founder, DigitalXRAID

The recent cold snap in the UK has provided a stark reminder of what conditions the winter months could bring. As with the rest of Europe, the country is experiencing an energy crisis triggered by Russia's invasion of Ukraine and subsequent sanctions imposed on the nation, made worse by Britain's reliance on Russian gas. As well as causing overheads to soar, UK organisations are also facing the prospect of blackouts, as warned by the National Grid. What's more, a lack of warning from the Met Office around the recent arctic blast is being blamed for even further strained energy supplies.

While energy blackouts pose obvious disruption to day-to-day operations that businesses will need to prepare for, it is also critical to consider the impact power outages could have on cybersecurity and what proactive protections organisations can put in place now.

The risk

The bottom line is organisations can be hacked during a blackout. One reason for this is that software-as-a-service (SaaS) platforms and servers are often hosted outside of a business' territory, meaning they would remain online and vulnerable to attack while an organisation experiences a power outage.

Additionally, many enterprises now rely on remote IT and security support following the widespread adoption of 'work from home' arrangements over the past two years. If a localised blackout were to be imposed, cybersecurity personnel could be cut off from their organisation, leaving it exposed and without a team to detect, monitor and respond to breaches. With bad actors better positioned to infiltrate an organisation's defences undetected, navigate through a network and exfiltrate more data, cyberattacks during blackouts are not just possible, but also have the potential to be even more destructive.

The solution

While the prospect of blackouts appears bleak, the good news is that there are a variety of ways organisations can prepare now to mitigate against the cyber risk of rolling power cuts.

Plan ahead

The National Grid has outlined that the most likely window for blackouts is between 4pm and 7pm. As with holidays and weekends, these more vulnerable periods are ripe for exploitation by cybercriminals. Knowing when outages may occur means attacks can be timed to have maximum impact. It would not be surprising if bad actors were to breach a network ahead of a blackout window, lie dormant in blind spots and then deploy malware once a power outage has been imposed. However, equipped with this knowledge, organisations who rely heavily on remote cybersecurity and IT support can consider bolstering their onsite taskforce during periods when blackouts are most likely to occur.

Go back to basics

In times of heightened cyber threats, it is always best practice to make sure you are covering the basics. Maintaining good cyber hygiene and ensuring security is front of mind for all staff is essential. This can be aided with regular phishing training and simulations – especially important considering phishing is now the most common threat vector for UK organisations – and security notifications for staff ahead of vulnerable periods like blackout windows.

At the same time, it's also vital to evaluate worst case scenarios. Updating business continuity plans (BCPs) and carrying out disaster recovery planning will identify existing vulnerabilities and new anomalies and risk factors that can be patched ahead of potential blackouts.

Work with the experts

For complete peace of mind, organisations may consider working with third parties to further support their cybersecurity strategy. Outsourcing to a trusted security partner is an excellent option for businesses who lack sufficient in-house expertise. Security operations centres (SOCs), for example, can provide 24/7/365 threat monitoring capabilities and the aggregate value of experienced cybersecurity professionals with extensive knowledge of the threatscape.

The threat of blackouts is indiscriminate, and therefore SOC services are also at risk of power cuts. While they will be preparing by ensuring power banks and back-up generators are on hand, it is also pertinent that organisations who rely on third parties have an open and transparent discussion with their cybersecurity providers about the potential risk. By having these conversations, organisations will be reassured that all eventualities have been planned for.

Looking ahead

The cyber risk of blackouts is something that will be a cause for concern across UK businesses. However, acting now, implementing proactive measures, and seeking additional support to mitigate against the fallout of a localised or nationwide blackout will put organisations in a much stronger position for the coming months. ■

The evolution of SD-WAN for enterprise applications

Is SD-WAN the future of enterprise networking, or is it already old hat? Amy Saunders checks in with those in the know

"Software defined wide area network (SD-WAN) is the first real-world implementation of software defined networking (SDN), which emerged a decade ago," says Marc Cohn, principal technology strategist, Spirent.

While it's not exactly new, "it's only in the last two years that SD-WAN has largely been considered the go-to technology for networking – and for good reason," states Anthony Senter, CEO, SDWAN Solutions Limited (UK). "As applications move to the cloud, backhauling traffic to a data centre first (as with MPLS or VPNs) is counterproductive for offices and remote workers. Relying on a single connection for all traffic is also unwise, as is using static routes and being at the mercy of a network provider to make changes."

Dave Greenfield, director of technology evangelism, Cato Networks, agrees, stating that SD-WAN addresses the high costs of MPLS compared to internet capacity while delivering enhanced agility: "an SD-WAN device can be deployed in minutes and getting an internet connection will take days and weeks. The provisioning of an MPLS connection can take months depending on location, if MPLS is available at all."

Introducing dynamic networking

For the modern enterprise, SD-WAN can dynamically route traffic, per packet in best scenario, using all available bandwidths, and dependant on the specific application priority and requirements. Moreover, SD-WAN enables the WAN to be tailored to support applications independent of the underlying WAN connectivity technologies and provides a common management front-end to offer single-pane-of-glass operations.

SD-WAN can essentially combine different technologies such as broadband, WiFi and cellular connections as well as firewalls and security functionality, all managed by a SD-WAN central controller. "When you bring all that together, you're not just getting the sum of all the components, you start to get a multiplying effect and achieve greater application performance," says Martin Saunders, product director, Highlight.

While originally envisioned as a campus interconnection technology to virtualize the WAN, SD-WAN has evolved into the cloud connectivity option of choice. As the global workforce rapidly moved to working from home during the COVID-19 pandemic and is now settling into a hybrid model, "SD-WAN is evolving again as the means of providing secure, multi-cloud connectivity," says Cohn. "Since cloud is here to stay, and typically will be deployed in the hybrid model, SD-WAN is a critical technology, especially as employees return to the campus for at least a portion of the workweek."

SD-WAN vs VPNs and MPLS

SD-WAN, virtual private networks (VPNs) and multiprotocol label switching (MPLS) are common WAN technologies, but how do they compare?

"While MPLS and VPN provide relatively low-level connectivity, SD-WAN has evolved to provide policy-based, application-level connectivity in the multi-cloud environment," explains Cohn.

MPLS continues to grow because of its ubiquity, ability to scale and bandwidth efficiency, asserts Cohn. While MPLS does not encrypt user traffic, the predominant use case is for private connectivity (which is fully isolated from the internet), which is inherently secure.

"Like SD-WAN, VPNs provide an overlay that may reside on top of distinct WAN connections. However, VPNs provide relatively low-level internet connectivity that is more complex to manage, less secure, and less flexible than SD-WAN, which can provide application layer connectivity over any VPN," adds Cohn.

SD-WAN will replace VPNs and MPLS, agree Greenfield and Senter. "The only companies still promoting VPN and MPLS above SD-WAN technology are those that have either high MPLS revenues to protect or do not have the skillset and expertise to be able to offer true SD-WAN and SASE solutions," asserts Senter.

"SD-WANs can configure themselves and aren't faced with IPsec's capacity limitations," says Greenfield. "SD-WAN also allows you to build a mesh of tunnels that would normally be very difficult to provision and create with VPN alone, where the network becomes very brittle. If one 'tunnel' breaks, there's no failover and no traffic control."

VPN and MPLS are both 25+ years old technologies: "VPNs need constant handholding, can only use a single connection, give all or nothing access which goes against zero trust methodology. VPNs cause an average of 30 minutes a day downtime for 90% of WFH staff," says Senter. "Similarly, MPLS performance can be replicated with a properly designed SD-WAN solution, while offering so many more business and productivity advantages. If you are currently running an MPLS only network, cost benefit alone should be enough to convince you to make the change."

An incomplete picture

With dozens of product and managed services offerings, a variety of security features, and a wide range of management capabilities, SD-WAN solutions vary significantly.

"Each SD-WAN vendor technology offers different benefits and use-cases," explains Senter. "From those that are SD-WAN in name only and offer basic failover functionality to those that provide superior technologies and benefits. Choosing the correct vendor solution for your business all comes down to the functionality you require, what your applications and users need and your budget."

"Enterprises need to have a clear understanding of their specific network requirements," agrees Saunders. "Many enterprises will not have this level of expertise inhouse and it is worth working with an organisation such as The Network Collective. They help companies to understand and document their network needs both now and in the future."

However, SD-WAN alone is not enough to meet today's networking challenges. "In the midst of the COVID-19 pandemic, SD-WAN vendors rapidly repositioned themselves as secure cloud connectivity suppliers based on the dramatic shift in the workforce," says Cohn. "A glance at the market leaders reveals fewer references to SD-WAN. Instead, one will find secure access service edge (SASE), zero touch network access (ZTNA), among other security functions."

A recent SD-WAN report from GigaOm reviewed 19 notable vendors and discussed the importance of considering SD-WAN as part of a broader SASE offering. As per Greenfield, SD-WAN was designed for an era where users and resources were predominantly located within offices.

"With hybrid work and the shift to the cloud, users and resources are no longer on premises. To access the cloud, SD-WAN devices need to be deployed in the cloud, which is not always feasible. Remote access is completely outside the scope of SD-WAN," explains Greenfield. "It's why Gartner and other analysts expect that in the future most SD-WAN purchases will be part of a much larger SASE strategy that pulls together sites, remote users, and cloud resources into one seamless network."

SD-WAN does not consider what happens when applications move from the data centre to the cloud, nor the element of security. Greenfield believes that SD-WAN is going to become a part of SASE, and will also include security, native cloud connectivity, and remote access all seamlessly converged.

"MPLS and VPNs were for organisations 10 years ago; SD-WAN was for organisations four years ago, but SASE will be for organisations moving forward," concludes Greenfield. ■

AI for networking – the time is now

AI is being lauded as the solution to modern network challenges, but is this the decade where every network gains a level of intelligence? Amy Saunders asks the experts

The first AI can be traced back to 1951, when Christopher Strachey developed a programme that could play checkers on the Ferranti Mark I computer. With the best part of a century under its belt, why is now finally the time for AI to join the network?

"Communications service providers (CSPs) have been under big pressure to cut operational costs, but until now they could get away with the traditional business and operational support systems (OSS/BSS) they use to manage the performance of their networks, while driving organisational and process transformations to improve efficiency," says Sasa Crnojevic, network AI & machine learning business principal, SAS.

Jamie Pitchforth, head of strategic business, UK & Ireland, Juniper Networks, agrees that businesses are now under increasing pressure to perform at a higher level. "As such, IT decision makers can use AI networks to reduce increasing cybersecurity threats and other organisational challenges like hybrid working," explains Pitchforth. "AI-based solutions can help to resolve the IT skills gap, allowing teams to work more efficiently with limited resources, and streamline processes to allow these resources to be allocated in the most effective areas. These solutions also facilitate the optimal user experience as issues are quickly resolved before working practices are impacted."

The rollout of 5G is bringing more complexity and greater operational challenges which will be impossible to manage without AI and network automation. Those challenges, according to Crnojevic, include network cloudification; network automation; network monetisation (B2B2X); network slicing; and transforming from multi-play operator to full digital service provider.

"Imagine a simple 5G service like network slicing, which ensures a B2B customer has dedicated bandwidth with a required service level agreement (SLA), based on which the customer will be charged. It is simply not possible to manage dozens or even hundreds of network slices without automation across all layers (radio, core, and transport network)," says Crnojevic. "That's why AI is a must. Not only for 5G, but also for legacy technologies to optimise operational costs and drive targeted capex investments."

"With the current economic pressure, AI is being used to boost efficiency, future proofing an organisation by saving time and money with faster problem resolution, fewer onsite technician visits, and more streamlined network deployment models," outlines Pitchforth. "To keep up with the development curve, IT decision makers will be required to implement AI technologies to maintain a steady pace with competitors."

Highlighting the boom in cybersecurity challenges for today's network users, Roman Tobe, product marketing director, global trust at RingCentral, states that "for security and risk management (SRM) leaders, the time to integrate AI for securing networks was yesterday."

But before a leader can use AI to counteract risks, whether they are from malicious AI or more traditional techniques, understanding the overall team competency needed to assess these solutions is critical. "This could mean having a team of data scientists, analysts, engineers, or developers who can build and maintain the infrastructure needed to support AI initiatives. To do this, there needs to be more experienced security personnel on hand to counteract increasingly sophisticated threats," explains Tobe.

Human vs machine

The discussion about humans being replaced by robots is widespread, with concerns that many thousands of jobs will be lost to self-scanning tills, driverless vehicles, etc. all making the headlines. Not to mention the inherent problems with today's technology, which remains in its infancy, causing frustration for end users – 'unexpected item in bagging area' anyone?

These fears have been amplified since the November 2022 launch of ChatGTP, which has captured the global imagination with the use of natural language processing. "People have rightly been left amazed by its capabilities," says Crnojevic. "But imagine adding other AI capabilities like computer vision, machine learning and deep learning, timeseries forecasting, streaming analytics. With all these tools we will be able to drive fully autonomous networks, or as CSPs define them, the 'holy grail' – 'zero touch, zero wait and zero trouble' services."

For the networking world, AI will deliver a huge leap forward. AI processing works in a fundamentally different way to a human brain and can process huge amounts of data without getting bored or tired. It works on patterns and quickly learns from mistakes so is better at delivering consistency.

Pitchforth asserts that AI enables better performance in networking; connectivity solutions have the uninterrupted speed and bandwidth to perform at the required level, despite variations in traffic. Moreover, "the repetition involved in AI-powered networks lead to a reduction in human error, avoiding unwanted lapses in security and service quality," he says. "Beyond the functionality of the network itself, AI solutions can also give better insights into how the network is performing and what it is being used for; increasing IT efficiencies, reducing support tickets, and decreasing main time to resolution, while transforming network operations from reactive troubleshooting to proactive remediation."

"There's a level of consistency that can be attained with AI systems that reduces the frequency of errors as well as the ability to introduce predictive analysis that prevents threats as they emerge," says Tobe. "Sound AI systems are also self-correcting, albeit with human analysts overseeing the model accuracy and maintaining the standards set by the organisation and end users. An example would be an attack on an AI/ML model itself, where malicious code could be embedded into the proprietary model. Machine learning security (MLSEC) would be the best and fastest way to detect this intrusion and correct any further damage from occurring."

"IT organisations must implement a solution that provides AI-driven operations with end-to-end visibility from the client to the cloud to optimise user experiences," says Pitchforth. "With AI technologies, enterprises can streamline and automate SD-WAN configuration, event detection, troubleshooting and capacity management. When a network team applies these capabilities to an SD-WAN deployment, it

can improve and protect user experience across a distributed enterprise."

Incorporating AI into the network enables a level of scaling and anomaly prediction that, coupled with the possibility to act in real time, before services are impacted, makes it a no-brainer.

Network incorporation

Rolling out AI onto the network is no easy task.

When updating legacy technology, IT decision makers may face resistance to the implementation of AI, often by teams who have misconceptions around these innovations and how they will be deployed in the business. "Digital transformation also requires investment, which can be difficult to come by in times of economic downturn," says Pitchforth. "However, many decision-makers now recognise the need to invest in AI for their business in the longer term."

Meanwhile, Tobe highlights the challenge of maintaining trust: "one of the tenets of good AI practices, for external experiences within the products themselves is explainability, which is making the end user aware of the AI and why it made the decisions it made. Meeting this challenge goes a long way in elevating the trust and confidence in the ethical and unbiased nature of the AI system."

As all network components must be compatible with each other, open and standardised APIs are key: "that's where you have organisations like 3GPP, TM Forum and GSMA working to help their members. Proprietary equipment and interfaces were very common in the past, especially among many leading network equipment providers," says Crnojevic. "Then we come to other things like analytics democratisation, which should allow business users faster access to insights through self-service, freeing data scientists to work on high-value initiatives like analytics development and digital transformation. Operators should also be mindful of GDPR and other privacy regulations."

Naturally, the advancement of an AI depends upon access to suitable data. "Successful AI systems need a large amount of high-quality data to be trained on, which depending on the endeavour, can be difficult to collect and maintain," explains Tobe. "Additionally, AI models are complex in nature and difficult for analysts to both interpret and decide on the appropriate response."

"Enterprises need to responsibly manage AI's growth with proper governance to stay ahead of regulation and minimise potential negative impacts. In Europe, regulators are starting to classify certain AI use cases as risky and requiring CE certification. AI regulation is changing quickly, and business leaders must make AI governance a strategic priority. Creating new regulations, setting up new governance frameworks or leveraging existing ones for entirely new technologies takes time, people, and capital," says Pitchforth. "Yet, if there was ever a technology worth the investment, it's AI. No matter what organisations spend today to build resilient AI governance structures, that investment will be trivial when compared to the resulting upside."

An automated future

Will we see a day when every network features AI? "Without a doubt the answer is yes - but not at 100% full automation," says Crnojevic.

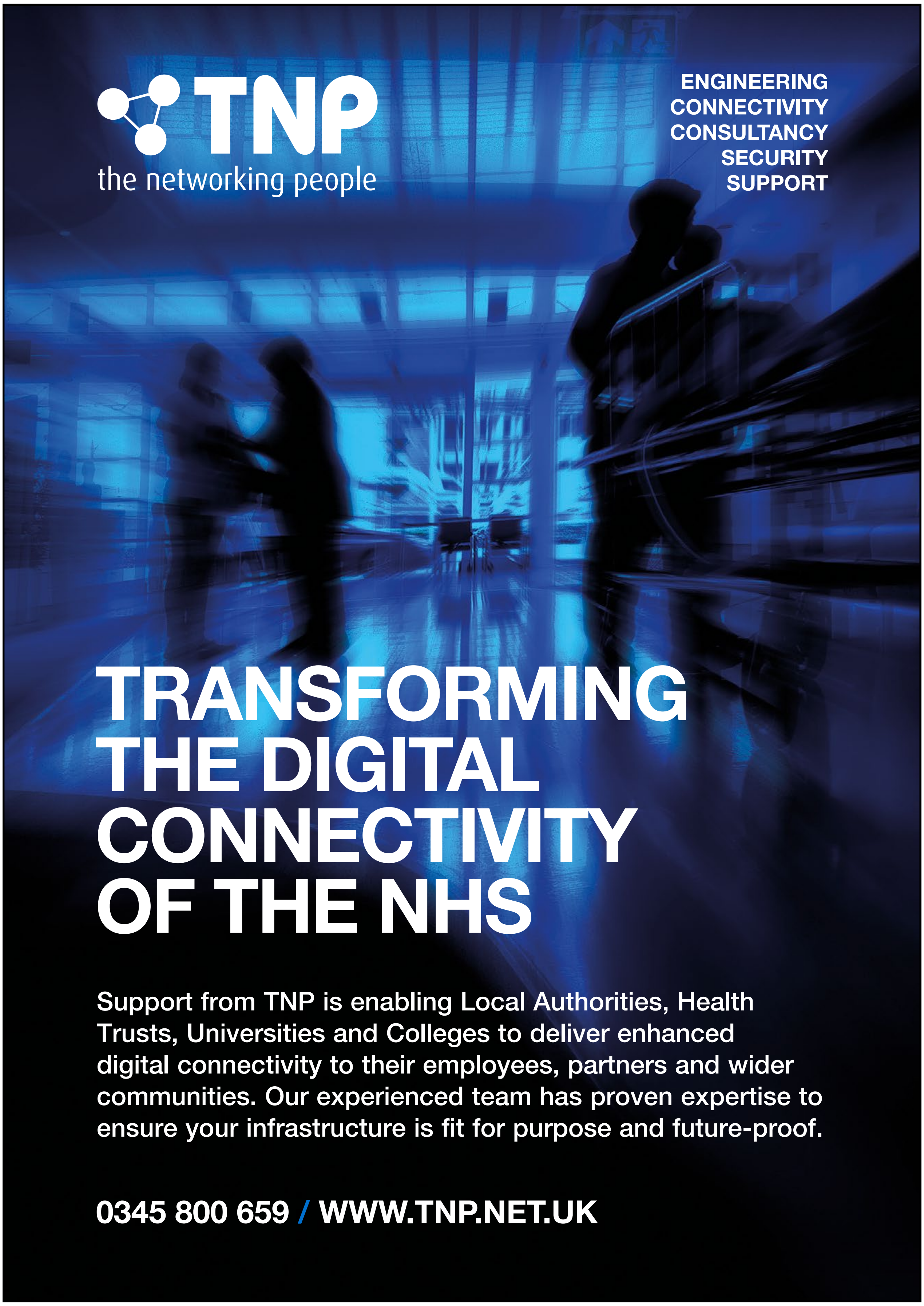
"It's almost a near certainty that by the end of the decade we will see AI in some form integrated into every network security system," agrees Tobe. "We will also see AI engineering and governance principles guiding these systems to maintain a level of trust and ethical standards."

It's widely anticipated that AI will become universal within IT networks. "The well-publicised benefit of AI creating the secure, self-driving, self-healing network is an exciting prospect for business leaders who have lived with the cost of network operations spiralling ever since the advent of wireless devices and cloud applications in the early 2000s," says Pitchforth. AI, machine learning and data science will underpin automation and optimisation to drive efficient secure networks with improved experiences.

"We are not too far away from this being reality, especially for greenfield networks which are not burdened with legacy architecture," says Crnojevic. "You will always need people to calibrate and configure the AI in the way we want it, or in a way that is regulated. People will also be needed to ensure full transparency, to explain why a certain 'AI system' took a decision to understand whether it was justified to do so."

The days of legacy on premise systems are limited "because software-defined cloud architectures driven by AI have arrived and their benefits are becoming publicised and realised. The key barometer suggests that the entire networking industry has pivoted towards AI, running on next generation cloud architectures," says Pitchforth. "AI networking adoption will further increase as IT teams and business leaders demand more for less. Some sectors where policy demands data sovereignty may become late adopters, but in the not-too-distant future, AI will become a new normal."

Crnojevic reports that he often hears the phrase: 'It is not AI which will replace people, but it will be a person using AI.' "It's therefore important to transform our current workforce into citizen data scientists. Domain knowledge sits with the end business users and not all the tasks will be repetitive and therefore easy to automate, however the level of efficiency needed will be impossible to achieve without the implementation of AI," says Crnojevic. ■



Halton Housing future proofs with IoT

More than 150,000 IoT devices are installed in tenants' homes by social landlords across the UK. This number is expected to hit 1 million devices by the end of 2024, bringing about a paradigm shift in landlords' efforts to comply with regulations and offer tenants a better understanding of their home environment.

An increasing number of future-thinking landlords, both social and private, are turning to the IoT for solutions. Smart boilers, connected fire alarms, energy optimisers, air quality sensors, and water leak detectors are the most commonly deployed. Some landlords are also exploring smart locks, advanced assisted living solutions, predictive heating controls and dozens of other technologies.

Councils across the UK are meeting significant challenges in the IoT rollout across housing stock, including poor internet connectivity, operational inertia, and consumer devices being inadequate for multi-property enterprise deployments. There is also a loss of value in not having data in one place for cross-analytics and insight.

Safety first: Halton Housing automates emergency lighting maintenance

Established in Widnes in 2005, Halton Housing is a not-for-profit Housing Association that own and manage over 7,000 homes. Halton Housing has led the charge in technology adoption throughout all sectors of the company with its 'digital first' approach. Underpinned by core values of transparency, honesty and innovation, the Halton team have fully embraced digital transformation to help support and improve the lives of their residents.

Automated building compliance

Halton Housing wanted to focus on moving away from manual testing of emergency lighting in their residential housing blocks. Spread out over a wide geographic area, testing of emergency lighting in each block required in-person visits to all lights, at all locations, every month.

Because of the huge number of resources needed to execute testing and maintenance, work was outsourced to a third-party contractor who carried out testing, inspection and repairs on their behalf. PDF certificates of completion were then sent to Halton Housing's compliance team.

Until then, connecting information to streamline their emergency lighting process was impossible because manual testing gave no indication of failures in advance. Technicians had to attend the site to complete routine testing and determine if there were any problems. If there was an issue with any light the next step was to order the part for replacement and at a later date return to site to complete the repair.

"Our emergency lights which didn't use LED bulbs failed frequently leading to countless hours wasted going back and forth replacing bulbs," said Lee Reevell, head of innovation & architecture, Halton Housing. "Another shortcoming we identified in the process was that PDF testing reports generated by our third-party contractor existed in a silo and didn't feed into any of our inhouse asset management systems."

After some discussion about the emergency lighting already installed in their buildings and the methods used to test and maintain them, Halton Housing opted to explore alternative options.

Future proofing with IoT

Halton Housing's journey with Safecility began with a demonstration of Safecility's Emergency Lighting Controller, leading to an on-site pilot of five devices.

"We've big goals when it comes to using IoT to help us pre-empt maintenance in our housing stock," said Reevell. "We've tried a number of different sensors to help us monitor different environmental conditions and also automate compliance testing and improve safety. Many of these sensors work well but can be techy and difficult to set up. Safecility couldn't be more different - we simply plugged the sensors in and instantly had an automated emergency lighting testing system without any complex set up or extra wiring."

By taking an active rather than passive approach to emergency lighting, failures are highlighted in real time and remedied quickly.

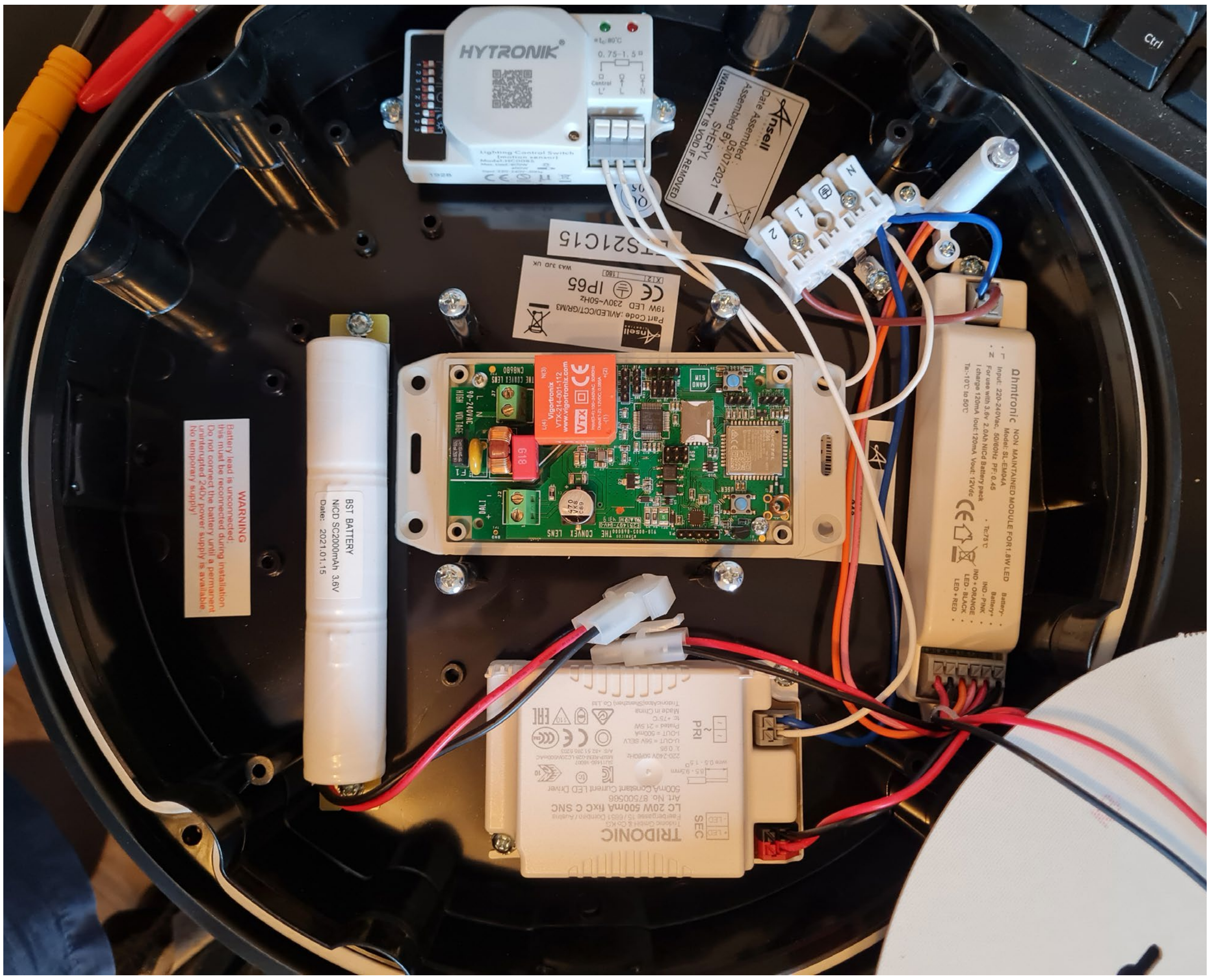
Automated testing has made managing emergency lighting compliance significantly easier.

"Safecility's sensor sends information directly to a software platform where bulb or battery failures are flagged without having to attend the light in person," said Reevell. "This saves double or triple visits to repair lights and prevents any failures slipping through the cracks. It allows us to be completely confident in the knowledge that nothing has been missed. That we're fully compliant and our residents are as safe as can be."

Key benefits of the solution include eliminating unnecessary site visits, the ability to view all pass and failure information for the emergency lighting on a single screen and having full confidence in compliance and safety status.

Safecility is infinitely scalable and can be stored in one building or one thousand, with no extra wiring or gateway installation required.

Other compliance sensor solutions like Legionella monitoring are also available. Results can be streamed directly to the Safecility platform, or via an API to other building management systems. ■



IoT: Stirling Council enhances social housing

Testing the waters

Back in 2018, a pilot trial was enacted as part of a Scottish Government funded programme, CivTech, which aimed to drive innovation in collaborative and cost-effective technology across the public sector. Homelync (now part of Aico) began an IoT trial across Stirling Council's social housing stock to tackle many of today's challenges like fuel poverty – which causes thousands of deaths in the winter every year – and fire safety, CO2 emissions, air quality, and water scarcity.

Homelync joined forces with BT, BlueGreen, Verv, Smart Compliance and Conservation Labs to deploy an integrated IoT trial across five Stirling Council properties. Smart boilers, water leak detectors, connected fire alarms, air quality analysers, and energy optimisers were installed alongside the deployment of Homelync's IoT Gateway, which provided the internet connection for data to be passed to the cloud-based analytics platform. Insight was then presented in a unified 'process friendly' dashboard.

Data from the deployment was extrapolated to represent Stirling Council's total portfolio of approximately 5,500 properties. The analysis indicated that there would be net annual savings of £452,000 for the council by reducing the number of unnecessary visits, enabling preventative maintenance strategies, optimising investment, reducing voids and helping people to live in their properties longer. While also improving quality of life and reducing fuel poverty, the tenants would directly save £700,000 per year due to energy efficiency and damage prevention. The environment would benefit by a reduction of 1.3 million kg CO2 and saving 15 million litres of water. Through knock on societal benefits like NHS savings, wider society would benefit by a total of £5.4 million per year once the system is fully scaled.

There were, however, deployment challenges. Some devices were difficult to install due to space limitations and several supplier technologies were trialled to identify the most suitable for Stirling's assets. Some consumer devices required significant commercial and technical integration work before they could be deployed as enterprise solutions. Lessons were learned with regards to sensor placement, for example, air quality analysers must be strategically placed to give accurate readings.

"We've seen some interesting insights on these trial properties with several high-risk indications of condensation caused damp and mould; this has really got us thinking how we help the resident manage their environment better and discern if it is actually something inherent with the building performance," said Stirling Council.

50,000 devices

Following Aico's trial with Stirling Council, Aico has now committed to a wider rollout including environmental sensors to collect information around tenant's homes. Collected data will include temperature, humidity and carbon dioxide (CO2) gas levels, along with smoke detection sensors and will dramatically improve the health, safety and wellbeing of residents. Tenants will be able to take actionable measures from insights via a free mobile app and analytics portal.

Delivering more affordable housing and well managed energy efficient homes
Ei Electronics
aico
Ei1025
CO2, Temperature and Humidity Environmental Sensor
Ei1000G
SmartLINK Gateway
Ei1020
Temperature and Humidity Environmental Sensor

This is the first full rollout of a multi technology and sensors connected home solution across an entire housing portfolio stock and currently the largest UK social housing sector rollout, with 50,000 IoT devices being installed over the next ten years in homes managed by Stirling Council Housing Service.

Environmental sensors around the properties will alert the council in real-time and provide early warning of damp, mould, ventilation and any other potential issues, while helping the tenant to understand energy consumption levels with heating their home. In a time of fuel poverty, connected devices are emerging as a powerful tool ensuring social homes are healthy to live in and used in an energy efficient manner. Homes will also benefit from a significant fire safety upgrade and be equipped with connected smoke, heat and carbon monoxide (CO) alarms.

Having the ability to identify the least thermally efficient homes means that Stirling Council can take intelligence led decisions to target capital investment programmes at those properties.

"When considering our sustainability goals, the data generated will help us identify the least energy-efficient homes and take action," said Stirling Council. "It will also provide insight into the performance of properties that have been recently retrofitted to ensure they remain healthy environments to live in."

The Fuel Poverty Act (Scotland) also seeks to protect residents of all households but particularly those in rural, highland and island communities from facing fuel poverty. Stirling council have around 20% of its housing portfolio in rural areas.

By connecting all of its housing stock, Stirling Council will continue to make intelligence led and data-based decisions, enabling more efficient safety checks, identification of trends and improvements for planning staff, and property investment and budget decisions. It will also trigger preventative maintenance measures by alerting staff to early causes of deterioration in a property's environment.

"This technology helps us manage our housing stock through reliable data driven intelligence, take prioritized investment decisions and improve customer satisfaction," said Stirling Council.

Residents using the free app gain a view of the safety and health of their indoor environment. The app also provides advice and guidance on how to improve living conditions and live a healthier and safer life whilst reducing carbon footprint and saving money on energy. ■

Making food storage smarter and safer with IoT

Chris Potts, marketing director, ANT Telecom explains how IoT sensors enable food companies to automate processes and free up resource while providing 100% accurate and reliable real-time data 24/7, that helps provide peace of mind, reduces costs, and saves money.

Storing food at the correct temperature is crucial for food companies to protect the quality and integrity of food products. Food poisoning bacteria becomes inactive in the cold, and most are killed by heat. Controlling the temperature of food is an effective way of controlling the growth of bacteria, reducing the risk of food poisoning.

Fridges generally operate between 1°C to 5°C and no higher than 8°C. Naturally, freezers keep some foods for longer and so must operate below -18°C. Although, if these conditions aren't met because an appliance has a fault, for instance, and the food rises to a higher temperature for a sustained period (approx. 4 hours) then often it must be thrown away.

Therefore, to ensure food produce is safe to eat, companies must check and record the temperature of their fridges and freezers daily to ensure that they are working correctly; and that they comply with the food safety standards – HACCP in particular, which is an important safety measure to meet. However, the challenge is that often this process of checking compliance is executed manually with paper-based systems. This task is generally time consuming and an onerous burden on staff.

Solving this productivity and HACCP compliance challenge requires a fresh approach. Particularly in an economic environment where every penny counts. Food companies cannot afford to get caught out and waste food either – this is not good for health, the environment, and business.

> **"With all these capabilities, why would food companies not want to trial these systems, digitise their processes, reduce costs, and free up resources?"**

Temperature monitoring

Using sensor technology is not new to the industry, but a lot of traditional sensors are hardwired into equipment, making them difficult and expensive to install. Also, cables may need to be fed through seals in fridge doors when retro fitted. This isn't ideal as it can leave a gap that lets cold air out and warm air in, affecting the temperature of the appliance and the contents within.

Wireless sensors are far easier to install but they require connectivity. 2G, 3G, 4G and WiFi sensors aren't usually suitable either, as batteries don't last long, and many commercial fridges and freezers are like metal boxes that mobile signals can't penetrate. The better approach is to use wireless sensors based on LoRaWAN technology. These low powered, long-range sensors are ideal for measuring fridge/freezer temperatures as data can be transmitted up to 12km away (direct line of sight).

LoRaWAN's long range capabilities and radio wave signals permeate through seals in the appliances too, making it possible to cover large sites with a small number of 4G/LAN gateways that upload the data to a secure online portal for management to access. Batteries can last for many years too before they need to be replaced.

Threshold breaches and data analytics

When setting up an IoT sensor system and linking it to a cloud portal system, food companies can label each sensor as they like.

They can build out site maps and images to match sensors according to relevant appliances. This can provide management teams a realistic accurate map of sensors and fridges according to their operations. Since information is available online, teams can view data-led dashboards about site performance on mobile devices and laptops.

Historic information can be displayed in a chart form, showing how temperatures vary throughout the day, week, and month.

Attention can be drawn to anything unexpected or out of the ordinary that could affect food quality or safety. For instance, temperature monitoring thresholds can be set to notify staff if there is an issue that needs to be investigated. A team may wish to know if a freezer drops below –18°C for more than 5 minutes. Just having an awareness of this could indicate a fault with the appliance and affect food quality and safety.

> **"These early warning systems can help food companies to move the contents to another freezer to avoid food being thrown away unnecessarily, along with the huge expense of replacing all the contents."**

These early warning systems can help food companies to move the contents to another freezer to avoid food being thrown away unnecessarily, along with the huge expense of replacing all the contents. Furthermore, the online data collected by the sensor will provide 100% proof and peace of mind that any food moved is still safe to eat. Moreover, the data generated and tracked can also inform fridge and equipment maintenance strategies.

Reporting for HACCP

Typically, these newer and more digitally led approaches towards temperature tracking enable teams to standardise how data from sensors is stored within cloud systems and online portals.

This means reporting formats can be set up to meet business and HACCP reporting requirements. It also means traditional paper-based record keeping and manually inputting data to generate weekly/monthly reports for auditing and compliance purposes can be replaced.

These previous manual systems are often prone to human error and inaccuracies too, in comparison to today's more modern, automated, and digital systems.

Conclusion

Today, IoT sensor systems are affordable and easy to install.

They're also scalable and make it possible for teams to trial their use and start with a small number of sensors to test their effectiveness across a site. Additionally, many systems can also be integrated to monitor other conditions such as power (on/off) and energy usage of appliances – or even how often a fridge door is opened to assess the impact on the performance of a fridge and the effect on its contents. Monitoring for energy usage, for instance, can reduce energy bills significantly since a poorly functioning unit can consume 100% more energy than a well-maintained unit.

Manually monitoring and recording the temperature of fridges and freezers for quality, safety and compliance can be very time consuming.

It isn't always accurate and reliable. IoT monitoring solutions, using state of the art LoRaWAN sensors, are far more reliable and cost effective.

Continual monitoring provides insight on how temperatures can vary and help organisations to improve food quality. Early warning of temperature breaches helps food companies to move food fast, reducing waste and costs. Further, auto-generated reports enable food companies to fulfil compliance obligations efficiently.

The further, and final, question is: with all these capabilities, and the opportunity to execute accurate, cost effective and productivity enhancing processes – why would food companies not want to trial these systems, digitise their processes, reduce costs, and free up resources? ■

Collaboration happens at the speed of trust

Duncan Swan, chief operating officer, British APCO

British APCO held its annual conference and exhibition in March. It's interesting reflecting back on some of the key discussions around the planned Emergency Service Network (ESN) that will underpin public safety critical communications.

The update from the Home Office Emergency Services Mobile Communications Programme highlighted that they are seeking a new partner for the key MCX[1] elements – not just a mission critical app, but everything that sits around it to provide the service required by their public safety users. It's not a trivial ask and the Home Office were clear that this part of the jigsaw would require a consortia approach. It will take time to procure and will need to slot in alongside the other 60 contracts in the programme.

Which dovetails nicely with a quote I heard from a major manufacturer this week – 'collaboration happens at the speed of trust.'

There is so much that is true with that quote – and in the case of delivering ESN in the UK, it's not just about the consortia who are lining up to bid, but the Home Office teams managing the procurement and writing the requirements documents. How all the elements that go into putting a contract in place work together will determine how quickly a contract can be let, ready to be delivered. It needs collaboration; and to be successful and to be delivered demands trust.

So how is industry seeking to tackle the move to mission critical broadband as both standards and user thinking mature? There is no doubt that the approach by industry and users alike has morphed since the early days of the ESMCP. There is recognition that there is the need for unique expertise to design, develop and deliver these programmes of work.

In all areas of society, smartphones have become an extension of ourselves; they are a transformational tool. And in the case of critical communications, they provide a myriad of enhanced features that all help first responders and incident managers; improved situation awareness, team monitoring, emergency management, alert, telemetry and video.

It's no surprise then that industry is hiring new skills and talent to tackle the mission critical broadband challenge - business analysts are a key part of the team to ensure all facets of the user experience are understood and baked into the design. And that architects able to facilitate both System and Service integration provide the collaborative glue to bring everything together.

Whoever is leading such a consortium needs to develop partnerships with integrators, the mobile network operators (MNOs), device providers, communication control room suppliers and other key vendors. The needs of the critical communications community also diverge from the public and business users; MNOs who want to be involved need to recognise the change of paradigm for critical communication support. And there are different models that critical communications programmes are following to incorporate one or more MNO into their solution; the UK and France favour building out a thick MVNO (mobile virtual network operator), other jurisdictions are adopting a MOCN (multi-operator core network) approach.

But following a similar approach still has some fundamental differences in how availability and resilience are built in. In France, the RRF (Réseau Radio du Futur) has two core networks (Orange and Bouygues) with the ability for national roaming across all four MNOs 'just in case'; the UK ESN has just a single core network provided by EE. And looking beyond the radio access elements at overall business continuity and disaster recovery, both seek by design to eliminate single points of failure, have in place vulnerability management, seek to ensure threat prevention and detection, and provide security and crisis management.

There are differing approaches being taken to rolling out a national mission critical broadband network, with the majority following a phased programme that recognises co-existence of current technology for some time. Timelines vary; supplier combinations too; and even where significant progress has been made to date, the key players continue to evolve their involvement and scope.

When a programme is asked to confirm their delivery timelines it should be remembered that 'collaboration happens at the speed of trust' and until you have all of the collaborating parties in place, whilst you may be able to define the journey, it simply is not possible to say when you will arrive at your destination. ■

[1] Mission Critical Services (Mission Critical Push-To-Talk - MCPTT, Mission Critical Data - MCData and Mission Critical Video - MCVideo, collectively known as MCX services)

Navigating the NAS market

Sergei Serdyuk, VP of product management, NAKIVO

Network-attached storage (NAS) systems have emerged as the go-to solution for storing and managing data in enterprise environments. A NAS system is a centralised storage solution accessed via network to store and share data as well as allows others to do the same.

Small, medium, and large businesses have different needs and requirements when it comes to NAS systems. These specifications may vary depending on performance, ease of use, encryption level, capacity requirements, cost, etc. There are many options, which can be confusing at times. So, how do we choose a suitable NAS system that meets your needs while remaining within your budget?

How to choose the right NAS

Based on our experience in enterprise data protection, we have compiled a list of recommendations that should help you choose the best NAS for your organisation.

Capacity needs

An enterprise-level NAS should have enough storage capacity to meet the organisation's needs. Start by identifying the speed at which your organisation generates data. Note that data growth depends on a multitude of factors, including relatively recent ones like regulatory requirements. In addition to the data growth rate, consider the number of sources from which the data is collected, as well as the size of your files. Then select a NAS with performance specifications that meet the demands of the enterprise.

Scalability requirements

As a business grows, data storage capabilities can get depleted quite fast. Whether your organisation is adopting new technology to digitise operations or growing its customer base, you can hit a storage bottleneck. This is why a storage solution that can scale as your organisation grows is important. Estimate how your storage requirements can change over time based on future needs. Then look for a NAS system that adds more storage capacity or adjusts performance without rebuilding the entire environment.

Performance characteristics

High performance is one of the key strengths of NAS storage systems. However, the enterprise setting poses some additional challenges. The equipment is expected to handle large numbers of simultaneous requests with as little delay as possible. In large organisations, every minute of downtime leads to substantial losses. To prevent this, your NAS should be able to handle the workloads and data access patterns of your organisation. Consider factors such as read and write speeds, IOPS, and RAID configurations.

Data protection

NAS devices are designed to provide a certain level of data protection out of the box. Built-in capabilities often include encryption, access controls, snapshot functionality, and backup capabilities, among others. However, these capabilities vary from device to device and may not suffice for enterprise needs. Check whether the NAS meets your data protection requirements. Keep in mind that leading vendors often integrate their products with data protection software. This option comes in handy if you need advanced data protection functionality.

System compatibility

Speaking of integration with other systems, ensure the NAS you select is compatible with your current infrastructure. It should be able to integrate seamlessly with your inventory to ensure smooth transition and minimise disruption. Check the network interfaces, operating systems, and applications used in your organisation. This information should help estimate how well the NAS fits into your environment.

Ease of management

An enterprise-level NAS should be easy to manage and maintain. Check whether the chosen solution has a user-friendly interface, provides automation options, and has remote management capabilities to simplify the management process.

High availability

Enterprises require a NAS that can operate continuously without interruption. Look for features such as redundant power supplies, dual controllers, and failover capabilities to ensure that your NAS is always available. On the software level, availability can be further enhanced with the replication and disaster recovery capabilities of the data protection solution used in combination with the device.

Support and service

Choose a NAS from a vendor that provides timely, effective support and regular software updates. You can check customer reviews and rankings on dedicated platforms.

Total cost of ownership (TCO)

Finally, consider the cost of the system. Look beyond the upfront costs and consider factors such as support and maintenance to ensure you get the best value for your investment. Keep in mind that the software you plan on using in combination with your NAS also adds to the TCO. Look for solutions with affordable and flexible pricing to keep costs low.

There is no one-fits-all solution. NAS is a versatile technology useful for a range of applications. With a solid understanding of your enterprise's needs and this list of recommendations, you can find the solution that works best for you. ■

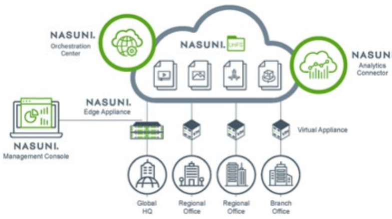
PRODUCTS

Nasuni delivers a file data services platform that leverages object storage delivering a simpler, lower cost, and more efficient SaaS solution that scales easily to handle rapid unstructured data growth. Nasuni, combined with Microsoft Azure, AWS, or Google Cloud object storage delivers a modern file infrastructure that spans any number of locations, eases administration, and costs less.

Nasuni's unique features are built on a cloud services platform backed by the largest, most available and secure object storage. Users need not worry about running out of capacity, backup capability, or reaching the limits of file sharing across the globe, and benefit from the ability to store and access unlimited files across any number of locations, without cloud latency or high data egress fees.

By eliminating the on-premises infrastructure required for legacy file servers, NAS, backup, and disaster recovery, Nasuni provides 40-60% savings over traditional architectures. By fully leveraging cost-effective cloud object storage instead of just tiering to the cloud, Nasuni costs significantly less than other cloud file data services solutions, too.

Nasuni provides cloud file storage for an unlimited number of sites from a single console, with capacity on-demand where and when it's needed and includes built-in backup and disaster recovery. With a design that accommodates cloud, hybrid cloud, and on-premises deployments, Nasuni replaces multiple data silos and toolsets with a single global file system that offers a 360-degree view of your file data, and a single platform that is easy to deploy and manage.



The **Dell PowerScale** is designed to be reliable at any scale - regardless of the kind of data, where it lives, or how big it gets, the data lake always stays simple to manage, simple to grow, simple to protect, and simple enough to handle the most demanding workloads of today and tomorrow.

New QLC drives for PowerScale offer optimum economics for demanding NAS workloads with massive raw capacity of up to 186Pb in a 252-node cluster.

With PowerScale, enterprises can choose from all-flash, hybrid and archive nodes for the best fit for the data. All-flash nodes accelerate demanding file workloads with extreme performance and efficiency, while hybrid nodes handle a wide variety of large-scale data workloads while lowering costs.

Archive nodes are the lowest cost way to support both, active and cold archives. Meanwhile, cloud services support AWS, Microsoft Azure, Google Cloud and Oracle cloud-based workloads with PowerScale.

The Dell PowerScale system can run multiple data protocols with simultaneous access to avoid storage silos and deploy as a NAS appliance, in APEX or in the cloud, a particularly useful feature for certain applications. Data management is fully scalable, up, down or out non-disruptively to tens of petabytes. Storage infrastructure can be managed with a single UI with CloudIQ.

Dell's PowerScale solution comes complete with built-in availability, redundancy, security, data protection and replication with OneFS, can protect from cyber-attacks with integrated ransomware defense and smart AirGap, and is designed for 6x9s availability.

Powered by NetApp® ONTAP® data management software, **NetApp FAS Storage Arrays** provides customers with a balance of performance and capacity. Optimized for easy deployment and operations, NetApp FAS systems deliver the flexibility to handle future growth and cloud integration. With highly available hardware and powerful software, FAS systems cost-effectively deliver the data protection, security, and scalability to safeguard data and help increase team efficiency.

With NetApp FAS, the enterprise can go from initial power-on to serving data in less than 10 minutes with provisioning for key business applications. Software or service storage can be upgraded during regular business hours with zero downtime. Operations can be streamlined via one unified system for SAN and NAS with proven storage efficiency.

NetApp FAS Storage Arrays, of which there are six versions for different use cases, help reduce costs with leading data reduction technologies and built-in configuration efficiencies, while protecting against data loss and accelerate recovery from local and regional outages. Critical applications stay online with continuous data availability, and business disruptions are eliminated. Each system can automatically tier cold data to the hybrid cloud, and avoid unauthorized data access and secure data at rest and in transit across hybrid cloud.

IBM Storwize V7000 is a virtualized storage system to complement virtualized server environments that provides unmatched performance, availability, advanced functions, and highly scalable capacity never seen before in midrange disk systems.

The powerful midrange disk system has been designed to be easy to use and enable rapid deployment without additional resources. Storwize V7000 is virtual storage that offers greater efficiency and flexibility through built-in SSD optimization and thin provisioning technologies. Storwize V7000 advanced functions also enable non-disruptive migration of data from existing storage, simplifying implementation, and minimizing disruption to users. IBM Storwize V7000 also enables the user to virtualize and reuse existing disk systems, supporting a greater potential return on investment (ROI).

Key features include automatic migration of frequently accessed data to high performing solid state drives (SSD); provisioning support for business applications that need to grow dynamically but consume only the storage space they are actually using; migration capabilities that provide efficiency and business value in a non-disruptive migration; support for near instant data copies for backup or application testing; integrated instant copy capabilities for critical business needs; and integrated tools and capabilities for server and storage management.

“ Please meet...

Martin Saunders, product director, Highlight

Who was your hero when you were growing up?

I love science and space and was fascinated by the moon landings from a very early age. So, my heroes growing up were Neil Armstrong, Buzz Aldrin, and Michael Collins. I still love watching any moon related documentaries and films, particularly the 1990s Dark Side of the Moon.

What was your big career break?

There have been a number of key phases in my career. My very first job was when I joined Easynet in 1996 at the age of 18 as a technical support agent. This was originally intended to be a gap year, but I loved it. I went to university for three months but returned to Easynet. The lucky break was that they took me back and I got wrapped up in their networking systems team in the brand-new and exciting internet industry.

Career break number two was again at Easynet in about 2000. I was working as a presales solution architect and decided I wanted to create my own products. My first offering was a VPN managed firewall product, which now looks alarmingly similar to the SD-WAN products of today.

The third break was much later at Claranet when I was promoted to the role of technical director. This was a huge opportunity to broaden my experience and where I had the good fortune to work with a large team of very talented and highly skilled technical engineers.

Joining Highlight in 2017 has given me the opportunity to combine all this experience and show how Highlight can help both enterprises and service providers achieve the best outcomes from all their networking services.

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

I wanted to be a sound engineer. I was heavily involved in my school’s theatre productions, but rather than being an actor I was always interested in the sound area. For a short while I did start my degree in engineering and acoustics at Southampton University, but the networking industry had captured my interest and imagination.

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

I’d love to have met Alan Turing. I think he would be a fascinating person to talk to, although at the time he was so misunderstood and mistreated that I doubt we’d talk much about computing or science! To be honest I don’t tend to hold much regard for modern celebrities, I’d be far more interested in talking to a refugee to understand what’s happened in their life and how we can learn from it.

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

‘Start a pension as soon as you can’ was the valuable advice given to me at 18 by an excellent head of finance at Easynet. Another bit of advice he gave me has proved extremely useful over the years. It was to ‘never let systems get in the way of good business’ – so if you can solve a customer’s problem, you can always fix the systems later. At the time, he was talking about the complexity of billing systems.

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

I’ve been running The Level Up Laptop Appeal since 2019, so if I wasn’t working for Highlight, I’d focus on making this a much bigger thing.

I set up the appeal during the initial Coronavirus lockdown when I began hearing that schools in my local area of Horley, Surrey were losing touch with large numbers of students because they didn’t have anything to study on at home. Through my industry connections, I have been given old laptops and computers and once refurbished, the devices are sent to the disadvantaged children.

To date, we have donated 2,000 laptops.

This work is very rewarding, and whilst still in the tech industry, I would give it my full attention with greater focus on helping young people and particularly young girls in STEM education. Gender stereotypes are still a major issue, and I believe it is preventing many young girls from entering a career in science and engineering.

The Rolling Stones or the Beatles?

Beatles, 100%. Love Me Do is a current favourite mainly because my son is learning it on his guitar for GCSE music. I Feel Fine and Day Tripper are my other favourites.

What would you do with £1 million?

I would push forward with my Level-Up Charity and really make it happen, that’s what I’d do. ”