

NETWORKING+

IN DEPTH:
SD-WAN,
p7-8



Running the network hot!

Bringing the puzzle pieces together

Martin Saunders,
Highlight, p5



Critical communications

When networks go down

Duncan Swan,
British APCO, p14



Questions and answers

I am worried about the erosion of freedom

Stewart Laing,
Asanti, p16



Ensuring business continuity when disaster strikes



Within the last month, two IT catastrophes have rocked the world. On 19 July, global TV channels, transport networks and banks were knocked offline in a massive outage causing Windows computers to suddenly shut down; a CrowdStrike update was ultimately identified as the source of the error. Then on 30 July, another widespread outage affecting Microsoft 365 and Azure services was reported; this was initially blamed on a VMWare update, but later attributed to complications from a DDoS attack.

The impact on organisations was significant. OAG, a provider of digital flight information, reported that the world's 20 largest airlines cancelled nearly 10,000 flights between 19-21 July. Digital banks and financial companies also struggled to serve their customers during the outage; Visa received more than 64,000 user reports on 19 July compared to its typical daily average of just 1,500. The NHS' healthcare platform EMIS was adversely affected, leaving many GPs unable to make appointments, prescriptions, or receive test results.

The outage showcased just how vulnerable today's networks are to software glitches and updates.

"The CrowdStrike situation is a reminder that delivering software quality at scale is

incredibly difficult," reports Greg Notch, chief information security officer at Expel. "While it's easy to pile on the criticism, the security industry and its customers should take this opportunity to reflect on our own practices and review our threat models to ensure that when things like this happen in the future – and they will – we have prevention and resilience strategies in place to mitigate the impact."

Jack Porter, public sector specialist at Logpoint, warns of the risk associated with relying on single providers and complex cyber ecosystems: "long term, this has the potential to see such software dependencies regarded as an additional risk. Large cybersecurity vendors may now be included with the likes of digital service providers such as AWS, Microsoft and Google services as key suppliers by insurance companies as this has illustrated the devastating impact a security software failure can have."

Ultimately, this demonstrates the need for more robust and resilient solutions, so that issues can be resolved quickly without causing such widespread chaos.

"Preparedness is key – every IT and security vendor must have a robust system in place across its software development lifecycle to test upgrades before they are rolled out to ensure that there are no flaws within the updates," asserts Mark Jow, security evangelist, Gigamon.

According to Notch, one way for companies to help themselves avoid these situations is to diversify their security technologies: "adopting best-of-breed solutions for each organisation's specific needs and ensuring they integrate with each other is a huge first step in achieving that diversity and avoiding unnecessary risk. And if a company already has a comprehensive security platform in place, it would be in its security team's best interest to look at ways of reinforcing redundancy plans for when a software issue impacts their security capabilities. Resilience is a critical outcome security teams should be delivering and testing."


"Service Disruption Management (SDM) has emerged as a crucial tool for addressing these challenges, and these internal systems can be enhanced by integrating them with crowdsourced service disruption management (CSDM) solutions that can assess the scale of an outage and provide real-time information to affected users," adds Mark Giles, lead industry analyst, Ookla. "By integrating CSDM with existing network management systems, service providers can gain a more comprehensive view of their performance and take swift action to mitigate the impact of service disruptions on end users. Identifying priority areas allows for a more coordinated response, minimising impact and protecting the company's reputation." ■

QNAP® 1 Petabyte Storage Solution

1 Petabyte of Disks Included | 5 Years On-Site Support



TS-h3087XU-RP



TL-R2400PES-RP



University of Dundee implements HID Mobile Access

The University of Dundee is updating its city campus estate implementing HID Mobile Access and signature HID Signo readers throughout its buildings to guarantee it has a modern, secure and reliable access control system to allow staff and students to enter using both RFID cards and smartphones.

The project will involve buying and installing new mobile-ready HID Signo readers at around 40 buildings – a staged rollout being completed over a two-year period by specialist security installer, Scottish Communications Group. In addition, the University has purchased 10,000 HID Mobile Access licenses to offer its academic community the option to use their Apple and Android smart phones for touchless entry into its facilities.

“We wanted a modern system which is safe, secure and easy for everyone to use,” says Colin Stebbing, the University’s head of precinct services. “Complying with forthcoming legislation was also another important project requirement. With bills like Martyn’s Law soon to be enacted, ensuring the University is ready for this was important given that we have a duty to protect to ensure everyone is safe. The HID solution enables us to not only lock down buildings immediately, but it has built-in functionality which we can leverage over time, meaning we’ve invested in ‘future proof’ equipment which will last us long term.”

The new HID Signo readers integrate with the University’s existing AEOS access control software from Nedap. Supporting both native Bluetooth® and Near Field Communication (NFC) connectivity, they allow touchless smartphone entry and are fast to install as the wiring uses common protocols like OSDP [Open Supervised Device Protocol] and Wiegand. Furthermore, existing access cards already in circulation can be used with the new HID Signo readers thereby speeding up the rollout.

Historically, the University used to print and issue plastic RFID cards so staff and students could access buildings. This process was laborious and time-consuming, especially during peak times like Freshers Week, when some 2,500–3,000 undergraduate and postgraduate students enrol. Issuing cards was logistically complex due to the high demand and the need for thorough identity checks, which could take up to 10 minutes per card.

Shifting to HID Mobile Access – which utilizes cloud-based HID Origo management software integrating with

the AEOS system – completely changes this and delivers wireless credentialing. This significantly simplifies all the licensing, allocation of credentials, setting of building access rights, validating or revoking of IDs – all of which is now done virtually and remotely.

“Once registered by Student Services in AEOS, a student simply gets an email to their phone, they tap on a link, the app automatically uploads and a mobile credential is granted,” says Paul Brady, HID’s end user business manager for physical access control solutions. “Not only does this improve the overall student experience because it’s substantially quicker and more efficient, but it’s far more sustainable as you’re not issuing PVC cards anymore.”

“We recognize that some visitors and staff still want to use a physical pass and not all employees have a university issued mobile credential,” said Stebbing. “HID Signo readers allow us to run both credential types in tandem, with HID Mobile Access giving us the option to scale up to include digital wallets from Apple and Google, as well as integrate with digital campus cards should we decide to go down this route in the future.”

Given RFID cards are still required today, the University of Dundee utilizes its reliable FARGO DTC4500e printers to back up this transition to digital transformation. The FARGO range of ID card printers integrate easily with the AEOS software so that Student Services staff can easily issue physical IDs themselves.

“HID Signo readers are going in now across the main buildings including the new Innovation Hub site,” says Stuart Leslie, Scottish Communications Group’s director. “HID’s reputation is built on reliability and security with its solutions supporting the latest encryption, communications and authentication standards. Their devices have an open architecture so they’re easy to install and integrate which reduces the cost for the university and makes time to value that much quicker.”

In addition, Scottish Communication Group is supplying Motorola MOTORTRO Ion smart radios to the University’s security staff. The radios will be configured to run HID Mobile Access so they can open doors fitted with the new HID Signo readers. Because these smart radios also link to the University’s CCTV, alarm systems and CriticalArc Safezone App, security staff need carry only a single device to fulfil their duties. ■

Leicestershire’s GigaHubs project connects 43 public sector sites

Leicestershire County Council’s (LCC) recently completed £1.5 million GigaHubs project has now connected 43 public sector sites (schools, libraries etc.) to a new gigabit-capable full fibre broadband network, which forms part of the UK Government’s wider £5 billion Project Gigabit programme.

“This is a real feather in our cap and great news for our rural areas. I’m delighted we’re one of the first

counties to complete the roll out, which means more children can benefit from cutting-edge digital resources, creates new opportunities to bring communities together and encourages commercial suppliers to bring the fastest speeds to more places,” said Councillor Pam Posnett.

Newly connected public sites include libraries, schools, waste sites, recycling centres, and council offices. ■

Westminster to become ‘safer city’ with new CCTV

North is helping Westminster City Council create safer communities through the deployment of a state-of-the-art CCTV network.

As part of a contract worth £1.2 million, North is initially deploying 100 cameras across the city to support the Council’s campaign against anti-social behaviour and crime.

The new CCTV cameras feature specialist audio and noise detection AI technology. This will alert operatives to loud noise complaints, ensuring real-time responses to potential incidents and providing immediate access to supporting footage.

The new surveillance system will feed into and be monitored at Hammersmith & Fulham Council’s (LBHF) control centre, with Westminster City Council investing a further £150,000 to support the collaboration. This includes investment made into new specialist equipment and has created five new full-time roles for system operators and a CCTV manager to drive community safety.

By working collaboratively with LBHF, it reduces operations costs for Westminster City Council, effectively using public money and allowing the team to gain specialist knowledge and experience. North also supports this control centre, which was part of a £5 million contract to upgrade its CCTV operations since 2020.

This has already created seismic benefit for safety within the community, with LBHF reporting that the upgraded CCTV and control centre has supported more than 500 arrests in 2023.

“We are delighted to be working with Westminster City Council to deploy leading public space CCTV technology that will create safer and smarter environments for residents,” said Andrew Foster, managing director for public services at North. “This flagship project is a great example of collaborative working between local authorities, with the new CCTV network feeding into Hammersmith and Fulham Council’s innovative control centre. Enhanced

public space CCTV is a vital intervention in the effort to make public spaces safer to live in and visit. The project serves as a prime example as to how Westminster City Council is making effective use of resources whilst prioritising the safety of its residents.”

“By implementing and feeding AI-based audio camera technology into the Genetec advanced security platform, Westminster City Council will operate one of the most advanced CCTV networks in the UK. This is strengthened through its partnership with LBHF which by sharing a control centre, will enable the neighbouring councils to collaborate on insight and resource, which ultimately will further improve safety and accessibility,” said Tony Oliver, head of physical security, at North. “North’s ethos is rooted in making communities smarter and safer, and we’re really excited to welcome Westminster City Council as part of this journey.”

The new surveillance system will be the first time Westminster City Council has run its own public realm CCTV cameras since 2017 when the previous network was closed and one-off capital funding was given to the Metropolitan Police to acquire its own cameras. While police-run cameras will continue to monitor pan-London hot spot areas in the West End and Covent Garden, the new council system will concentrate on addressing problems that most affect local people.

“Anti-social behaviour and crime in our communities blights the lives of residents across Westminster and as a Council we want to do what we can to help tackle it. This new local CCTV camera network will help keep an eye on ASB hotspots in local communities across the city, assist the police in identifying wrongdoers and provide the evidence to support work to design out crime,” said Councillor Adam Hug, leader of Westminster City Council. “The safety of our residents is of utmost importance, and we want to play our part in helping keep our streets safer and to ensure that residents feel more secure in their own homes.” ■



EDITORIAL:

Editor: Amy Saunders
amys@kadiumpublishing.com

Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Dave Walker, Martin Saunders, Dogu Narin, Dominic Norton, Phil Beecher, Duncan Swan, Stewart Laing, Martin 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

© 2024 Kadium Ltd. All rights reserved.
The contents of the magazine may not be reproduced in part or whole, or stored in electronic form, without the prior written consent of the publisher. The views expressed in this magazine are not necessarily those shared by the editor or the publisher.
ISSN: 2052-7373

UK misses £57.2 billion annually due to skills shortage

A chronic data skills shortage has developed across the UK, costing the country £57.2 billion every year, according to new data from Multiverse Skills.

It found that workers, on average, spend 14.3 hours each week on data tasks including data entry, analysis and report generation, taking them away from high value tasks.

The Multiverse Skills Intelligence report highlighted that workers feel they are wasting 4.3 hours a week on data tasks on average, equating to 10% of their total working time.

The report also found that staff are relying on Excel for the majority of their data tasks, with many lacking

understanding or avoiding tools such as Python.

“In challenging economic times, building a national talent pipeline of candidates equipped with the latest digital skills is crucial to boosting the jobs market and driving growth. Companies need tech talent in order to thrive, and currently many businesses are struggling to recruit and train candidates in core areas such as data analysis, automation and predictive modelling,” said Derek Mackenzie, CEO of Investigo. “With the severe lack of data skills across the UK workforce costing the country £57.2 billion per year, nearly nine-in-ten business leaders believe their organisation has significant skills gaps,

and half of employees said they lack the necessary skills, it is evident that a much greater focus is needed on developing high skilled opportunities for future generations in the technology industry.”

Businesses are aware of the data gap facing their organisation, with almost nine in ten business leaders reported that their organisation is facing a significant skills gap.

“Building digital skills throughout the workforce is essential to the UK’s ongoing aim to cement itself as a global technology superpower. It’s clear there’s still a lot of work to be done, with 9 in 10 business leaders stating their organisation has a significant skills gap. Businesses need access to skilled

staff to maximise the benefits of their technology solutions, especially when it comes to the rapid development and adoption of tech such as AI, which rely heavily on data foundations,” said Sachin Agrawal, UK managing director at Zoho UK. “Solving the skills gap requires a collaboration between government, industry and education to identify the most in-demand skills, such as data, in order to build a pipeline of talent. Bootcamps focusing on key skill sets including data, cloud computing and software development can enable the next generation to develop sought-after skills, as well as help others to reskill and upskill in line with technology advancements.” ■

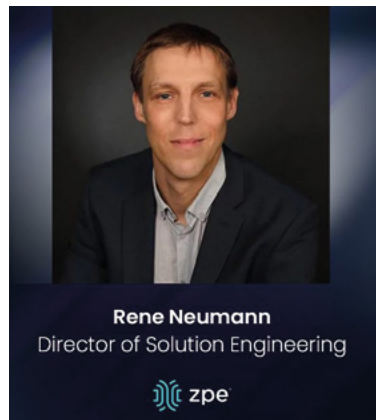
iomart to generate 250,000kWh of solar energy for Maidenhead DC

iomart has installed 560 solar panels at its flagship data centre in Maidenhead to reduce carbon emissions and enhance energy efficiency across its UK operations.

The solar panels are expected to generate around 250,000kWh of energy annually, offsetting around 96,061kg of CO2 emissions annually. The 2,800sqm Maidenhead facility is the largest data centre in iomart’s portfolio, which includes 13 data centres across the UK. It also serves as iomart’s main self-managed infrastructure hub, powering over 12,000 servers.

“We have already committed to powering all our data centres with 100% renewable energy. This installation at Maidenhead takes that commitment one step further, generating our own energy onsite, and in addition, the potential to export energy back into the grid network in the future,” said chief technology officer at iomart, David Gammie.

The project, delivered by 3ti and completed in May, uses the extensive roof space available at the Maidenhead site to maximise solar energy production. This installation represents a key component of iomart’s long-term goal to power all its data centres with renewable energy from sources like wind, hydro, and solar. ■



Why Securing IT Means Replacing End-of-Life Console Servers

The world as we know it is connected to IT, and IT relies on its underlying infrastructure. Organizations must prioritize maintaining this infrastructure; otherwise, any disruption or breach has a ripple effect that takes services offline for millions of users (take the recent CrowdStrike outage, for example). A big part of this maintenance is ensuring that all hardware components, including console servers, are up-to-date and secure. Most console servers reach end-of-life (EOL) and need to be replaced, but for many reasons, whether budgetary concerns or the “if it isn’t broken” mentality, IT teams often keep their EOL devices. Let’s look at the risks of using EOL console servers, and why replacing them goes hand-in-hand with securing IT.

The Risks of Using End-of-Life Console Servers

1. Lack of Security Features and Updates

Aging console servers lack adequate hardware and management security features, meaning they can’t support a zero trust approach. On top of this, once a console server reaches EOL, the manufacturer stops providing security patches and updates. The device then becomes vulnerable to newly discovered CVEs and complex cyberattacks (like the MOVEit and Ragnar Locker breaches). Cybercriminals often target outdated hardware because they know that these devices are no longer receiving updates, making them easy entry points for launching attacks.

2. Compliance Issues

Many industries have stringent regulatory requirements regarding

data security and IT infrastructure. DORA, NIS2 (EU), NIST2 (US), PCI 4.0 (finance), and CER Directive are just a few of the updated regulations that are cracking down on how organizations architect IT, including the management layer. Using EOL hardware can lead to non-compliance, resulting in fines and legal repercussions. Regulatory bodies expect organizations to use up-to-date and secure equipment to protect sensitive information.

3. Prolonged Recovery

EOL console servers are prone to failures and inefficiencies. As these devices age, their performance deteriorates, leading to increased downtime and disruptions. Most console servers are Gen 2, meaning they offer basic remote troubleshooting (to address break/fix scenarios) and limited automation capabilities. When there is a severe disruption, such as a ransomware attack, hackers can easily access and encrypt these devices to lock out admin access. Organizations then must endure prolonged recovery (just look the still ongoing CrowdStrike outage, or last year’s MGM attack) because they need to physically decommission and restore their infrastructure.

The Importance of Replacing EOL Console Servers

Here’s why replacing EOL console servers is essential to securing IT:

1. Modern Security Approach

Zero trust is an approach that uses segmentation across IT assets. This ensures that only authorized users can access resources necessary for their job function. This approach requires SAML, SSO, MFA/2FA, and role-based access controls, which are only supported by modern console servers. Modern devices additionally feature advanced security through encryption, signed OS, and tampering detection. This ensures a complete cyber and physical approach to security.

2. Protection Against New Threats

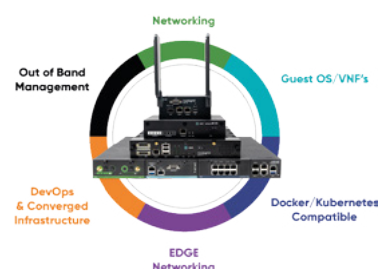
New CVEs and evolving threats can easily take advantage of EOL devices that no longer receive updates. Modern console servers benefit from ongoing support in the form of firmware upgrades and security patches. Upgrading with a security-focused device vendor can drastically shrink the attack surface, by addressing supply chain security risks, codebase integrity, and CVE patching.

3. Ease of Compliance

EOL devices lack modern security features, but this isn’t the only reason why they make it difficult or impossible to comply with regulations. They also lack the ability to isolate the control plane from the production network, meaning attackers can easily move between the two in order to launch ransomware and steal sensitive information. Watchdog agencies and new legislation are stipulating that organizations follow the latest best practice of separating the control plane from production, called Isolated Management Infrastructure (IMI). Modern console servers make this best practice simple to achieve by offering drop-in out-of-band that is completely isolated from production assets. This means that the organization is always in control of its IT assets and sensitive data.

4. Faster Recovery

New console servers are designed to handle more workloads and functions, which eliminates single-purpose devices and shrinks the attack surface. They can also run VMs and Docker containers to host applications. This enables what Gartner calls the Isolated Recovery Environment (IRE), which is becoming essential for faster recovery from ransomware. Since the IMI component prohibits attackers from accessing the control plane, admins retain control during an attack. They can use the IMI to deploy their IRE and the necessary applications — remotely — to decommission, cleanse, and restore their infected infrastructure. This means that they don’t have to roll trucks week after week when there’s an attack; they just need to log into their management infrastructure to begin assessing and responding immediately, which significantly reduces recovery times, for the complete blog click [here](#).



For more expert comment from ZPE Systems on the CrowdStrike outage, take a look at:

How to Recover Fast and Avoid the Next Outage

www.zpesystems.com

Unlock 1 Petabyte of ZFS Storage with Enterprise-Grade Speed and Reliability

For a long time, 1 petabyte of storage was seen as some mystical capacity, reserved for only the largest data centers and beyond the reach of most organizations. However, technological advancements have turned this once-distant dream into a practical reality. QNAP, a leader in network-attached storage (NAS) solutions, is making this possible with its latest pre-configured bundle, providing 1 petabyte of ZFS storage.

This impressive storage solution is built on QNAP's latest enterprise 24-bay rackmount NAS, combined with a 24-bay expansion enclosure. Both components leverage the power and reliability of Seagate EXOS 24TB drives, known for their exceptional performance in enterprise environments. The total configuration brings together a massive 1 petabyte of raw storage, harnessing the robustness and data integrity features of the ZFS file system.

QNAP's bundle is not just about storage capacity; it also addresses the needs for high-speed data transfer and future-proof networking. The NAS and its expansion enclosure offer 10GbE (Gigabit Ethernet) connectivity as standard, ensuring rapid data access and transfer speeds. For those requiring even faster connectivity, the system is designed to support up to 100GbE network interfaces, making it suitable for bandwidth-intensive applications such as big data analytics, AI development, and large-scale video production.

The inclusion of ZFS in this setup brings added benefits, such as end-to-end data integrity, efficient data compression, and powerful snapshot capabilities, all critical for enterprises that require not only large storage capacity but also data reliability and security.

In summary, QNAP's 1-petabyte storage bundle combines cutting-edge hardware with the robustness of ZFS, offering an enterprise-ready solution that was once considered a distant goal. Today, it is not just achievable but also optimized for modern, data-driven environments.

www.qnap.com

39% of UK companies ready to invest in 5G SA

New research from Vodafone disclosed that 39% of UK companies are ready to invest in 5G Standalone with 14% making the move within 12 months, demonstrating the immediate appetite for next-generation digital services. Further, 89% of businesses are looking to technology to improve the operational efficiency of their business in an increasingly competitive digital environment.

There is an immediate appetite for UK businesses to invest in both smartphone and advanced 5G services (such as network

slicing), with 93% highlighting reliable data connections as critical to success.

Existing 5G services rely partly on 4G; the 5G Standalone network, however, is a fully updated and future-proofed network that delivers many new benefits not previously available on 4G or 5G non-standalone.

"Our customers are telling us they are ready for 5G Standalone," Nick Gliddon, business director, Vodafone UK. "Whether it is to keep employees connected with more reliable services or to customise their business through next-generation services

such as network slicing. 5G Standalone is the doorway to innovation, new revenues, and better connection with employees."

86% of customers suggested the rollout of 5G Standalone is either important or extremely important, with 44% stating lower latency would help business growth, while 83% would slightly or significantly increase 5G investments once advanced capabilities are available. 46% believe 5G Standalone would offer them a competitive advantage within three years by better-enabling innovation. ■

CISOs: security teams unprepared for AI threats

Over half (54%) of chief information security officers (CISOs) feel their security team are unprepared for evolving AI-powered threats, as per new research from Absolute Security.

According to the NCSC, AI will 'almost certainly' make cyber-attacks against the UK more impactful, because threat actors will be able to analyse exfiltrated data faster and more effectively and use it to train AI models.

46% of CISOs believe that AI is more of a threat to their organisation's cyber resilience than a help, highlighting AI as a potential danger in safeguarding organisations from cyber threats, rather than strengthening cyber resilience. Additionally, 39% of CISOs have personally stopped using AI due to fears of a cyber breach, and 44% have banned AI use by employees at their organisation due to fears of a cyber breach.

"Our research has highlighted the significant danger posed by evolving AI threats, and we urge organisations to strengthen their cyber resilience structures to cope. As AI-driven cyber threats continue to advance in complexity, proactive measures are essential to safeguard sensitive data assets and mitigate the associated risks," said Andy Ward, VP international of Absolute Security.

"Although this report highlights how AI offers positive opportunities for organisations in terms of workforce development, updating and prioritising a policy of cyber resilience should be a top priority, not an afterthought. The repercussions of a breach, which can compromise both customer and employee data, can inflict irreparable damage. Therefore, organisations should focus on threat protection, deterring attacks, and preparing to defend against cyber threats. Achieving this requires clear visibility and effective control over networks, along with a robust framework to improve network supervision and establish a solid defensive stance. Organisations must leverage AI for competitive advantage, while simultaneously strengthening cybersecurity defences to prevent potential vulnerabilities."

On the other hand, a higher percentage of CISOs see AI in a positive light, with 77% of CISOs stating that AI has filled the cybersecurity skills gap. Furthermore, 85% of CISOs stated that their C-Suite has been sent on AI training courses. Accordingly, there has been a clear shift towards AI and a growing recognition of its importance in strengthening cyber resilience, with 83% of CISOs prioritising the hiring of AI experts over the past year. ■

Cabinet Office ponies up £6.5 million for remote working

The Cabinet Office, the ministerial department coordinating and delivering government policies, has injected almost £6.5 million in remote working technology to enhance digital infrastructure and support flexible working.

The research was revealed under the Freedom of Information (FOI) Act, and analysed by the Parliament Street think tank, uncovering the investment in remote working devices by the department for the

past three financial years.

A total of £6,411,133.30 was invested in remote working devices from April 2021 to April 2024, including laptops, tablets and phones. Laptops accounted for 87% of the overall expenditure, with the largest investment coming in FY21-22 to facilitate remote working following the pandemic. Tablets made up 12% of the spending, while mobile phones were only 1% of the spending. ■

Scottish trains to gain 'best WiFi' in the UK via satellite

The Scottish Futures Trust (SFT) will begin a year-long trial that will upgrade trains on the Far North and Kyle railway lines in the Highlands of Scotland with 'the best Wi-Fi experience of any train service' in the UK, enabled via low Earth orbit (LEO) satellite.

The project aims to start fitting the

new system during autumn 2024, with the service becoming available from December 2024 through December 2025.

Trains that run on these routes typically pass through some of the most intermittent and least reliable areas of mobile network coverage in the UK, which the new system could tackle – at significant expense. ■



Word on the web...

Adaptable networks: building resilience in connectivity

Dave Walker, customer solutions architect, M247

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





Running the network hot, hot, hot!

Martin Saunders, chief operating officer, Highlight

IT and network managers face considerable constraints on their budgets. With funds shrinking due to inflation and downward pressures to get more for less, many are reevaluating their network infrastructure. This is a good area to review particularly since 70-80% of many IT networking budgets are spent on the underlay connectivity such as Ethernet and broadband.

Running a network hotter may sound hazardous, particularly since any downtime is hugely expensive for an organisation. However, the latest IT observation tools for both the network and applications, alongside intelligent SD-WAN software, can bring all the pieces of the puzzle together and make it possible to run the network hotter without sacrificing performance or reliability.

Service observability platforms are key to understanding how much network capacity an organisation genuinely needs and where capacity can be reduced whilst maintaining a good quality user experience. With full-service observability, organisations can identify if something is starting to go wrong and then utilise proactive support processes to ensure there are no outages.

Bring on the heat!

Network capacity and performance are the first elements that need to be understood to deliver the best possible user experience at the most optimal cost. A large cause of cost inefficiency is when network connections

are either massively over specified and underutilised or they are underspecified and suffer performance issues at peak times. The former means overpaying and limiting the reach of budgets and the latter results in business operations being directly impacted by poor performance.

The problem when trying to 'right size' networks is that it can be difficult to properly measure and estimate network capacity requirements. This is where network observability becomes essential. Having a top-level view of different locations and metrics that show the performance and utilisation of all related connections over time is essential to making effective data-backed capacity decisions.

An extra source of headroom in SD-WAN

However, even when taking utilisation and performance trends into account using past report data, there are bound to be unforeseen events and new peaks that are difficult to predict. This is where technology like SD-WAN can come to the rescue.

The value of SD-WAN is its clever routing of traffic to the least congested route. Currently, most SD-WAN deployments are applying this intelligence to empty networks with no decisions to make. When organisations look to reduce the capacity of their underlay connectivity, deploying intelligent SD-WAN can be highly effective

and ensure the users' digital experience of their applications remains good.

The network isn't always to blame...

The next piece of the puzzle is the users' digital application experience and understanding if users are having a good or bad time. With business relying more and more on applications hosted in the cloud, it's important to distinguish between issues occurring because of the underlying network as opposed to problems with those cloud providers. This is especially true when running an optimised network.

Digital experience monitoring needs to be as unintrusive as possible whilst also being easy to deploy. The latest approach is to use agents with synthetic transactions that mimic a user accessing applications such as Salesforce, Amazon Web Services or Microsoft 365. In addition, organisations like Cisco ThousandEyes and Meraki are building agents into its equipment to capture application performance. These developments deliver a good indication of a user's digital experience when using the same network.

Unified service observability

If a network is going to be optimised, the speed of response is vital, particularly in fast-paced industries such as retail or finance.

The main problem is when managers use separate monitoring tools with isolated displays that present information in technical terms. It can then take valuable time and effort to identify if there is an issue and then translate the information into a form that can be understood by non-technical stakeholders.

Service observability tools that have easy-to-understand charts and diagrams enable managers to gain a fast overview of how the network, their application experience and SD-WAN are performing in one single informative view. It can show managers exactly where to direct their attention if something is about to go wrong with time to fix it. For example, Visionist, a provider of IT services to UK government departments, used the Highlight Observability Platform to double its visibility of a department's infrastructure and achieve a 60% increase in proactive detection of issues with faster resolution times.

By combining the insights of network performance, the digital experience and SD-WAN into one observability platform, managers can clearly identify if they can reduce the overall capacity on the underlay and perhaps replace an expensive Ethernet network with a mix of broadband and cellular connections, redeploying those funds to other important areas. Overall, it can give managers far greater control over the services they deliver to their users and how they manage their service providers. ■



Call us for impartial expert advice and pricing on these brands

[Contact us](#)

0345 899 5010



Specialist Suppliers of Leading Brands
























POWER (PDUs)

- Office
- Desk-Port
- Rackmount
- Intelligent IP / Data Centre

Do you need?

- Environmental Monitoring

COMPUTER CONTROL

- Desktop Switching
- Remote Access
- Secure Access

KVM

Server Control?



NETWORKING

- Racks & Cabinets
- Network Switches
- SFP Transceivers



CAT5e / CAT6

24/7 SUPPORT*

Free Advice

- Onsite Maintenance
- Installation Services

Solution Design



Unified SASE is the future

**Dogu Narin, VP of products,
Versa Networks**



As organisations have evolved throughout the cloud revolution, their networking and security needs have changed radically.

Secure Access Service Edge (SASE) consolidates networking services, such as SD-WAN, with security services, such as Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Leak Prevention (DLP), and other functions into an integrated solution that better enables organisations to support a broad set of use cases, including secure branch office connectivity, network access for remote workers, and cloud networking and data security.

The benefits the industry is realising from SASE are significant, including improved corporate agility by adopting a software-defined infrastructure; reduced security risk; and significant cost savings from fewer vendors, fewer devices and less complexity.

The race is on

Gartner predicts that by 2025, 80% of enterprises will have adopted a strategy to unify web, cloud services, and private applications access using a SASE/SSE (Secure Services Edge) architecture, up from 20% in 2021. One way to get a clearer view of the pros and cons of any given SASE solution is to understand if it has a 'bolt-on' or 'built-in' approach. We can broadly lump SASE offerings into three types:

Multi-vendor SASE: Some of these solutions have been created by third-party integrators who combine products from multiple vendors into a consolidated offering. A slight variation of this is found in offerings from a single vendor who has acquired or licensed and connected multiple technologies.

Single-vendor SASE: Several leading SD-WAN vendors have ramped up efforts to add a cloud-based security stack to their offerings to deliver a single-vendor SASE solution. And a number of SSE vendors have come from the other direction, acquiring SD-WAN technology to deliver single-vendor SASE. These 'bolted together' solutions are integrated across multiple products with different architectures and centricities, often creating significant challenges in terms of management, performance, and troubleshooting.

Unified SASE: Single vendor by definition, unified SASE offers an organic, purpose-built consolidated platform. This approach integrates all SASE components and functionality at the software platform level using one operating system to achieve single-pass architecture.

Why is a 'unified' approach better?

Unified SASE embeds security into the global fabric of a software-defined network, taking full advantage of the synergies between the two worlds to optimise latency, scalability, and performance in ways only possible when everything is built-in from the beginning as a single service.

The challenge for multi-vendor solutions is obvious – the lack of a shared platform fails to fully capture the simplicity and performance benefits of SASE. Similarly, many single-vendor and multiple-service SASE offerings that aren't truly unified SASE are immature and lack sufficient integration

to deliver on the full promise of SASE. These single-vendor approaches have, of course, different levels in their depth of integration, including:

1. Basic integration – products interoperate with each other through the creation of a tunnel or route, but lack broader data, management, unified policy engine, or visibility integration.
2. Data plane integration – products share information that can alter or steer traffic routing in an automated fashion but lack integrated management and visibility.
3. Management plane integration – one vendor product pulls relevant information about the other vendors' management planes to enable performance management and visibility.

Even non-unified single-vendor offerings that extend to management plane integration still have a bolt-on level of integration in terms of performance and the underlying complexity.

In contrast, a well-architected unified SASE solution comes with a unified management plane encompassing all the functionalities, including single policy engine, one language to define or import apps and users, an API that exposes most capabilities, and a common data lake.

Unified SASE delivers important benefits over the other two SASE categories, including:

Integrated security and networking – A unified solution offers a more tightly integrated security and network stack that can be centrally managed and monitored, reducing the risk of security gaps or misconfigurations across otherwise separate functions.

Tightest integration of components – All components are designed to work together seamlessly, making it easier to manage and troubleshoot, which reduces complexity and streamlines IT operations.

Easier to scale up or down – Since it's a single-service cloud-native architecture designed for flexibility and scalability, adding additional components or capacity is simpler and quicker.

Consistent user experience – Users can have a consistent experience across all locations and services, with the same set of policies and controls in place.

Reduced operational burden – By combining security and networking policy into a single policy repository, unified SASE avoids the manual and often difficult and inconsistent policy reconciliation found with multiple implementations.

Vendor accountability – With both a unified and single-vendor solution, accountability for issues or outages rests with 'one throat to choke,' simplifying the process of problem resolution.

Alignment of service level agreements – When considering uptime and performance, SLAs associated with unified SASE are straightforward as compared to multiple vendor SLAs.

Futureproof – It protects future projects because the company can be sure that when it is ready to tackle something new, there will be no need to change platforms.

Given the complex environment of most organisations today, reducing complexity with fewer products and moving parts while improving network performance and security makes obvious sense. ■

highlight Service Observability Platform



The SaaS cloud-based network visibility solution with a difference.

 Find out more

Protect Monitor Control

AKCP

Environmental monitoring experts and the AKCP partner for the UK & Eire.



How hot is your Server Room?

Contact us for a **FREE site survey** or **online demo** to learn more about our industry leading environmental monitoring solutions with **Ethernet and WiFi** connectivity, **over 20 sensor options** for temperature, humidity, water leakage, airflow, AC and DC power, a **5 year warranty** and automated email and SMS text alerts.

 **Server Room**
environments

0800 030 6838
projects@serverroomenvironments.co.uk





SD-WAN: strong foundations are required for future-proof networking

SD-WAN – arguably the future of networking across the globe – relies on a flexible, scalable, and secure foundation. But how can the UK's enterprises ensure they have the stable foundational platform required to reap all the benefits?

Getting strategic

Deploying Software-Defined Wide Area Network (SD-WAN) involves careful strategic planning to balance quality of service (QoS), cost, and ease of installation.

“The starting point is to consider why you want SD-WAN and what objectives you want to achieve with it; whether that's prioritising and distributing traffic, delivering cost savings, or flexibility to grow and be future ready,” says Neil Gobsill, head of networks and security, Abzorb. “Then understanding which

applications are mission critical and require higher levels of performance and reliability.”

This understanding “will not only help determine if SD-WAN is the right solution, but also act as a guide in selecting suitable vendors,” shares Jonathan Wright, director of products and operations at GCX. “Organisations should consider speaking with a managed service provider (MSP) that offers multiple SD-WAN original equipment manufacturer (OEM) vendor options. This can provide valuable insights into

the advantages and limitations of various solutions, ensuring decisions are tailored to specific needs.”

From identifying network requirements and evaluating the current infrastructure, to vendor selection, service level agreements (SLAs), and a QoS strategy, all the while optimising the costs – implementing the right SD-WAN is no mean feat.

“Seek out a partner that works with you and does not just implement the tech and disappear. A strategic partner will assist in looking at what technology

you have in place, what your objectives are and the best solution to meet them,” advises Neil Gobsill, head of networks and security, Abzorb. “From a tech perspective, look for robust QoS features, cost effective pricing models and ensure that it is intuitive. The SD-WAN solution should include traffic prioritisation, load balancing and dynamic path selection that supports QoS requirements. Keep it simple by making the installation and deployment intuitive and simple with Zero-Touch Provisioning (ZTGP), pre-configuration and remote management.”



Mark Daley, Epsilon Telecommunications



Eyal Webber-Zvik, Cato Networks



Neil Gobsill, AbzorB

Enterprises must also look beyond a siloed SD-WAN project and towards their greater digital and IT infrastructure transformation, reports Eyal Webber-Zvik, VP of product marketing at Cato Networks: “the market is shifting from point products to platforms that solve more than one problem at a time. It is for this reason and more that we believe led Gartner to predict that, by 2027, 65% of new SD-WAN purchases will be part of a single-vendor SASE offering, an increase from 20% in 2024.”

Building a strong foundation

Setting a strong foundation for modular SD-WAN architecture can significantly enhance an organisation's ability to be responsive and adaptive to future trends, which means that additional bandwidth, sites, and services can be added without overhauling the entire infrastructure.

“A strong SD-WAN foundation allows organisations to be more responsive and adaptive to future trends,” agrees Mark Daley, director, digital strategy & business development, Epsilon Telecommunications. “SD-WAN's flexibility and ability to manage application performance means that changes in priorities can be implemented quickly and efficiently, ensuring adaptability to emerging trends, market changes, technological advancements, and evolving business needs.”

“By using the latest tech your network can grow with the business, so it is scalable and flexible to adapt for elastic bandwidth and changing traffic patterns,” concurs Gobsill. “You can improve services internally and externally resulting in increased efficiencies and productivity by assuring everyone has the bandwidth capacity they require. Also, in the event of a natural disaster you can have a business continuity plan in place, so the network won't fail ensuring an automatic failover and load balancing with continuous availability and resilience against outages. SD-WAN future proofs the network and new technologies and applications will be easy to integrate.”

In choosing the right technologies, Anthony Senter, CEO of SDWAN Solutions, recommends “making sure the hardware is multi-purpose and is not near end-of-life. Your connections should be upgradeable and changeable, and your contract should not tie you into a static solution for 3-5 or even 10 years. Choose a solution that integrates easily with others and has add-on functionality like multi-cloud access, XDR or smart IoT.”

“Every IT team today would like to

be as fast and dynamic as their business needs, thus I would recommend factoring potential projects into the product evaluation and PoC. For example: how fast can new sites be onboarded? How fast can global expansion be achieved? How quickly can two enterprise networks be connected in an M&A?” asks Webber-Zvik.

End-to-end WAN underlay visibility

To build a strong SD-WAN foundation, end-to-end WAN underlay visibility is vital. Organisations must monitor and manage the underlying physical network infrastructure, ensuring optimal performance, quick issue resolution, and enhanced security.

“Advanced solutions that monitor application performance will offer multiple benefits such as enhanced performance through optimised path selection, strengthened security, detailed insights for fault diagnosis and informed decision-making for future investments,” says Wright. “To achieve this, QoS policies need to be well-defined. An ideal solution should provide a holistic view of both the physical circuit underlay and the virtual SD-WAN overlay.”

Daley agrees that visibility is vital, “particularly in global networks where low latency is essential. High, unpredictable latency can severely impact software application performance. A recommended strategy is to use internet access at the network edge, routing through an SD-WAN hub, and utilising a deterministic MPLS core. Additionally, applying application acceleration techniques can improve performance for internet access and MPLS global cores. By implementing these strategies, organisations can ensure they have a clear, comprehensive view of their network.”

Further, Webber-Zvik highlights that “while most SD-WAN solutions will overcome periodic underlay blackouts and brownouts, understanding when there are systematic issues is far more challenging.”

Future-proofing

A mature SD-WAN foundation sets the stage for adopting SASE, wireless WAN, and other future network trends by providing a scalable, flexible, and secure network infrastructure, enabling organisations to stay ahead of the curve.

“A mature SD-WAN offer serves as a springboard for adopting future networking trends, and provides the necessary infrastructure for seamless

integration of cloud-based security services, a key component of SASE,” says Senter. “For wireless WAN, SD-WAN's ability to manage multiple connection types makes it easier to incorporate 4G/5G links. The programmability and automation capabilities of a well-established SD-WAN also facilitate the adoption of AI-driven networking and edge computing solutions.”

However, Webber-Zvik points out that “this is exactly the difference between tactical and strategic approaches to enterprise networking: SD-WAN maturity alone does not guarantee anything beyond reliable branch connectivity. SD-WAN as a feature of a SASE platform creates the foundation needed to support future trends and changes. IT and networking teams should look beyond their current SD-WAN projects and understand how a SASE platform can enable them to achieve their business outcomes in the near and far future. Buying SD-WAN from a SASE vendor does not mean a complete lift-and-shift of the entire network and security infrastructure. It does mean that whatever the future holds, buying SD-WAN from a SASE vendor minimises the chances of being caught unprepared.”

Resilience by design

Cyber-attacks are, as always, on the rise. The ‘Cyber Security Breaches Survey’ recently revealed that 50% of businesses and 32% of charities report having experienced some form of cybersecurity breach in the last 12 months. As such, incorporating security by design into deployments from the outset is critical for protecting the expanded attack surfaces inherent with SD-WAN solutions.

Working with a security-focused vendor is an absolute must, and choosing vendors with integrated security features like next-generation firewalls (NGFW), intrusion prevention systems (IPS), secure web gateways, and antivirus is recommended; particularly those who undergo regular third-party security audits.

“Working with your technology partner, it is advisable to conduct a risk assessment identifying threats and vulnerabilities, then determine which assets are most critical to your business and would have the highest impact if compromised,” advises Gobsill. “Your SD-WAN solution needs to possess robust security features like integrated firewalls, encryption, secure connectivity and intrusion detection/prevent systems (IDS/IPS). It also needs to meet all compliance and certifications regulations. When designing the solution with your

tech partner think of segmentation zero trust architecture, redundancy, resilience and encryption. Also implement a robust multi-factor authentication and access contrails.”

It's also important to define and enforce consistent security policies across all network segments and sites, using dynamic policy enforcement based on real-time context, such as user identity, device type, and location.

“Organisations should start with a foundation and implement clear, practical policies and distinct responsibilities between the Security Operations Centre (SOC) and the Network Operations Centre (NOC). Additionally, leveraging technologies such as next generation firewalls and network segmentation further enhances security,” says Wright.

Secure Access Service Edge (SASE), which combines networking and security-as-a-service functions into a single cloud-delivered service at the network edge, is widely considered an ideal solution to modern networking challenges, embedding security into the very foundations of the network. Effectively delivering consistent secure access to all applications while maintaining full visibility and inspection of traffic across all ports and protocols, SASE radically simplifies management and reduces complexity – solving the challenge of the increased attack surface.

Indeed, “this is exactly what a single-vendor SASE platform is designed to overcome. When SD-WAN and a robust security stack are ONE software delivered as a cloud-native service, the enterprise is inherently put in the optimal security posture,” explains Webber-Zvik. “The alternative, legacy approach is to tailor the security stack to the various ways and forms the enterprise edges are connected. We already know this is a near-impossible mission for most enterprises. A SASE platform makes this a no-brainer, and available to all sizes of enterprises.”

“To address the expanded attack surfaces inherent in SD-WAN, organisations should adopt a SASE architecture,” agrees Daley. “This approach routes internet traffic through a cloud-based Secure Service Edge, providing high-level protection. Trusted and fully qualified domain traffic can be directly routed, ensuring security from the initial stages.”

In or out?

The decision to handle SD WAN in-house or using a managed service largely depends on several factors, including internal expertise, resource availability, and specific business needs.

According to Webber-Zvik, “some solutions use extensive AI and automation and can be self-managed by most enterprises. Others require special skilled staff and expertise. Managed services can always help, regardless of if the solution is simple or complex to operate. An easy to deploy, use and monitor SD-WAN or SASE is of great value to self-sufficient IT teams and to those who rely on managed services.”

“Most UK businesses that require SD-WAN for their networks tend to outsource network management to service providers,” says Daley. “This is because in-house expertise is often lacking, making managed services a more viable and efficient option. Ultimately, the choice depends on a thorough assessment of the organisation's capabilities, needs, and long-term strategic goals.” ■



The role of IoT in smart water management

Phil Beecher, CEO and president, Wi-SUN Alliance

With the huge growth in the global population, the need for conservation of water resources has never been more important particularly in areas of water scarcity. While at the other extreme, we are seeing predictions that rainfall will increase in many regions around the world, and more locally in the UK.

The UK has become wetter over the last few decades, according to a State of the UK Climate report published in 2023. Apparently 2011-2020 was 9% wetter than 1961-1990. This is dependent on location, with Scotland experiencing the biggest increase in rainfall, while most southern and eastern areas of England have experienced the least change. Since records began in 1862, six of the 10 wettest years across the UK have occurred since 1998.

The concern is that climate projections show that on average winters will become wetter while our summers get drier. For any rain that does fall in the summer months, it's likely to be more intense, increasing the risk of flooding and the danger of surface water.

“Given the opportunities in the water industry – including smart metering and remote equipment monitoring – it’s not surprising that sensors in the water and wastewater treatment industries are forecast to grow to \$2 billion globally by 2030.”

Communities in rural and urban areas prone to flooding, will have to find ways to handle these events – and new and innovative solutions to help mitigate the effects. IoT technologies that can collect, share, and analyse data from water networks and systems offer the promise of more efficient ways of managing floods and stormwater capture and run-off, identifying mechanical malfunctions, and potentially curbing issues with pollution and sewage.

Extreme weathers driving utility investment

With extreme weather events on the rise, we were not surprised to see in Wi-SUN's latest research that utility companies are already investing in smart technologies and tools to boost their network resilience.

What is clear is the need to build extreme weather events, like flooding, storms, and other climate change-related disasters, into the risk profile of every utility company. While advanced weather prediction tools topped the list of new initiatives, there is also a much bigger focus on things like disaster response and recovery plans.

Pilot projects and proof of concepts will serve as catalysts in promoting initiatives like smart flood and stormwater management by providing a platform to experiment and optimise new technologies and strategies before rolling out programs on a larger scale.

For many organisations this progress is well underway. Our IoT study published in 2022 examining levels of IoT maturity among global decision makers across a range of industry sectors revealed that half of organisations with smart IoT strategies have already successfully completed projects. This was an increase of more than 10% from the first IoT report we published five years ago.

Smart collection, measurement and efficiency

Given the opportunities in the water industry – including smart metering and remote equipment monitoring – it's not surprising that sensors in the water and wastewater treatment industries are forecast to grow to \$2 billion globally by 2030, according to a report published by IDTechEx.

IoT sensors can provide remote monitoring, maintenance, and assessment of data across a range of applications, from distribution pipelines and storage tanks to treatment plants and more. With the use of edge computing, big data and now with AI and machine learning technologies, IoT will enable the processing of large quantities of data, making it more manageable and useful for companies in the water industry.



The problem with water infrastructure monitoring in the UK is that it has been based on traditional SCADA systems, which do not provide sufficient insight to efficiently manage issues like fault finding and leak detection. According to Ofwat, leakage in England and Wales is at its lowest levels, but the water authority admits that companies need to go further to preserve water and better service customers.

The use of IoT sensors allows for real-time monitoring of water and wastewater networks, providing companies with a transparent view of their pipelines and operations. With predictive analytics, water companies can help conserve water, and identify leaks, while maintenance teams are alerted to any problems and malfunctions on the network so they can be dealt with quickly.

Real-time monitoring systems also provide insights into the status of water collection systems, particularly when they are nearing or surpassing their limits. Such advanced tools can also identify areas with excessive runoff and allow for the necessary adjustments to flood water infrastructure.

Most important, IoT devices can help measure water quality and purity, ensuring compliance with water quality standards, and providing data about the environmental impact of flood water.

Standards-based secure networks

But IoT innovation needs proven ROI. Employing IoT technology based on

open standards will ensure reliability, resilience, and security.

Communications technologies like cellular fail to offer the energy and cost efficiencies required, while struggling with often-challenging environments they operate in. Unlike standards-based field area networks (FAN) based on wireless mesh technology, which provide access to a wider choice of IoT device manufacturers, driving cost efficiencies and reducing the risk of vendor lock-in.

Flood and stormwater management solutions also need to cover a large area with a range of IoT devices – pressure sensors, flow meters, water quality and measurement devices – all without interoperability issues. Integrating FANs to create a canopy network from which water companies can attach leaf nodes for their edge devices should be viewed as an investment rather than an expenditure.

Finally, with critical infrastructure like water networks increasingly targeted by cyber attackers, the importance of investing in smart devices and solutions certified to meet strict authentication and encryption standards is essential. Such devices and networks are then safeguarded from spoofing and data interception, significantly reducing the risk of sabotage or denial of service (DoS) attacks.

With the prospect of more flooding in the UK, water companies will need to make smart choices about how to manage the impact of these increasingly frequent and costly events. ■

Simplifying Cloud-Based Networking

Future proof your business with our flexible cloud-based network solutions.

ab2orb
www.abzorb.co.uk





Commercial critical communications

When we talk about critical communications, it's usually the public sector that we have in mind. However, the UK's profit-making enterprises, too, rely upon always-on, high quality communications services, lest they face severe consequences...

Recent news (see page 1) has perfectly exemplified just how much can go wrong from a single error in the network. The July CrowdStrike outage hit public sector and commercial enterprises alike and has been dubbed 'the biggest internet outage in history.'

"Every modern business relies on connectivity to function," explains Andy Sawyer, manager system engineering, Cradlepoint, part of Ericsson. "For example, retailers use it to support point-of-sale devices, stock tracking and pop-up sites at events like festivals. Any disruption to this network can negatively impact these enterprises, leading to loss of sales, talent and more. Cradlepoint's recent 'State of Connectivity in Europe' report found that 45% of UK firms experienced higher operational costs due to connectivity issues, 27% reported a loss of earnings, and 23% stated it caused their business reputational damage."

"There are a significant number of risks that can emerge when communications are suddenly no longer available. However, the significance of their impact is directly tied to the activities in which the business is involved," confirms Aaron Page, senior consultant, Actica Consulting. "This is best considered by broadly grouping organisations into having Mission Critical or Business Critical activities. Considering Business Critical activities, a loss of communication will inhibit, reduce or limit the company's ability to operate efficiently, serve customers and generate revenue. For enterprises with Mission Critical activities, loss of communications could result in catastrophic consequences: loss of life, significant damage, substantial financial loss, etc."

Cecilia Jordán, market development manager for Industry 4.0, Teltronic, adds that "beyond critical scenarios, the progressive implementation of Industry 4.0 and the increasing value of data for companies make communication networks play a fundamental role. Their interruption can affect production operations, inventory management, quality processes, and more. Automation and real-time analysis of various processes are a reality in many industries, and all of this requires the support of a solid and reliable communication network."

Critical decisions

When it comes to critical communications, enterprises must ensure they have a reliable

and resilient network.

"It is important to not rely on one technology. For example, cellular connectivity can often be used as a failover solution, meaning if the primary fibre network suffers interruption, the organisation can still function," says Sawyer. "It is also important not to invest in technology that is being built on soon-to-be out-of-date technology. For example, copper lines are being decommissioned in the UK, meaning any connectivity infrastructure that relies on this must be changed again soon."

"Companies must consider the reliability and robustness of the system, ensuring that it is capable of offering the required levels of availability and Quality of Service at all times," asserts Jordán. "They should also consider the frequency bands, coverage capacity, and deployment and operation costs, as well as ease of use and maintenance. Another relevant aspect is scalability, so that it can adapt to future growth and needs."

In ensuring continual critical communications, it is also becoming increasingly vital that firms can secure sensitive data.

"Combining 5G cellular connectivity with Zero Trust Network Access (ZTNA) principles, a crucial component of the Secure Access Service Edge (SASE) framework, offers a robust foundation for safeguarding a network," opines Sawyer. "ZTNA, which assumes that anyone on the network may pose a security threat, constantly evaluates a user's security posture during a session, in contrast to VPN's one-time authentication for network access. Some companies may choose to utilise both ZTNA and VPN depending on the diversity of user needs. Furthermore, ZTNA policies can be tailored to each device, establishing security measures before any connectivity occurs and concealing public IPs and IoT resources from discovery, enhancing overall security."

Moreover, "in an Industry 4.0 environment, two other absolutely crucial aspects emerge: on the one hand, the network must offer the highest guarantees of security and data protection, and on the other hand, the ability to integrate with other AI or Big Data systems," adds Jordán.

We have the technology

Getting the right technology in place is crucial to ensuring reliable

communications; however, given the rich variety in features available and organisation demands, this is easier said than done.

"Unfortunately, a one size fits all approach for commercial businesses does not align with their varying activities," agrees Page. "For organisations which engage in Mission Critical activities, current narrowband radio solutions would typically provide a better alignment to their broad generalised needs of reliability, security, dedicated channels and instant communication – although this may change with the advent of Mission Critical Broadband. Alternatively, companies with Business Critical activities will likely be more focused on data capacity, coverage, cost and scalability, this would tend to align better with cellular solutions."

The advantages of cellular networks are clear for industrial environments, where higher transmission rates, lower latencies, and more connected devices are advantageous. However, they require availability that commercial networks cannot guarantee.

"From our perspective, the cellular vs. radio dilemma has a very clear answer: it will depend on the users' data transmission needs, and we believe that the key issue is private vs. public network," shares Jordán. "Radio remains an excellent option for environments where voice is still a critical factor, and large volumes of data transmission are not required. TETRA is perfectly suitable for telemetry applications and SCADA systems, with the added advantage of covering large areas at a lower cost."

"Radio services like TETRA offer reliable voice communications, but basic data services which can be restrictive for modern enterprises. For example, manufacturers using industrial IoT devices to create digital twins must be able to access this data in real time if they want to use it to its fullest effectiveness," adds Sawyer. "TETRA networks are ill-suited for handling the large volumes of data this requires. Likewise, cellular networks are better suited for supporting multimedia content like high-quality video streaming. As such, for most modern enterprise use cases, cellular connectivity is the better choice as it allows them to embrace new technology to its fullest."

According to Jordán, "companies should take note of the advantages offered by the private network concept (radio or cellular), which has proven to be the best

way to guarantee communications even in emergency situations, something that can be crucial for maintaining operations in the business environment."

Shifting to cellular

The future of critical communications is inevitably linked to 4G and 5G, which offer high speed, low latency, and greater control over the communication infrastructure. Their integration with AI applications will be fundamental for the automation of industrial environments, making operations more efficient and secure.

"IoT applied to industrial environments allows for more efficient communication between devices, improving automation and real-time data collection. All of this will foster a new concept of the Smart Factory, enabling better monitoring of all processes and flexible adaptation to manufacturing, logistics, and other needs," says Jordán. "Furthermore, advanced cybersecurity will be a crucial aspect, as attack vectors are increasingly numerous and frequent. Cybersecurity has become mandatory and strategic to ensure the security, integrity, and availability of information."

Meanwhile, Sawyer highlights network slicing as a 'game changer' for the UK's enterprises: "as enterprises begin to make wider use of 5G network slicing, they'll be able to cut the cords often synonymous with connectivity. Instead, they'll leverage versatile cellular networks that greatly reduce implementation costs and maximise business resources."

Page, too, agrees that network slicing, "which can provide dedicated customisable virtual networks offering enhanced capabilities to match an organisation's specific use case (designing the trade-offs between; capacity, connectivity, reliability and low latency), will likely continue to enable growth in IoT, edge computing and AI as well as convergence in both information and operational technology, and will subsequently continue to add focus to the development of encryption and security protocols."

Just as the UK's public sector begins to move to cellular – the UK's Emergency Services Network (ESN) will support fire and rescue, police and ambulance services via cellular technology – so too does the UK's commercial sector, for all but the dirtiest and most dangerous missions. ■



Private networks: protect your farm's IT system from hackers

Dominic Norton, sales director, Spitfire Network Services Ltd.

Until recently, it was relatively straightforward to keep a farm secure. Farmers relied on physical barriers and isolated systems, and traditional methods, such as fencing, locked gates, and the use of basic alarms, were the norm.

Today's agricultural operations have, however, evolved dramatically. Modern farms rely on IP-based security systems, integrated and interconnected, capable of remote management and often reliant on the internet. This provides necessary flexibility and scalability, but also introduces new vulnerabilities.

How today's security systems function on farms

The shift to IP-based systems has transformed how farmers monitor, control, and secure their operations. This transformation is fuelled by the advent of the Internet of Things (IoT), allowing a wide range of interconnected devices, offering unprecedented control and monitoring capabilities.

Modern agricultural security systems integrate various components into a cohesive network, including video surveillance, access control, and environmental monitoring. Video surveillance using HD cameras can monitor livestock, crop fields, and farm storage areas, providing real-time feeds, accessible from anywhere. Smart locks provide better managed access control to restricted areas. Sensors measure and detect temperature, humidity, and other environmental changes.

These modern capabilities offer clear benefits, from the reduced need for constant human monitoring to comprehensive visibility of large farm areas and the ability to quickly detect anomalies such as unauthorised entry or hazards – fires, floods, or equipment failures. Meanwhile, centralised control through cloud platforms makes managing security across multiple locations more efficient.

However, new challenges arise. IP-based systems, while powerful, are also vulnerable to cyberattacks. Hackers can exploit these systems to gain unauthorised access, disrupt operations, or steal sensitive information.

Common vulnerabilities that can be leveraged in agricultural IP-based systems include using default usernames and passwords; lack of network segmentation; open ports; wireless connections; and outdated firmware and cryptography.

Attacks are also becoming more sophisticated, leveraging AI/ML to identify weaknesses. AI tools can quickly scan and identify vulnerabilities in farm security systems, adapting strategies dynamically to bypass defences; or AI-powered drones could be used maliciously to gather information on farm layouts, security camera blind spots, and entry points, providing attackers with detailed information to plan their breaches.

A security breach can lead to unauthorised access to live and archived video feeds, compromising the privacy and security of farm operations. Hackers can also take control of operational technology, potentially causing physical damage or disrupting critical processes such as irrigation, feeding schedules, and temperature control.

In this landscape, it's essential to proactively address vulnerabilities by regularly reviewing and managing the

network's attack surface – the weak links in your systems which are most likely to be exploited by an attacker. It's also important to understand just how your devices are connected.

One of the biggest challenges here is that as the scale of your networks grows, so does the complexity involved in updating, managing, and supporting them. Each additional device introduces new potential vulnerabilities which require meticulous security planning and ongoing management and updates to maintain high levels of cybersecurity resiliency.

The solution?

Given these challenges, a strong and effective solution is needed to improve farm security installations and reduce vulnerabilities.

Exposure to the public internet is at the heart of these vulnerabilities, necessitating a network solution that connects unlimited devices, systems, locations, and applications without this exposure. A fully secure, private network with fast, easy connection, control and communication between all devices introduces several key benefits for farms, including enhanced

security; simplified management; and flexibility in deployment.

The best of both worlds

The transition from isolated, standalone security systems to interconnected networks has increased security capabilities for farmers but also introduced new risks. With secure, private networks now a realistic option for agricultural businesses, it's possible to leverage solutions that offer all the features and functionality of modern installations, without their vulnerabilities. ■

MobileMark

antenna solutions

STAY CONNECTED

with Advanced 5G
Antenna Solutions for
Autonomous Vehicles,
Public Transportation,
Precision Agriculture,
Medical IoT, Robotics,
and More!

www.MobileMark.com

Contact Us Now:

+44 1543 459555

enquiries@MobileMarkEurope.co.uk





EEAST pilots Hybrid Connex for cost-effective ambulance connectivity

A significant and successful pilot study at the East of England Ambulance Service NHS Trust (EEAST) has proved that cost effective improvements in NHS connectivity are available now and can be implemented within days, leading to better quality and more flexible patient care, improved staff wellbeing and the potential delivery of a wider range of healthcare services by NHS providers.

With clarity still lacking on when the long-awaited Emergency Services Network (ESN) will come to fruition, the

Connecting the impossible

Hybrid Connex, available from Excelebrate Technology, was developed through a €5.7 million European Space Agency-funded research and development programme featuring the latest technology that goes well beyond 4G limitations and into satellite territory, providing robust connectivity for ambulance crews and vehicles in areas where traditional cellular connectivity has been extremely challenged or impossible to achieve.

During the pilot, four vehicles from EEAST had Hybrid Connex Technology installed. Apple iPads were configured to auto connect to the vehicles' WiFi bubbles, and this was 99% successful during the trial period. Moreover, crews operating in fleet not equipped with Hybrid Connex have reported being able to access the trial vehicles' WiFi bubbles when in proximity and therefore receive patient records.

The results showed that, where crews on the trial vehicles experienced stable high-speed WiFi connection, they were able to access data and information while responding to calls in areas of low or no cellular coverage.

"There was very stable Wi-Fi in the

middle of nowhere, achieving 150Mbps download. I conducted a Teams meeting in the passenger seat with excellent clarity and connection stability," noted one paramedic using the system.

The successful trial at EEAST enabled paramedic crews to achieve almost permanent connectivity in areas where they previously had very little, or no internet connectivity at all. During the pilot, cellular connection was utilised in 88% of jobs attended in areas where previously the signal would not have been good enough to achieve a stable connection.

Connection availability was 93% during all jobs carried out in low or no coverage areas throughout the pilot and satellite was utilised in 47% of jobs in low or no coverage areas, which many times was bonded with the cellular to provide a faster internet connection for crews on board.

"The Hybrid Connex technology bonds clever software, cutting-edge hardware and cellular and satellite services into one package combining seamless 4G, 5G and satellite connections that ensure ambulance crews get a fast, resilient connectivity solution and are seldom offline. The hardware is unobtrusive and the technical fit-out can be done in a day, meaning the vehicle doesn't need to be off-line for long," said Bethan Evans, chief operating officer at Excelebrate. "Patients and staff are the ones who really benefit when strong connectivity enables better clinical technology at the frontline, with new ways of working too. Importantly we also started to see how this technology can support reductions in unnecessary conveyance to hospitals, something which is a key NHS priority."

While satellite connectivity is not currently 'the norm' when it comes to emergency services communications,

its inclusion into a single bonded solution, where it is called upon when cellular connectivity is unavailable, will have significant benefits for resilience, especially in a large-scale, mass casualty incident, where experience has proved that one of the first things to fail or become overloaded are cellular communications.

An always-on WiFi bubble around the ambulance allows staff to connect to digital systems such as NHS Spine-connected services, giving them access to patient history and enabling them to identify alternative care pathways, make the right decisions for the patient and provide the opportunity for the best possible clinical outcomes.

New care pathways

Complementing the next phase of the Ambulance Radio Programme (ARP) rollout, part of the ESN, this advanced level of permanent connectivity will open the door to new patient care pathways, taking advantage of digital advances, while increasing the range of point-of-contact diagnostic services and tests that ambulance crews can carry out on-the-spot, without taking patients to hospital. It will also ensure that crews can quickly and easily access immediate clinical information through electronic patient records.

With Hybrid Connex, crew will be able to remain in constant contact with specialists about patients and their conditions while travelling to receiving hospitals and locate patients faster in areas where connectivity is compromised. Helping crews find key information about local health and social care services, enabling them to signpost patients to more appropriate, alternative sources of health and care, will

provide a truly transformative effect for patients in need.

"When we lose connection, clinical apps stop being able to pull information from our CAD system, cease being able to pull information from our PDS trace to bring the patient's NHS number into record and prevent us being able to upload information to our key partners," said Philip Elvidge, electronic patient care records lead (paramedic) at EEAST. "However, with Hybrid Connex we have been able to access the Summary Care Records and National Record Locator consistently, which gives staff access to patients' End of Life and Mental Health Plans, giving access to key information any time of the day to help us make the right clinical decisions. As we move forward with the integration of digital technology to ambulance front line care, we have access to more information about our patients than ever before, but we need to be connected all of the time to take advantage of it. Paramedics need to know they can always have the same information available no matter where they attend to their patients. With Hybrid Connex in place, we are already seeing how a guaranteed connection improves our patient care, as we can download information about the patient and access their clinical records whenever needed. We are already starting to use new functionality like video calling to a stroke consultant in a specialist centre, for example."

The system will further enable fleet managers and financial managers within ambulance services handle the often-complex commercial aspects of connectivity - such as billing - in a much more efficient way. Ultimately, it will also enable users to be better prepared and able to take advantage of developments in telemedicine and video technology. ■

West Midlands Ambulance Service adopts satellite for emergency medical response

The West Midlands Ambulance Service University NHS Foundation Trust (WMAS) serves as a critical lifeline for the West Midlands region of England, providing essential NHS ambulance services. As one of ten ambulance trusts within the NHS, WMAS is entrusted with delivering emergency medical services across a vast geographical area.

Covering Herefordshire, Shropshire, Staffordshire, Warwickshire, Worcestershire, Birmingham, Coventry, Dudley, Sandwell, Solihull, Walsall, and Wolverhampton, WMAS's reach extends to the unitary

empowering WMAS to make informed decisions swiftly during emergencies; seamless connectivity on the move, ensuring operational readiness regardless of location within the West Midlands region; and consistent and dependable connections, mitigating the risk of communication breakdowns during critical operations.

Advancing modern healthcare

The adoption of Starlink's advanced mobility solution marks a significant milestone in emergency communication technology for

"To continue to provide timely and efficient emergency medical response, WMAS faced challenges inherent to traditional geostationary communication systems. These limitations, including slower speeds, high latency, and fixed location constraints, threatened the agility required for effective emergency response operations across its expansive service area."

authorities of Stoke-on-Trent and Telford & Wrekin. Additionally, the trust offers non-emergency patient transport services in Birmingham, the Black Country, Arden, Cheshire, and the Wirral.

Shooting for the stars

To continue to provide timely and efficient emergency medical response, WMAS faced challenges inherent to traditional geostationary communication systems. These limitations, including slower speeds, high latency, and fixed location constraints, threatened the agility required for effective emergency response operations across its expansive service area.

Recognising the need for change, WMAS partnered with Clarus Networks Group to overhaul its Command Unit's communication infrastructure. Leveraging Starlink's mobility service, WMAS aimed to unlock unprecedented levels of connectivity, mobility, and reliability essential for optimising emergency response capabilities.

Key components of the solution included high-speed internet connectivity, enabling real-time data sharing and communication,

WMAS. Advancing beyond the limitations of traditional geostationary systems, WMAS stands poised to provide faster, more efficient services precisely when they are most urgently required.

The partnership between WMAS, Clarus Networks Group, and Starlink Mobility exemplifies a shared commitment to innovation and excellence in emergency medical services. Through the deployment of cutting-edge technology, WMAS reinforces its dedication to safeguarding the health and well-being of the communities it serves across the West Midlands region, ensuring that critical emergency communication capabilities evolve in tandem with the ever-changing demands of modern healthcare.

The results speak for themselves. WMAS gained speeds of 220Mbps download and 40Mbps upload, even whilst in motion, and latency of just 20-99ms. Reliable coverage – even in rugged terrain and remote valleys – was achieved, while instant communication was made possible with emergency personnel and other stakeholders. Finally, WMAS now benefits from a future-proofed primary and backup internet solution. ■



Secure your business's continuity with expert backup power solutions

Talk to the experts



CP Critical POWER

Call: 0800 088 5315 or visit www.criticalpowersupplies.co.uk



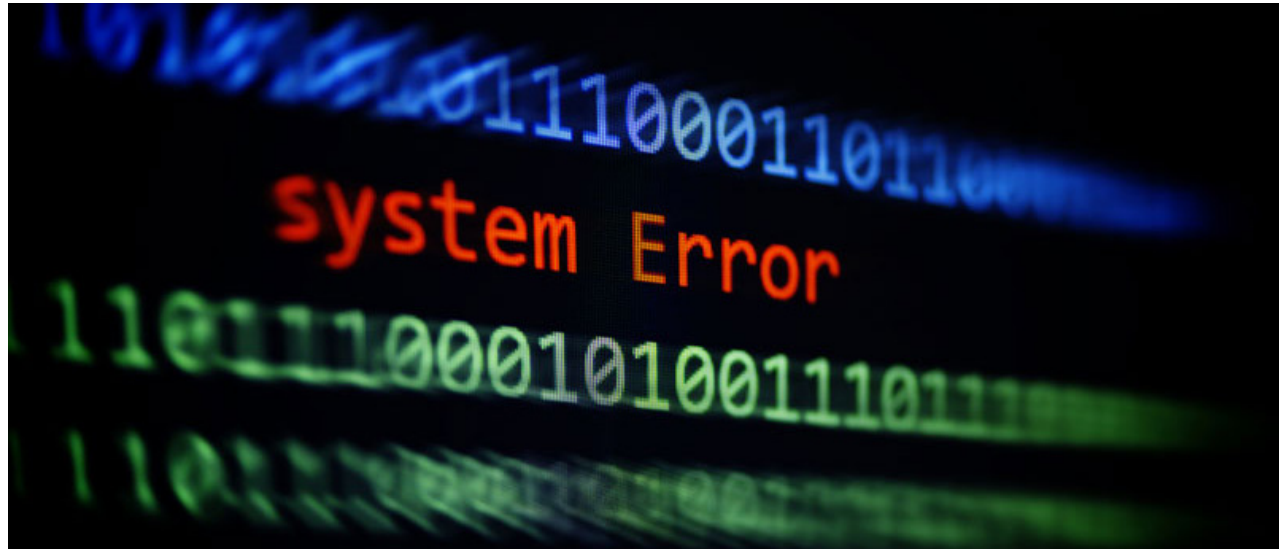
Critical communications – when networks go down

Duncan Swan, chief operating officer, British APCO

The Microsoft/Crowd Strike issue of 19th July got headlines across most of the world due to the impact of the loss of IT systems and services had on many people's day-to-day lives. Businesses came to a standstill; transport was disrupted; and healthcare services reverted to pen and paper supporting only the most urgent cases. Away from the UK, it also impacted delivery of critical emergency calls.

IT & comms failures impacting delivery of emergency calls, from those in their time of greatest need to an emergency agency, are becoming ever more prevalent. And the underpinning reason why these failures are occurring is often software failure or upgrade/configuration errors. There is an air of inevitability that systems and services are likely, at some point, to fail. And often not in the way you might expect. Critical service providers must, therefore, take business continuity more seriously than ever before. It's not just about knowing there is built-in resilience to the core infrastructure; it's about having robust alternatives that minimise the impact to critical service delivery, with clear communication plans that let those needing emergency assistance know precisely what to do and expect.

The Collaborative Coalition for International Public Safety – of which British APCO is a founding member – has recently published a Best Practice Guide for emergency agencies to consider when three-digit emergency calls can't be received. Most organisations have emergency plans should they need to evacuate their premises; or there is a major incident to deal with; or they need to move to a back up system. But many have yet to establish and rehearse plans as to how to allow the public to make contact when the primary emergency communication



was unexpected," the Optus MD told the Australian Senate not long afterwards.

Two recent network outages in Canada also have their root cause analysis in software upgrades. In April 2021, Rogers, a Canadian wireless provider had an 18-hour outage affecting ~ 11 million people; wireless and landline internet access was affected; and it was not possible to use 911, the emergency communication number. And again, in July 2022, the same provider suffered a similar duration outage affecting ~14 million subscribers, roughly a third of the population of Canada. This latter network failure was almost identical to that suffered by Optus in Australia a year later where, due to incorrect configuration, a flood of IP routing data from the distribution routers into the core routers exceeded their capacity to process the information.

In Europe, both Ireland and France have seen prolonged carrier network outages – each of which impacted critical

outage that disrupted wireless services for many customers. The issue was eventually attributed to an incorrect process during network expansion. T-Mobile experienced a major outage in June 2023, primarily affecting voice and text services due to a routing issue. This disruption also had knock-on effects on other carriers, leading to widespread connectivity problems. And on multiple occasions, Verizon has faced outages, often linked to network changes or issues with inter-carrier connections.

So where critical communications are concerned, it is critical that citizens facing a

critical situation at a critical moment in their life can get through to the emergency agencies. Emergency agencies and network providers need to be critical as to how they manage risk and ensure business continuity in situations where the normal, trusted, method of emergency communication becomes unavailable. There is also a growing body of evidence underpinning that no level of investment or planning in technology resilience can survive the human elements of poor software upgrades or configuration errors. Neither scale nor ignorance can be an excuse. ■

"IT & comms failures impacting delivery of emergency calls, from those in their time of greatest need to an emergency agency, are becoming ever more prevalent. And the underpinning reason why these failures are occurring is often software failure or upgrade/configuration errors."

lines are down – and how this will be effectively communicated.

Back in November 2023, the Optus network in Australia suffered a national outage of all Optus internet, cellular and fixed-line services in Australia. Emergency services were compromised. Hospitals were hampered in their critical work. Businesses lost the ability to trade. And nearly 2,500 Optus customers were unable to get through to emergency services during the 16-hour blackout. The outage occurred when many Optus routers automatically self-isolated to protect themselves from an overload of IP routing information – all resulting from a software upgrade, where the network received changes in routing information from an alternate Singtel peering router located out in Singapore.

Some 10 million Optus customers had no way to get through to Triple Zero emergency services – "We didn't have a plan in place for that specific scale of outage. I think it

communications – due to a software upgrade or configuration error. In the UK, the 999/112 system went down for some 10 hours in June 2023 (the first time since its inception in 1937!) – and for which the public emergency service communications provider BT were recently fined £17.5 million. In their report, Ofcom the UK telecoms regulator, said the emergency call handling outage was caused by an error in a file on a BT server, which meant systems restarted as soon as call handlers received a call. It led to staff being left logged out and calls being disconnected or being dropped as they were transferred to the emergency services. The level of preparedness of BT, all the other UK network operators, and the emergency agencies themselves has all come under scrutiny; with work to resolve this situation put in place soon after.

And in the US the three major network carriers have all suffered recent outages. In February 2024, AT&T suffered a nationwide

telent
talent with technology

High performance IT networks for demanding applications, combining wired, Wi-Fi, 5G and SD-WAN technologies with security designed in from the start and AI management applications to optimise network performance.



Find out more about Telent

w www.telent.com **t** 0800 783 7761 **e** talktotelent@telent.com



Three business continuity tips for navigating uncertainty

Martin Lewis, cyber and operational resilience sales manager, Daisy Corporate Services

Business continuity managers have been kept busy in recent years, with supply chain issues, a pandemic, and ongoing cyber-attacks threatening to cause significant disruption to operations. Consequently, continuity planning is now a constant feature on boardroom agendas. But given the array of risks facing organisations, what steps should be taken to build resilience?

Step 1: Get ahead of the game

The first step organisations should take is to review incident response management and continuity plans. While in times of non-crisis, it's easy for companies to focus on other areas. But when incidents do occur, it's often already too late. That's why it's vital to regularly review and update current plans to ensure they are still operational and relevant. With the risk of cyber-attacks remaining a constant threat, businesses must develop a separate incident response plan for cyber resilience to discover, prevent, and respond to security threats. This should include elements such as identifying and reporting the incident before containing and eliminating it. It's vital that this plan also includes steps to assess the damage

and restore order, as well as analysing and improving post-incident strategies. There is no one-size-fits-all approach, given the breadth of attacks. So specific measures must be in place within organisations to combat incidents, whether this is due to a malware attack or caught up in spear phishing attempts.

Step 2: Creating a smart backup strategy

The old maxim of backing up your work is no longer enough, and this is where the 3-2-1-0 backup strategy comes in. This approach offers enterprises the best chance of data recovery in the event of a cyber-attack. Following this framework involves creating three copies of important data sets, in addition to the original, while splitting these copies across two different storage methods. These additional backups must be stored separately from the primary one, too. One should be kept offsite, and the other copy must be air-gapped and immutable to prevent any chances of the data being compromised. The final step that enterprises should follow – achieving zero errors in the data backup. Inconsistencies, errors, or missing data

could put a successful backup at risk. The 3-2-1-0 backup strategy offers enterprises the best chance of data recovery. While this approach certainly isn't new, it continues to be crucial for maintaining data resilience and enabling recovery in the event of a disaster or cyber incident. This strategy ensures that you have at least two backup copies of all important data and can recover from incidents more efficiently.

Step 3: Test, test, test

Finally, conducting regular tests and rehearsals of existing business continuity, crisis management, and cyber incident response plans is vital. How can business continuity managers know if the organisations will remain resilient against threats if the procedures in place have never been tested? To ensure these plans are strong enough to protect against all types of disruption, organisations must assess tolerance levels across components such as their network, and plan and test for worst-case scenarios, not just plausible ones. Testing remains a highly effective way of ensuring that everyone within the organisation comprehends their role and responsibilities in the event of an incident.

It's far better to identify failures in existing plans during rehearsal rather than in a real-world incident.

Align and shine in crisis

To stay in the driver's seat on the road to resilience, business continuity and security teams must now prioritise organisational alignment by communicating to executives the importance of resilience through threat assessments, cost evaluations and other relevant documentation. And the entire organisation must be included in this journey. The more capable a business is at mitigating risk, the more robust and adaptable it will be when faced with uncertainty. By adequately preparing for, detecting, anticipating, and adapting to the ever-changing risk landscape, a business can position itself to withstand almost any potential disruption. To achieve this level of resilience, organisations need to their plans beyond the immediate risk landscape and prioritise long-term preparedness. While tackling daily challenges is demanding and costly, the ability to anticipate and navigate future obstacles will set businesses up for lasting success.

PRODUCTS

Keepit provides next-level SaaS data protection purpose-built for the cloud, by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience and future-proof data protection. Keepit owns its tech stack and operate a vendor-independent, cloud-native infrastructure, ensuring data availability. Its certified security means the enterprise is fully protected against data loss: human error, cyberattacks, malicious deletion, and even when the SaaS vendor is down. With complete and granular recovery features, Keepit helps organisations recover data intelligently and fast, getting individual files or entire app datasets back fast in only a few clicks — with protection across all of the most popular SaaS applications. Moreover, tamper-proof data storage means data availability 24/7. With Keepit, businesses can easily comply with even the strictest data policies like GDPR and NIS2 with guaranteed data sovereignty — the user can pick the data centre region of choice, and data will never leave that region.

Cohesity SiteContinuity helps simplify disaster recovery (DR) through automated orchestration, so the enterprise can get critical applications online after a breach or outage. With Cohesity, organisations stand to gain from flexible DR options — self-managed site to site, turnkey disaster recovery as a service (DRaaS), or DRaaS from a Cohesity-Powered service provider. As such, the enterprise can meet SLAs without breaking the bank with automated disaster recovery powered by SiteContinuity. Features include one solution for backup and disaster recovery with automated orchestration across multiple clouds. Applications and data are protected across tiers, service levels, and environments with a unified policy framework. Business risk is mitigated with automatic failover and fallback orchestration across multicloud environments. Applications and data can be restored to any point in time — from years to just seconds before the disaster hit. SiteContinuity delivers near-zero downtime and no data loss with hot standby, plus automated recovery of a



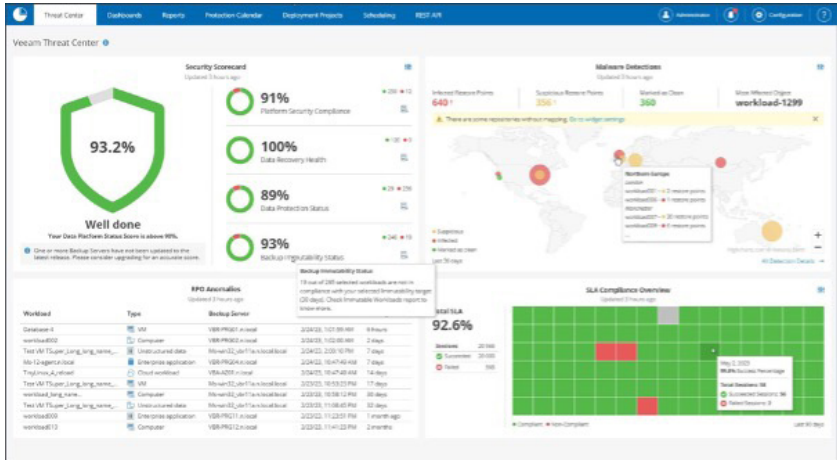
single application or an entire site within minutes. The user can meet compliance needs and ensure DR readiness with detailed audit trails, reporting, and non-disruptive testing. Intelligent insights and monitoring ensure fast and reliable recovery at scale, while the company's security risk can be reduced with a detailed dashboard that gives the health status and recoverability index of the backup snapshot. All this comes alongside the elimination of unnecessary infrastructure, avoiding data deduplication across workloads.

NinjaOne Backup offers the ability to simplify the backup of critical business data and meet security goals with a solution designed for MSPs. With data protection built to benefit your business, NinjaOne delivers flexible and customizable file & folder or image backup plans that focus on each client's unique requirements. Experience data protection designed to add a key solution to MSPs' existing product stack while enhancing the ability to make more money with less labour costs to the team. NinjaOne Backup is fully integrated into the NinjaOne platform, giving your staff one place to manage, remediate, and secure devices. Key features for MSPs include flexible backup plans, with the option to create and apply fully customizable file & folder or image backup plans that balance data protection, retention, and storage requirements across endpoint types. It also features multiple restore options, such as end-user self-service file recovery, web-based file restores and download, bare-metal restore and more. The natively cloud-based solution means that the organisation can remotely configure, administer, and customize backups, set up smart scheduling, and utilize built-in deduplication and forever incremental image backups to protect your clients' data without impacting client networks. Ransomware recovery comes as standard with backups that are encrypted both at rest and in transit, MFA is required for any deletions, and cloud storage with triple redundancy data centres. Proactive alerting via a number of channels provides full visibility into all backups - if something goes wrong permitting, the team can act quickly. Moreover, the enterprise can remediate backups and other device issues easily using NinjaOne's built-in remote terminal, registry editor, and remote access tools.

The Veeam Data Platform, built on the principles of data security, data recovery, and data freedom provides enterprise with resilience in the face of growing cyber-attacks. With it, organisations stand to gain

from reduced incident response time with proactive threat hunting integrating SIEM platform support, YARA powered scans, and NIST cybersecurity best practices. For secure backup and fast recovery,

application aware, image based backups are available for VMware, NAS, Windows and more. Native backup and recovery for AWS, Azure and Google Cloud comes as standard, with bulletproof ransomware protection with immutable backups functionality. With the Veeam Data Platform, organisations can achieve sub-minute RPO and fail over to the latest state instantly with Veeam CDP; immediate recovery and production data access for VMs, entire NAS shares and SQL/Oracle databases with Instant Recovery; and 1-click site recovery and DR testing with Veeam Recovery Orchestrator. Proactive Monitoring & Analytics include unified monitoring and reporting across on premises, cloud and remote agents. Built in intelligence can identify and help resolve common misconfigurations and backup problems, while effective capacity planning and forecasting to keep IT needs in check.





Please meet...

Stewart Laing, founder and CEO, Asanti

Which law would you most like to change?

There's not a specific law I would change but I feel some of the laws coming into play are encouraging people to become more and more offended at every little thing. We're at a point now where I feel people are scared to have their own opinions in fear of the reaction of others. It's incredibly frustrating especially watching younger generations not being able to learn and form their own views. I am worried about the erosion of freedom of speech and expression, and its implications not only for businesses in the next decade or two but for society as a whole.

Who was your hero when you were growing up?

My Dad. He was the hardest working person I've ever known. His ethics towards life and to work were incredible. He had a saying – "If you're going to do something, make sure you do it 100%." He was a great role model for me, and I've stuck to those words throughout my life.

What was your big career break?

I joined a small IT company in Glasgow called Altor. I went in as a Service Manager and within 12 months I was the Operations Director. Within 24 months we grew the managed services business from a turnover of £200,000 a year to £2.3 million.

The funny thing is that Altor was then acquired by ICM which, following subsequent acquisitions, later became Daisy and when I formed Asanti, we would go on to purchase their data centres a few years later.

Where would you live if money was no object?

It would have to be the west coast of Scotland. So not far! Having said that, I would also like to be able to visit the North of Mallorca whenever I felt like it.

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

Growing up I wanted to be a civil engineer. I love everything to do with roads and bridges. Still to this day I have an absolute fascination with The Forth Road Bridge. Built in 1964 it spans over 1,000 metres between two towers and was the fourth longest bridge in the world at the time. It really is something to behold.

I fully intended to follow that path but when I left school I stumbled into an apprenticeship at Honeywell as an electrical and electronics engineer. I was offered one of only two positions and it was one of the highest paid apprenticeships in Scotland at the time, so I took my dad's advice and went for it 100%!

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

If I had to choose just one person, it would be Andrew Carnegie. His achievements during his lifetime are truly astounding. Born in Dunfermline, he moved to America with his family in search of better opportunities and seized them fully. He sold his steel company to J.P. Morgan for \$480 million in 1901, but his philanthropic journey began as early as 1870, when he gifted a public library to his hometown of Dunfermline. Carnegie once said, "To try to

make the world in some way better than you found it is to have a noble motive in life."

What would you do with £1 million?

I would set up a charity called Asanti7. After visiting Uganda and witnessing the lack of support for vulnerable women and children there, I have felt inspired to make a difference. I visited in 2009 and 2011 with Watoto, who back then, were working to address the root problems through education and skills training. Their focus

was to work with vulnerable women and children, helping them to learn skills and to set up businesses so that they can support their families.

What's the greatest technological advancement in your lifetime?

These days everything is new! In all seriousness though it must be the smartphone. It is the best and the worst! I know these devices come with challenges but when you think about what they do, the technology is incredible.

It does take over our lives but when I look back to how computer technology changed within a relatively short period it is amazing. When I was a computer engineer, prior to joining Altor, the technology that I was working on become obsolete within two years.

The Rolling Stones or the Beatles?

The Rolling Stones wins it for me every single time. I always enjoyed my rock music and was never a huge fan of the Beatles. ■

HARNESS THE POWER OF ZOOK...

Remotely Monitor Basic & Metered PDUs

USE POWERZOOK TO IDENTIFY

- PDU power usage
- Power failure
- Equipment failure
- Near-overload conditions
- Unusual power usage patterns
- Cable/wiring faults



WHY POWERZOOK?

- No downtime installation
- Clamps around 3-core cables
- No cable modification needed
- PoE
- SNMP
- No additional point-of-failure
- Easy swap-out if needed

Jakarta

SENSORS FOR THE DATA CENTRE & BEYOND™

pz@jakarta.com | www.jakarta.com

+44 (0)1672 511 125