JANUARY 2024
networkingplus.co.uk

NETWORKING+

SF6-free switchgear

Enabling the sustainable DC

Peter Betts, VIRTUS Data Centres, p10

Is your network AI-ready?

There must be end-to-end visibility

Rob Quickenden, Cisilion, p14

Questions and answers

I'd set up an educational trust

Hubert Da Costa, Celerway, p16

'Mother of all breaches' exposes 26 billion records to the public

Towards the end of January, a 12Tb database of 26 billion records was exposed online, featuring data from 1.5 billion Tencent users, 500 million Weibo users, 360 million MySpace users, 281 million X users, and 251 million LinkedIn users, among others. The 'mother of all breaches' indeed.

On the plus side, the archive of data - comprising password lists, user accounts, and other personal details - consists primarily of databases from several high-profile security breaches that have occurred over the last decade.

"Almost none of the data contained within this archive is 'new' and it does not represent a new significant breach of any one organisation or database," outlines James McGoldrick, DFIR & CSIRT manager, Systal. "However, what is new is the fact that all these leaked datasets have been collated into one centrally stored resource."

"The raw number of lost credentials 26 billion should help everyone realise just how bad this problem is," says Corey Nachreiner, chief security officer at WatchGuard. "Often, threat actors don't have to 'hack in,' they just log in using credentials they have stolen or that have leaked in other breaches."

So, what's the big deal? Paolo Passeri, cyber intelligence principle, Netskope explains that "all of the leaked data here can potentially be misused by threat actors to carry out identity theft and opportunistic or targeted phishing campaigns, a scenario that is made even worse by the fact that this massive amount of records is readily available and contains information coming from different organisations in different sectors."

"Malicious actors are able to leverage these breached credentials at scale to conduct credential-stuffing attacks against other services and company accounts in an attempt to gain access to additional systems via reused passwords," adds Christian Scott, COO and CISO, Gotham Security, an Abacus Group Company. "Furthermore, this information allows malicious actors to infer commonly used passwords by staff at an organization to perform curated password spraying attacks."

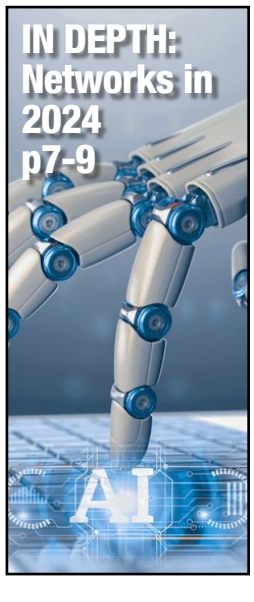
With much of the exposed data sourced from websites and applications heavily used by the business world, these sorts of discoveries should always serve as a wake-up call for enterprises, reinforcing the need to adopt a 'zero trust' strategy, according to Passeri.

"For businesses, a robust defence strategy is essential to protect against all rising threats," says Irvin Shillingford, regional manager Northern Europe, Hornetsecurity. "This should include email security solutions, backups, and effective security awareness training. All employees must be consistently educated and trained on security awareness to drive up company-wide protection and defend against any cyberattack."

"Attacks such as this one highlight - again - that simply putting strong passwords in place is no longer good enough. Instead, we need a mechanism that mandates users to frequently change their credentials as well. And, each time, this mechanism must require strong, unique passwords, not iterative Password1, Password2 changes," explains Andy Thompson, cybersecurity research evangelist, CyberArk. "Let's say it takes a threat actor six weeks to crack the password of a systems administrator. If that password is rotated once a week – which can be automated to allow for a seamless user experience – then that credential would have been changed six times before the threat actor could crack the original password via a brute force attack."

Moreover, the companies impacted in this leak risk significant consequences, including financial implications and potentially regulatory fines, as well as significant reputational damage.

"All businesses are trusted by their partners and customers to keep their data safe, and once that trust has been compromised, it's incredibly difficult to win it back," warns Scott… ■



Scottish FRS gains internet-based VoIP communications system

MLL Telecom has successfully implemented an internet-based voice (VoIP) communications system at the Scottish Fire and Rescue Service's (SFRS) newly opened £12 million Cambuslang Asset Resource Centre (ARC) in Glasgow. This was delivered by MLL as part of its ongoing contract to provide SFRS with fully managed wide area network (WAN) services.

SFRS required the new VoIP system to maximise the operational effectiveness of the new multi-purpose ARC facility, located at its national headquarters and training centre complex and which is designed to support the work of Scotland's firefighters. MLL's solution will ensure SFRS staff from various support departments who have moved into the new building, and its team of mechanics responsible for maintaining fire appliances, can count on high quality, reliable and secure voice communications around the clock.

The geographically diverse, fully resilient voice service was delivered by MLL from order to in-life within 48 hours and without any failures, allowing SFRS to meet the required go-live date. The solution was fully tested beforehand which also offered SFRS the opportunity to add new features that had not been considered during design.

Cambuslang ARC is the first of several VoIP installations that MLL is planning across various SFRS sites. In addition, MLL is currently trialling satellite-based communications at SFRS's site in Dumfries.

"We are very pleased to have been able to meet SFRS's challenging requirement to deliver resilient new telephony services within only 48 hours and which are aligned with its digital transformation cloud first strategy," said Roy Harby, MLL's Public Sector Enterprise Business Product Solutions Architect. "Together with the tools, facilities and expertise available on site for maintaining the fleet of fire appliances and other specialist equipment, our internet-based voice communications solution will be equally key to helping SFRS keep local communities safe."

"Cambuslang ARC is a major new development to enhance the working conditions for our staff working across different areas of the Service," said Iain Morris, SFRS Head of Asset Management. "The building includes a state of art workshop for our mechanics who work tirelessly to keep fire appliances maintained to protect communities across Scotland. The design and materials used in this project has created one of our most energy efficient buildings, representing a tangible commitment to delivering value for money."

In 2023, MLL successfully completed a nationwide Wide Area Network (WAN) transformation at SFRS. The new SDWAN connects over 370 fire and rescue sites located throughout Scotland, including highland and island areas, while ensuring reduced network latency for an enhanced user experience, especially at remote sites. ■

Teledata's new Manchester data centre to harness waste heat

Teledata's new Manchester data centre is being developed with heat re-use capabilities as part of the company's wider sustainability strategy. The scheme will see Teledata's new facility harness waste heat for conditioning, reuse, and delivery to local projects in Wythenshawe.

The system is being designed so that heat exchangers can be used to transfer the thermal load of the data centre cooling loop to a local community heating network via a heat pump system, which will reduce the amount of energy needed to deliver the required data centre cooling operation. The new facility is targeting a PUE of 1.2.

The new data centre (MCR2) is being developed next door to Teledata's existing facility and the most up to date sustainability best practices and standards are being embedded across all parts of the build process, from design to implementation.

In addition, the facility will be powered using clean energy from renewable sources with green certificates and solar PV roof panels. The PV system will generate over 83,000kWh/yr with a CO2 emissions reduction of over 7.4 tonnes annually. A chilled water-cooling system with free cooling technology will be adopted and renewable HVO (hydrogenated vegetable oil) biofuels will fuel the emergency generators. The new data centre has been specifically designed to handle an external ambient temperature of 40+°C, to help mitigate climate change risks related to extreme heat.

The new site involves demolishing the existing building and designing a newer, more modern, energy efficient facility. The data centre facility will offer over 50,000 sq ft of enterprise-grade colocation space with 2N power redundancy, 100% 24/7 uptime, ISO27001 certification and NSI Gold Approved BS5979 security. ■

His Majesty's Naval Base Portsmouth goes smart with IoT

Smarter Technologies has been supporting the digital innovations team at His Majesty's Naval Base (HMNB) Portsmouth, with their proprietary Orion IoT Data Network, to maximise the efficiency of port operations.

HMNB Portsmouth is home to the majority of the Royal Navy's surface fleet, including the flagship aircraft carriers, HMS Queen Elizabeth and HMS Prince of Wales, the formidable Type 45 destroyers, Type 23 frigates and mine countermeasures squadrons. The harbour at Portsmouth is one of the busiest in the UK, with around 130,000 significant movements annually, and it is also the home for ship repair and maintenance.

HMNB Portsmouth, like many defence establishments, is a large and complex estate that presents significant infrastructure management challenges and requires significant focus and innovative thinking to run efficiently, maximise operational capability and minimise costs. This is especially true where the estate is historic in nature and is not designed or constructed to meet modern operational needs.

The Infrastructure Asset Management team at HMNB Portsmouth, keen to adopt digital innovations, approached Smarter Technologies to assist with the provision of real-time data from multiple sensor platforms across a large geographic footprint, to inform critical operational decision-making.

Following an earlier demonstration of their smart sensor technology and Orion real-time IoT data network, Portsmouth invited Smarter Technologies to install depth sensors in each of the dockyard's key operational and historic basins (No 3 Basin alone holds over 300 million gallons of water) and transit locks to monitor water levels. Via an intuitive and customer-configurable dashboard, the sensors provided the Asset Management and Waterfront teams with the empirical evidence they needed to adjust how and when the locks and pumps were used to optimise water levels, assets to target for remediation to minimise unintended water flows and maintain effective waterfront operations. As a result, unnecessary pumping operations were avoided, both long- and short-term targeted mitigation measures were implemented and material operational efficiencies were realised, almost immediately delivering a return on investment.

"The management insight that Smarter Technologies have brought to the waterfront operation has been incredibly helpful, and it's been amazing just how quickly it gave us the evidence-base we needed to do things differently and do things better," said Simon Kierstan, the Navy's strategic infrastructure lead at Portsmouth. "This is just one part of a much broader digital innovation programme at Portsmouth Naval Base, which is gathering momentum and delivering significant step-changes in capability with each enhancement."

"We're just delighted to be working with Simon and the management team at Portsmouth and to deliver value for them," said Mark Read, CEO of Smarter Technologies. "We pride ourselves in delivering the end-to-end solutions that our customers need. It's our knowledge and expertise, working in partnership with our clients, that enables such digital transformation programmes to succeed and enable end users to improve their critical operational decision making using real time data." ■

EDITORIAL:

Editor: Amy Saunders
amys@kadiumpublishing.com

Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Simon Waller, Peter Betts, Rob Quickenden, Adam Maruyama, Hubert Da Costa, Mark Rushton, Earle Parsons

ADVERTISING & PRODUCTION:

Sales: Kathy Moynihan
kathym@kadiumpublishing.com

Production: Karen Bailey
karenb@kadiumpublishing.com

Publishing director:
Kathy Moynihan
kathym@kadiumpublishing.com

Networking+ is published monthly by:
Kadium Ltd, Image Court, IC113, 328/334 Molesey Road, Hersham, Surrey, KT12 3LT

Tel: +44 (0) 1932 886 537

ISSN: 2052–7373

Fortra identifies Phishing as top security risk for next six months

Fortra's new '2024 Fortra State of Cybersecurity Survey' found that most organizations anticipate phishing (81%), malware and ransomware (76%), and accidental data loss (63%) will be the top security risks over the next six months, followed by social engineering (55%) and third-party risks (52%).

To address these threats, security professionals' top five cybersecurity initiatives for this year are: limiting outsider threats (such as phishing and malware) (74%), finding and closing security gaps (73%), improving security culture (66%), securing the cloud (63%), and compliance (62%).

"While these may seem like disparate concerns, they can all be traced back to the headlong rush to the cloud," said Antonio Sanchez, principal cybersecurity evangelist, Fortra. "The impacts of this rapid migration – weak policies, poor container security, misconfigurations, and gaping security holes – came home to roost in 2023 and the consequences will still be playing out this year. Now, the top focus is on improving controls and processes around phishing and malware followed by identifying the latest attack vectors for hardening. Security leaders know that improving security awareness has a direct correlation to improving phishing and malware defenses, so they have made improving security culture a top initiative as well. Improving security culture should also free up resources so they can focus on cloud security as organizations continue to adopt cloud-first and cloud-preferred strategies."

In line with this, 64% of respondents in Fortra's survey reported having a hybrid environment, while 19% were cloud-first, and 12% were cloud-only. The 6% who said they had no plans to move to cloud cited security concerns as the reason to not make the jump (77%).

The research also explored the hurdles hindering the execution of security strategies, with budget limitations (54%), the constantly changing nature of threats (45%), and lack of security skills (45%) topping the list. In addition, the survey revealed that while everyone is seeking to implement principles of zero trust, a quarter said they aren't planning to due to insufficient resources.

Many organizations are aware that upskilling needs to occur to strengthen their security position, with 67% saying they are focusing on improving the skills of their staff. Organizations are also leaning into managed security services to offload some of the weight. The most popular areas to offload are: email security and anti-phishing (58%), vulnerability management (52%), data protection (51%), and compliance (40%). ■

Complete Fibre and Raven Housing Trust address digital poverty

Complete Fibre has been selected by social housing provider Raven Housing Trust to enable the safe and strategic rollout of Full Fibre networks to its residents.

The partnership aims to support tenant welfare by unlocking an array of opportunities through improved access to full fibre broadband.

Raven owns and manages more than 7,000 homes across the South East of England, of which approximately half are MDUs. Notoriously difficult to connect, residents in MDUs are often left behind when it comes to accessing full fibre. However, the united approach between digital advisor and housing association is tackling digital poverty head on.

Poor connectivity prevents residents from accessing online work, education, healthcare, and housing platforms. Supporting tenant welfare, the rollout of full fibre allows residents to access vital online services and unlock opportunities that may not be accessible without reliable connectivity. As more services including healthcare and education rely on having internet access, the urgency to provide social housing with fast, reliable connectivity is increasing to ensure residents don't become digitally excluded.

Complete Fibre will install single, open-access 'plug-and-play' digital infrastructure within the flats to ensure safe, ultrafast, ultra-reliable broadband is available. Multiple Internet Service Providers (ISPs) can then connect into the infrastructure, ensuring Raven's residents have more choice when selecting full fibre packages whilst minimising disruption of different ISPs each installing its own infrastructure. Complete fibre infrastructure also comes at no cost to the landlord or resident. ■

Data Centre World '24 - see how EkkoSense Disrupts Data Centre Optimisation Through Machine Learning and AI

EkkoSense AI provides an entirely new way for operations teams to understand what's going on in their data centres in real-time.

Artificial intelligence and machine learning at this level change the optimisation game. AI software takes all those complex datasets and crunches the numbers in seconds. Manually, this would take weeks to attempt and most likely fail to achieve. With EkkoSense AI in place, data centre teams benefit from fully correlated real-time data that's presented in a distinctive, actionable way.

From a thermal management perspective, it's also a lot easier to identify cooling issues quickly by using comprehensive 3D digital twin visualisations. This helps particularly in terms of highlighting potential cooling anomalies and displaying suggested airflow and cooling improvements.

Additionally, augmenting measured datasets with machine learning algorithms provides operations teams with easy-to-understand insights that support real-time optimisation decisions. And because recommendations are presented each time for expert human auditability, data centre teams are always on hand to ensure that any changes are delivering the expected results.

By following these steps, operations teams can benefit from an AI and machine learning-powered, software-driven optimisation approach that unlocks significant benefits. Focused cooling performance recommendations and advisory actions help EkkoSense customers reduce their data centre cooling energy costs by up to 30% - translating directly into quantifiable carbon savings and the recovery of stranded capacity. Ensuring 100% ASHRAE thermal compliance also helps to remove thermal and power risks for data centre operations.

Visitors to the EkkoSense Data Centre World stand (D210) can view innovations such as embedded, automated ESG Reporting and new Cooling Anomalies detection functionality. DCW visitors will also get to preview the next key EkkoSense development – a unique new data centre modelling and simulation solution that draws on the EkkoSense data lake to build precise simulation models that help take the guesswork out of data centre capacity planning.

Lightning Fibre to connect social housing with full fibre internet in East Sussex

Lightning Fibre has signed a new deal that will see its multi-gigabit speed full fibre service being expanded to cover homes managed by Southern Housing in East Sussex.

The agreement means Southern Housing residents in areas including East Sussex, Wealden and Rother will benefit from having access to the new full fibre network. Southern Housing is a large UK housing provider with more than 78,000 homes across London, the South East, the Isle of Wight and the Midlands.

Lightning Fibre has also previously signed a wayleave agreement (legal land/property access agreement) with Eastbourne Homes, who own thousands of properties across the same area, as well as Orbit Homes in conjunction with Complete Fibre Group (CTG); and is also working with Trinity Homes to deliver Full Fibre to new developments, including social housing projects.

"A strong and affordable broadband and internet service is one of the five elements of digital inclusion," said Stefan Stanislawski, Lightning Fibre's CEO. "With a move towards digital services to modernise and streamline how housing associations interact with residents, an affordable internet connection is vital. Lightning Fibre will ensure people are not left behind as we help create 'Digital Britain'." ■

Average annual cost of cyber-compromise exceeds $5 million

Barracuda Networks, Inc. has published its Cybernomics 101 report, which reveals the average annual cost of responding to compromises exceeded $5 million.

The report also raises the alarm over hackers exploring how they can use generative AI (GenAI) technology to increase the volume, sophistication, and effectiveness of their attacks. 50% of respondents believe AI will enable hackers to launch more attacks. The survey also identified that 71% of respondents had experienced a ransomware attack over the last year, and 61% paid the ransom.

The research identifies the behaviours and proven security measures implemented by 'High Performers' that can serve as models for success. The report presents best practices that will help any organization become more effective in identifying, containing, and recovering from attacks. They include adopting a platform approach to security rather than relying on a collection of disparate individual security tools or solutions, implementing privileged access rights to ensure that sensitive data remains accessible only to authorized individuals, and creating (and regularly rehearsing) a security incident response plan. ■

DWP appoints Computacenter to update DC facilities

The Department for Work and Pensions (DWP) has signed a £4.86 million deal to update equipment installed in data centre facilities.

The three-year contract has been awarded to Computacenter and extendable for two additional 12-month periods.

"This contract provides DWP with the required network infrastructure, software, and support services to refresh the existing ageing infrastructure within the department's on-premises hosting (OPH) data centres," said the DWP in a statement.

Computacenter will complete a design for the new OPH and Secure Data Centre Exchange by Week 16 of the contract; once this has been signed off, delivery of the equipment will be before the end of the fiscal year 2023/24.

Computacenter is tasked with planning the transition from the current network to the new one post-installation. The provider is also required to be prepared to minimise risk and ensure there are no adverse impacts on the DWP's business operations. Computacenter will then be tasked with removing redundant equipment like the current network switches. ■

Kao Data completes £206 million debt raise via Deutsche Bank

Kao Data has completed a new, £206 million debt raise, with an accompanying accordion facility extendable to £356 million, via Deutsche Bank.

The announcement marks a significant step forward for Kao Data, providing debt financing to fast-track its new contracted developments with customers across the cloud, AI, and financial services, and the build-out of its KLON-06 data centre in Slough.

The debt facility, for which Deutsche Bank have been named mandated lead arranger and sole underwriter, will allow Kao Data to consolidate its debt with a single, large financial services organisation, refinancing those existing lenders who have played an integral role in the advancement of its secure, highly scalable, and sustainable data centre platform during the last decade.

Kao Data's new financial capability reinforces an exceptional 12 months for the organisation, which has secured several key customers from within the AI, hyperscale cloud, research, and financial services sectors. ■

Word on the web...

DC: using AI more swiftly and affordably

Earl Parsons, director data centre/ intelligent building architecture evolution, CommScope

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

SD-WAN and SASE: matching security with flexibility

Simon Waller, regional sales director, Epsilon Telecommunications

Retailers are increasingly blending online and physical storefronts, transforming how they manage data, applications, and enterprise resource planning (ERP) systems to adapt to the complex networking environment. They require massive scalability across diverse enterprise locations and must establish a flexible and secure foundation for new services.

Digital transformation demands networking models that can move with the speed and agility of the cloud, while minimising business risks. Retailers are challenged to go beyond legacy networking and adopt new solutions like software-defined wide-area networking (SD-WAN), while enhancing their security posture with Secure Access Service Edge (SASE).

It is critical that retailers evolve their networking strategies. SD-WAN provides better performance, reliability and scalability, with an optimised cost base; however, retailers must protect themselves against emerging threats stemming from modern network practices. The cloud, network expansion, and ongoing digital transformation have created vulnerabilities across many attack surfaces, including physical location-to-location or point-of-sale networks. SD-WAN alone cannot fully secure all points of vulnerability.

SASE is proving to be one of the most effective ways to tackle these potential issues. SASE integrates SD-WAN, security, and remote access into a single, global, cloud-based model. With digital transformation and cloud adoption on the rise, online threats will become more common and more dangerous.

There has been a marked increase in the number of vulnerabilities and attacks on retailers' IT ecosystems in recent years.

With the ongoing digital transformation of retail businesses, network complexity has also risen. Legacy networking often lacks the flexibility and security needed to migrate retailers' data to the cloud and accommodate new digital services.

With the increased growth of cloud and network services, security regulations have become increasingly comprehensive, exemplified by regulations. Compliance to these regulations can be difficult for retailers without prior expertise.

As the retail world forges larger connections, retailers need a secure and stable network that can counter the vulnerabilities associated with digital transformation and network expansion.

Retailers are increasingly adopting SASE because of its flexibility and ability to deliver security to any edge, while enabling a zero-trust model. By bundling SD-WAN, remote access, and security, retailers can utilise SASE's different features to enhance their security posture and benefit from agile, efficient, and fluid networking.

Through encryption, multiple layers of firewalls, and traffic tunnelling, SASE can ensure that retail networks remain insulated from attack. Retailers can maintain flexibility by scaling SD-WAN features for both on- and off-site network requirements, ensuring fast network workloads without overburdening online and physical on-site operations.

SASE's comprehensive suite of security capabilities makes it well suited to address regulatory compliance challenges. Its data loss prevention (DLP) features can help retailers prevent unauthorised access to sensitive data, ensuring it remains accessible only to authorised users. SASE's secure web gateway and firewall-as-a-service components can help retailers protect their networks from external threats, such as malware and phishing attacks, a key requirement of the Payment Card Industry Data Security Standard (PCI DSS). SASE also supports separating credit card data from corporate data by adding Business Intent Overlays (BIO), which is another PCI DSS requirement.

All of this can be centrally managed through the SASE platform, providing retailers with complete visibility and flexibility across disparate networks at multiple retail locations. This allows retailers to optimise applications, such as point-of-sale application networks, via SD-WAN's ability to prioritise business-critical applications and dynamically route traffic across any number of locations.

Moreover, SASE simplifies network management, potentially reducing costs while maintaining or even improving overall performance and agility. With SASE, retailers can fully utilise both SD-WAN and the cloud, allowing them to secure and expand their retail networks on a global scale.

With the right tools, retailers can advance their digital transformation and cloud adoption. Investing in cloud connections brings many benefits, from security to efficiency, for any retailer looking to migrate their retail services online.

SASE offers retailers looking to enter today's cloud-centred business landscape a means to alleviate many of the issues that come with online activities. Retailers that adopt SD-WAN and SASE can seamlessly migrate their data, applications, and ERP systems online, while also improving their location-to-location networks. With this approach, retailers can rapidly expand their business in line with the digital economy and confidently navigate the digital ecosystem. ■

Current approaches can't mitigate the AI cybersecurity threat. What can?

Adam Maruyama, field CICO, Garrison

A recent National Cyber Security Centre (NCSC) report represents a much-needed shift in the AI security dialogue from the very real implications that AI has for information operations and intellectual property rights. The report looks to the near future when AI will make it easier for hackers to identify targets, trick them into opening malicious content, and deploy harder-to-detect malware and ransomware into target networks. By examining each of these steps in the attack chain in sequence, it becomes clear that even supercharged versions of current approaches will be insufficient to counter this threat. Instead, proactive security that leverages robust technical controls to move risk away from users and outside the network are necessary.

Reconnaissance and social engineering: making it easier to trick users

The first two capabilities that AI will enhance for hackers are reconnaissance and social engineering – meaning that hackers will have an easier time identifying their targets and have generative AI's help in creating content that is compelling to them. For example, a hacker could use an AI research assistant to identify targets of interest at a company, enumerate their interests and contacts, and craft targeted phishing emails for each of them impersonating trusted members of their network or an announcement from their children's school.

Companies are already struggling with the trust and morale implications of phishing simulations, which seem to be the security method of choice to counter phishing emails. It's hard to conceive that sending even harder-to-detect phishing training emails to users will increase the rate of success, and even harder to conceive that generating tailored phishing campaigns on a per-user basis won't have severe privacy concerns that have legal, ethical, and trust implications for employers and employees alike.

Tools and exfiltration: evading traditional technical countermeasures

The predicted uplifts that AI will provide to the tools and exfiltration capabilities, particularly for highly capable state actors, mean that technical exploits like ransomware or other malware will have a better chance of taking hold in a target network, and adversaries will be more likely to be able to extract sensitive data from those networks without being detected. Adversaries will also be able to generate a greater number of unique signatures for their malware, making 'crowdsourced' signature-based threat intelligence even more difficult.

Faced with a more protean technical threat, it's clear that current detection and response technologies are not up to the task. Adversaries will be able to leverage AI capabilities to better hide their ingress points to the network, and there's already evidence that advanced nation state APTs like VOLT TYPHOON are focusing on low-profile, living off the land (LotL) tactics to avoid being kicked out of critical infrastructure networks. Even if similar AI algorithms to the ones attackers are using can be leveraged on the defensive side of cybersecurity – as they already are by numerous vendors – AI makes it more likely that a few well-crafted attacks would make it into target networks and more effectively be able to either remain in place or identify and exfiltrate target data.

Toward a more proactive security model

The common thread running through current cybersecurity approaches, and what renders them ineffective against the high-volume, highly-adaptable threat posed by AI-driven attacks, is their reliance on detecting that content is malicious before doing anything about it. Creating a security model that is resilient against this threat requires inverting this model and trusting only sites and code that has been scrupulously reviewed and treating all other content as inherently risky and potentially compromised.

A prime example of such an approach is the use of robust remote browser isolation (RBI) technology to shield users from the browser-based risks of phishing and ransomware. Remote browser isolation pushes processing of non-trusted websites outside customers' network perimeter, rendering endpoints safe from technical exploits while providing users with real-time awareness that they are interacting with a non-trusted environment. Hence, users and endpoints are protected from the potential exploits behind their 'first click,' and users are reminded of the risk before entering data into what could be a spoofed site designed for credential harvesting.

By isolating the vast majority of the 1.1 billion websites on the Internet from corporate networks, RBI can significantly mitigate the risk of AI-based attacks that would otherwise overwhelm the human and software-based detection algorithms that are the bedrock of anti-phishing and endpoint security today. Turning to develop similar technologies that treat more and more content as untrusted, rather than trying to mitigate the effects of a 'trust by default' network security model, provides a much more robust alternative to engaging in an offensive vs defensive 'arms race' using AI capabilities. ■

Networks in an AI world

The future of networks is on an unknown trajectory amidst paradigm-changing new technologies like AI shaking up the market. We speak to the experts to find their views for 2024 and beyond…

Enter chief AI officer…

There's no denying that 2023 was the year of artificial intelligence (AI). Hitting the headlines of all major IT/networking publications throughout the year, the impact of AI on the networking and IT space is only beginning to make itself felt.

Still in its infancy, Apricorn's managing director, EMEA, Jon Fielding, believes that 2024 will see more use of AI assisted data management, aiding businesses to automatically classify data according to whether it is relevant, valuable, or risky, to decipher which they should retain or remove, greatly assisting data retention strategies.

"In doing so, the business can conserve costs by saving a huge expense on unwarranted data storage space. Using AI to automate the process of classifying data also improves the efficiency of data compression with AI algorithms, again limiting the required storage space and the time needed to retrieve stored data," explains Fielding. "Those businesses that look to embrace the use of AI for data management in the coming year will reap the cost and performance benefits to data storage systems in the long term, as well as bettering their data security defences."

However, "despite all the hype around AI and generative AI, the technology is far away from being able to automate and optimise every aspect of our lives anytime soon," says Mark Pierpoint, VP of strategic innovation and partnerships, Keysight. "AI is making progress; however, automating a chatbot or creating a digital assistant are constrained problems that are much easier to automate. When it comes to helping manage real-world processes such as optimising call quality on a 5G network or managing energy consumption, these are incredibly complex operations, with a wide array of variables requiring vast unbiased data sets before AI can be effective."

Jim Liddle, chief innovation officer at Nasuni, asserts that the rush for an AI advantage is surfacing deeper data infrastructure issues that have been mounting for years: "AI doesn't work in a vacuum and it's just one part of the broader data intelligence umbrella," he says.

Many organisations have implemented data analytics, machine learning (ML) and AI into their sales, customer support, and similar low-hanging initiatives, but struggle to integrate the technology in more sophisticated, high-value applications.

"Visibility, for example, is a crucial and often-overlooked first step towards data intelligence," adds Liddle. "A shocking number of companies store massive volumes of data simply because they don't know what's in it or whether they need it. Is the data accurate and up to date? Is it

"Given the rapidly changing landscape, a pressing priority for businesses to consider in 2024, and one highlighted by Frank de Jong, programme director edge computing, CTIO office, Orange Business, is AI in the C-Suite and at board level: the role of chief AI officer has just emerged."

properly classified and 'searchable'? Is it compliant? Does it contain personal identifiable information (PII), protected health information (PHI), or other sensitive information? Is it available on-demand or archived? In the coming year, companies will be forced to come to terms with the data quality, governance, access, and storage requirements of AI before they can move forward with digital transformation or improvement programmes to give them the desired competitive edge."

Although AI is providing a competitive advantage for those that can leverage it effectively, Thomas King, CTO at DE-CIX, explains that many companies lack the internal resources to enable the development and operation of their own AI models.

"Here, AI from the cloud and AI as a Service (AIaaS) providers offer convenient alternatives. For these, optimised connectivity to clouds and specifically to the AIaaS providers is an essential component for ensuring low latency and high bandwidth, and thus better performance of chatbots, analytics, and other tools," says King.

Given the rapidly changing landscape, a pressing priority for businesses to consider in 2024, and one highlighted by Frank de Jong, programme director edge computing, CTIO office, Orange Business, is AI in the C-Suite and at board level: the role of chief AI officer has just emerged.

"AI technology developed rapidly through 2023 improving efficiencies in many departments within businesses. I predict that the speed of development will be maintained at a similar trajectory, and even increase in tempo, throughout 2024, which means that the time for businesses to internally consider the ethical development of AI technology is now," says de Jong. "Orange Business urges enterprises to put in place someone who can champion and lead this development from within… Things are going to move fast."

AI holds great promise for organisations of all sizes this year, but change won't be instant, nor necessarily even that fast. Industry experts believe that we'll be looking at several years of pilots, tests, and upgrades while those in the value chain get to grips with all that AI has to offer.

"While the intelligence will

New challenges in security

As digital transformation ramps up, never has cybersecurity been a more pressing challenge. Networks will experience tensions as the need for emerging technologies must be balanced with the operation and maintenance of legacy systems.

"There was no let-up in the sophistication of cyberattacks in 2023 with organisations left reeling from the impacts of attacks and the heightened geopolitical situation worldwide continues to be unstable, increasing the risks to organisations," says Alan Hayward, sales and marketing manager, SEH Technology. "IT staff are facing increasing administrative burdens and security risks; software solutions to help them overcome those challenges will continue to have a real place in the coming years."

And there's always a new cyber threat or type of attack that organisations fear – this time it's AI.

"The race between security teams fixing vulnerabilities and threat actors exploiting them will continue, however, it will be done by AI instead and at a much faster pace," says Rob Bolton, VP EMEA, Versa Networks. "There will be a greater focus on augmenting our human analysts with AI. Success among security teams will be measured by having applications that can surface anomalies hidden in the telemetry details to solve security issues, rather than just asking your teams to work harder."

Indeed, while AI will pave the way for threats, it will also form the bedrock of a variety of enhanced security solutions.

"In 2024, we'll see the proliferation of AI and generative AI platforms being integrated into security tools, allowing huge amounts of data to be processed much more quickly, which will speed up operations such as instant response," says James Hinton, director Of CST Services, Integrity360. "Where AI can triage data quickly and provide the results, organisations won't necessarily require skilled analysts to write custom queries. AI can be used to complete such tasks, freeing up highly skilled security professionals to focus on higher value tasks."

Given the type of cyber-threats that plagued organisations in 2023, it's no surprise that ransomware is one of the biggest concerns among UK enterprises for the year ahead.

"In 2024, we'll see more ransomware incidents in the UK as government agencies, health services, and critical infrastructure continue to lack the technology and funding to build adequate data protection and recovery capabilities," says Liddle. "Organisations that haven't addressed their data protection and recovery posture are now risking both security and compliance headaches, as regulatory penalties and recovery costs often outmatch ransom payouts. By delaying their investment in protection and compliance solutions until forced to, many large organisations will soon face the possibility of steep penalties, ransom demands, and business disruption simultaneously."

Remote desktop protocol (RDP) has long been the initial entry vector of choice for ransomware groups, closely followed by email. However, last year's MOVEit and SysAid campaigns evidence that change is brewing.

"We've observed an increasing number of zero-day vulnerabilities being exploited by ransomware groups, and it's unlikely this trend will abate. Forget the mindset that ransomware actors just go after 'the low hanging fruit'; they are now exploiting zero-day vulnerabilities at mass scale," says Raj Samani, SVP chief scientist, Rapid7. "This trend is seeing criminal groups that to date have not demonstrated any real capable skills in gaining access to previously unidentified vulnerabilities, exploit them and gain a foothold into victim networks. This demonstrates that potentially something is afoot in the ransomware ecosystem." ■


Jon Fielding


James Hinton


Don Valentine

undoubtedly help us in 2024, realistically, AI will not be ready to direct physical-world activities until the end of the decade," opines Pierpoint.

The changing face of storage

Data storage faces several significant challenges/opportunities coming into 2024 and beyond; capacity, security and, of course, AI.

"Many organisations that are reliant on data centres are reporting that their most pressing issue right now is one of capacity. A growing number of data centres are full, and don't have the space or power available to deploy new platforms," reports Fred Lherault, field CTO EMEA/emerging markets, Pure Storage.

This will result in widespread efforts to achieve efficiency gains to reclaim space and power to accommodate the use of new technologies. "We'll see operators looking to switch to new, more power efficient technology, with smaller space and cooling requirements; in essence extending the life of the data centre - an essential factor when considering the need for new technologies in the wake of the rise of AI," adds Lherault.

Moreover, as data generation continues to explode in line with digital transformation and AI adoption, so does its lifespan.

"At the end of the day, your data will outlive you," says Tim Sherbak, enterprise products and solutions marketing, Quantum. "This means your organisation must have a plan for its long-term management and ongoing platform infrastructure today. How can it be easily curated, accessed, and analysed in the future when the current experts are no longer present, plus, the need to ensure that data is always durably protected. This includes implementing an evolutionary storage architecture that can seamlessly adopt and decommission across multiple generations technologies and platforms for decades to come at a cost that doesn't break the bank. It's no longer just an option to consider the 'far future' of your data – it's a requirement for organisations focused on a fully digital-enabled future."

Data storage security, too, remains an ongoing but increasing concern: "I expect we'll see a growing trend in organisations moving data away from the public cloud globally in the next 12 months. It's also something that will drive budget decisions, as IT leaders determine whether to apportion budget from the cloud to use instead for on-premises storage for certain data types," says Guillaume Crapart, senior director of channel sales, Quantum. "The semi-private cloud is another storage option I believe we'll see rise in popularity in 2024, as organisations seek to have their cloud-based data closer to home and subjected to stronger security measures than the public cloud allows for. In combination with the cloud-also trend, organisations will gain more privacy and control over their data - a must in today's digital world."

Interestingly, the rush to develop and implement generative AI solutions is leading to a new wave of adoption of containers and Kubernetes from data scientists and developers.

"There's a growing realisation that containers are fundamental to AI at almost all stages, in that every AI tool is packaged in containers," says Patrick Smith, field CTO EMEA, Pure Storage. "They are also vital to the success of the hard part of AI – training large language models. Before a model can be trained, many processes must be performed, including data curation, cleaning, and amplification. The tools that perform these tasks all reside in containers."

According to Smith, there have been two waves in the rise of containers and their evolution: "the first was stateless, which involved workloads going into containers, the second was stateful, with databases and critical applications moving to containers, requiring data storage. We're now entering a third wave, with containers driving and enabling the AI data pipeline and toolchain."

Meanwhile, with AI already transforming data centres, huge investments are being triggered by cloud service providers to build out AI fabrics to keep pace with demand.

"In 2024, look for intense focus and investment in GPUs and other back-end infrastructure for large learning clusters," says Stephen Douglas, head of market strategy, Spirent. "Cloud service providers will also be looking to beef up front-end inferencing and investing in faster interconnect technologies to enable it. We expect Ethernet to dominate these front-end networks, and for 800G adoption to grow rapidly among Tier-1 cloud service providers next year as 51.2Tbps switches reach the market."

Indeed, global spending by businesses on cloud is forecast to top $1 trillion for the first time in 2024, driven by factors like adopting new tools such as AI.

"The cloud computing industry is set to change significantly. A trend expected to see gaining momentum is the adoption of software as a service (SaaS) public cloud offerings as part of next-generation ERP systems," shares Don Valentine, commercial director, Absoft. "This shift builds upon the recognition that merely moving existing ERP systems to the cloud does not automatically trigger innovation. Instead, it is the combination of cloud infrastructure with cutting-edge ERP products that propels businesses toward digital transformation."

The surge in AI adoption has so far had a limited impact on the cloud computing market, "however, it is expected to have a more noticeable influence once the offerings from major hyperscale cloud providers become more widely available and commercialised," says Lee Thatcher, head of cloud, CloudCoCo. "As these providers continue to invest in AI capabilities, businesses will increasingly leverage cloud platforms for AI-related workloads, driving the growth of cloud-based AI applications and services. Therefore, it'll continue to be about AI for the foreseeable future."

"Interestingly, the rush to develop and implement generative AI solutions is leading to a new wave of adoption of containers and Kubernetes from data scientists and developers."

Mergers, acquisitions, and subscriptions

According to all reports, companies are waking up from the post-covid hibernation, with much more M&A activity expected in the coming 12 months.

"The days of only working with the big globally recognised vendors, who likely have been the mainstay in the security stack long before the current security team was formed, is gone," says Bolton. "As a result, these older and more established companies are looking to acquire these start-up and scale-up companies to absorb the ingenuity held within them and repackage it as a differentiator for themselves before their value gets too high."

Despite this, continued concerns about the economy, difficult business conditions and high energy costs will have a significant influence in 2024, accelerating the trend towards OpEx spending over CapEx.

"Money is tight and continued belt-tightening in the coming year will make technology subscription services very attractive as customers only want to pay for what they use, avoiding the need for large CapEx outlays," agrees Lherault. "It makes sense to opt for a subscription to a service and avoid CapEx expenditure when there's a reasonable possibility that a CapEx asset will not be used to full capacity."

The 'as a service' model will, however, only gain traction if backed by relevant SLAs, since buyers are becoming increasingly discerning about what to invest in.

"This trend is also being observed in data centres, with operators beginning to favour on-demand models that enable just-in-time provisioning of assets," says Lherault. "This allows them to better control energy costs through lower power consumption, which also helps them realise their sustainability goals."

All in all, 2024 looks like a year of great change for the IT community. AI continues to bring huge advances – but also huge threats – to all aspects of the network, everywhere, changing and challenging the operating environment like never before. ■

'Dark NOC' will enter the lexicon of the networking world

Amit Dhingra, executive vice president, network services at NTT Ltd.

"With the speed at which AIOps has advanced, the idea of a completely automated, lights out Network Operations Center is quickly becoming an ideal. Over the next 12 months, we will see networking companies further embed AIOps into their broader operations to improve network quality, support engineers, and modernize infrastructures.

While automation lays at the heart of a 'Dark NOC,' human talent will be key to making it a success. Network providers will need to focus on upskilling, as well as ensuring they have made the necessary preparations from a technological standpoint – from standardizing APIs to optimising data processes.

Networking specialists must understand where automation helps and where human talent is still an essential part of the networking function. ■"

Innovation needed: SF6-free switchgear to reduce environmental impact

Peter Betts, engineering director, VIRTUS Data Centres

Switchgear plays a crucial role in maintaining the seamless operation of power networks due to its essential functions in the electrical infrastructure – serving as a protective device that enables the control, isolation, and distribution of electrical power. However, the widespread use of sulphur hexafluoride (SF6) gas in switchgear presents an environmental challenge.

With a Global Warming Potential (GWP) tens of thousands of times worse than carbon dioxide, and annual emissions growing (SF6 rose 24% between 2008-2018), SF6 poses a threat to climate stability and global warming. Furthermore, accurately tracking the release of SF6 gas in developing countries is challenging, indicating that the level of SF6 released into the atmosphere may be underestimated.

The environmental impact of SF6 gas: unveiling the challenges

Switchgear, an essential component of power systems, relies on SF6 gas due to its unique properties that make it ideal for insulation and arc-quenching purposes. However, with a GWP far exceeding carbon dioxide, and the fact that when exposed to high temperatures, SF6 transforms into a harmful powder, SF6 poses severe risks to human health.

Today, the wider understanding of the potency of this gas and the need to reach net zero carbon emissions by 2050 is causing a rethink of the use of SF6 gas, so the need to address this issue has become increasingly apparent. It's imperative for the data centre industry and other electricity-intensive sectors to take the lead in tackling this environmental concern. By championing innovative switchgear solutions that eliminate the use of harmful SF6 gas, these sectors can showcase their commitment to driving sustainable, technological advancements and pushing the boundaries of efficiency and effectiveness.

Leading the charge

While the European Community has taken steps to eliminate SF6, the UK is yet to implement such regulations. But, even in the absence of legislation, it is crucial for the industry to drive innovation and make environmentally responsible choices. By actively advocating for SF6-free switchgear and encouraging its adoption, data centre operators can demonstrate their commitment to environmental responsibility and sustainability and lead by example.

Due to its energy usage, the data centre industry has the buying power to create market demand for SF6-free switchgear. And in pushing for its use, operators can incentivise manufacturers to invest in research and development, leading to the development of more environmentally friendly solutions. This market demand-driven approach which prioritises innovation, can lead to a wider adoption of sustainable switchgear solutions in other industries such as renewable energy production and electric vehicles.

Considering the alternatives

To reduce the environmental impact of SF6 gas in switchgear, some data centre operators are actively exploring and adopting sustainable alternatives. These include air-insulated switchgear (AIS), vacuum-insulated switchgear (VIS), the development of new gases with lower GWP and solid insulation solutions.

AIS relies on air as the primary insulation medium, significantly minimising the environmental impact compared to SF6 and VIS utilises a vacuum as the insulation medium, eliminating the associated environmental risks of SF6 gas. Researchers and manufacturers are also dedicatedly working on developing alternative gases with lower GWPs like nitrogen, carbon dioxide and fluoroketones. Solid insulation materials not only offer excellent electrical insulation properties but also eliminate the need for greenhouse gases.

There are plenty of viable alternatives, and although the adoption of these solutions may require adjustments in design, engineering, and manufacturing processes – and many are currently in their infancy - the rising demand for SF6-free switchgear is expected to drive improved affordability. Whilst the cost implications of adopting SF6-free switchgear are not yet fully understood, driving market demand will likely lead to improved affordability. As more manufacturers invest in research and development and scale up the production of alternative switchgear solutions, economies of scale can drive down costs. The more stakeholders express their preference for SF6-free switchgear, the more favourable the cost-benefit equation becomes.

A bright future ahead

Addressing the environmental impact of SF6 gas in switchgear necessitates a collaborative effort across diverse sectors that are reliant on electricity. By advocating for SF6-free switchgear, the industry can drive innovation and facilitate the development of environmentally friendly alternatives.

Data centre operators should demonstrate their commitment to mitigate climate change by inspiring the industry and catalysing a transformative shift towards sustainability, paving the way for a greener and more sustainable electrical ecosystem. Through collective action and shared responsibility, the industry can forge a path towards a brighter and more environmentally conscious future. ■

Improving ISR missions success rates: the growing role of Change-Bitrate-on-the-Fly technology

Mark Rushton, global defence and security lead, VITEC

Intelligence, Surveillance and Reconnaissance (ISR) missions are rarely executed in controlled laboratory environments — quite the opposite. The platforms — from airborne drones to terrestrial and underwater remotely piloted vehicles (RPVs) — that carry ISR payloads are often deployed in the harshest conditions and connected to users and operators over wildly inconsistent communication networks.

"The ability to ensure high-quality images, regardless of network conditions in a theatre of operations, has emerged as a critical success factor for ISR activities that depend on video-based intelligence to establish situational awareness and support effective decision-making."

The ability to ensure high-quality images, regardless of network conditions in a theatre of operations, has emerged as a critical success factor for ISR activities that depend on video-based intelligence to establish situational awareness and support effective decision-making.

This is where Change-Bitrate-on-the-Fly technology comes in.

Change-Bitrate-on-the-Fly technology: what is it and why is it essential to the ISR mission?

When talking about video streaming, we often focus on bitrates, which are measured by considering how many frames are taken every second, along with the size of each frame. The higher the video quality, the more images are needed to process for each second of video, which, of course, results in higher bitrate requirements.

Change-Bit-Rate-on-the-Fly technology is an increasingly important feature for the ISR community because it directly affects the quality and timeliness of tactical field intelligence. Receiving information too late because of network latency or being unable to understand what is being analyzed because of dropped packets that result in fuzzy or pixelated images can mean the difference between life and death.

In many ways, the need for Change-Bit-Rate-on-the-Fly capabilities reflects the technological progress that has allowed more sensors with greater capacity to be loaded on ISR platforms — such as drones or helicopters. Innovations around ISR have led to cameras that capture video images in stunning detail and sensors capable of detecting subtle temperature changes in the environment, including ground-penetrating radar. As a result, more information can be shared from a single ISR platform than before.

It does, however, create a challenge.

While devices to capture this wide array of data are becoming increasingly advanced, there are still challenges associated with the wireless networks used to access the data in terms of bandwidth, capability and change.

Change-Bit-Rate-on-the-Fly is a technology that can help address network constraints by adapting the bitrate as it changes.

What challenges leads to network constraints or variability?

The ISR community has done a lot of excellent work in adopting standards across the technical elements needed to capture, share and act on digital intelligence. As a result, most platform and payload technologies can use almost any wireless network in the field to maintain connectivity — and, therefore, the flow of intelligence.

The agility and flexibility that enable drones and other RPVs to use multiple networks means these platforms can dynamically switch from a cellular network to a satellite link and then to a terrestrial mesh network.

However, as these platforms shift from one data carrier to another, they will likely experience a difference in bandwidth available to support the data traffic. Sometimes, that delta can be quite significant. A cellular network might deliver up to 100Mbps in connectivity only to switch to a satellite signal that supports a fraction of that capacity.

The other challenge revolves around the roving nature of ISR platforms. The quality and strength of wireless signals are better when platforms are near antennas. The signals weaken as the distance from antennas grows.

While the connectivity environment is highly dynamic – with bandwidth fluctuating from total capacity, only to be cut by half and then a third of capacity — the overall ISR objective of sharing the highest quality image possible remains the same.

That's why Change-Bitrate-on-the-Fly is a differentiator for IP video applications on ISR platforms. With it, we can make changes dynamically in real-time to ensure the continuity of images at the highest possible quality. This can't be underscored enough because video in a live environment is crucial for ISR. It represents a major improvement over the previous ISR video capabilities. With Change-Bitrate-on-the-Fly, ISR teams can execute their missions with confidence. ■

Digitally transforming East Midlands Railway

East Midlands Railway (EMR) connects people across the East Midlands and through to London. Working in partnership to connect cities, support communities and create easier journeys for everyone, EMR is investing £600 million bringing customer improvements to its services, trains, and stations.

"To facilitate these significant infrastructure and service improvements, EMR needed to increase its network connectivity capacity by a factor of four, while also adding previously unconnected greenfield station sites to its network for the first time."

As part of this investment, the company is improving its trains and introducing a new intercity fleet, as well as refurbishing two new, faster, and more modern regional fleets. To keep passengers up to date, they have launched a new website, mobile app and ticket buying facilities, while encouraging Smartcard use to help reduce paper waste and streamline the travel experience.

Meeting Department of Transport obligations

To facilitate these significant infrastructure and service improvements, EMR needed to increase its network connectivity capacity by a factor of four, while also adding previously unconnected greenfield station sites to its network for the first time – representing approximately one-third of their overall station estate. This was an obligation put to EMR by the Department for Transport to ensure it could provide excellent passenger connectivity across all EMR stations.

Key to delivering these objectives was upgrading and replacing legacy IT infrastructure hardware, software and services inherited by EMR when they took over the franchise. The existing technologies were not only both costly and unstable; they didn't provide the data connectivity needed by 21st-century passengers, who expect to be able to use their digital devices at all times.

Digital transformation with SD-WAN

Node4 provided a comprehensive response to EMR's tender process alongside offering flexibility around delivery and terms, all supported by competitive commercials. This included the availability of its Midlands data centre for EMR server hosting, extensive networking capabilities and references from businesses EMR had experience working with.

The digital transformation solution comprises fully managed, secure SD-WAN connectivity across 104 EMR sites, six racks of colocation space within the Node4 data centre, and offsite backup services providing 60Tb of capacity. The sites were broken into five key bands; head office locations, depots and Category A, B and C stations. Key milestones included the hardware build, fixed line delivery (Ethernet, FTTC and xDSL circuitry) and mobile connectivity, with most connectivity services deployed within six months of site readiness completion.

Quadrupled connectivity

The Node4 solution has provided EMR with significantly more bandwidth at previously connected sites and connectivity into previously greenfield locations (where EMR had no network infrastructure before the project was initiated).

"We saw huge improvements in our key 'Category A' stations with footfall increases going from 100Mbps connectivity to dual 300Mbps connectivity," said Lee Styles, head of IT at East Midlands Railways. "A great example of this is our critical station in Nottingham, which increased from 20 Mbps to dual 300Mbps."

Overall, EMR experienced quadrupled bandwidth of previous capacity at 70% of its stations and doubled capacity at a further 12%, achieving its Department for Transport obligation. Moreover, levels of 'acceptable' connectivity rose from approximately 30% to 100%.

Total Cost of Ownership was significantly improved, with connectivity across each site now costing thousands of pounds less per year to operate than before, with the upgraded and newly installed infrastructure acting as a catalyst for EMR to implement more effective retail solutions – an average cost reduction of 40% per station. This includes upgraded ticket machines, smart ticketing, new customer information screens and a major expansion of station WiFi performance for customers.

"Working with Node4 on this key digital transformation initiative has enabled us to enhance the passenger experience while significantly improving performance and reliability," said Lee Styles, head of IT at East Midlands Railways. "Our partnership with Node4 has been a positive experience and has played an important role in driving the development of a data culture within EMR – something we see as crucial to the long-term strategy of the business and our ability to deliver an excellent service to our customers."

Looking ahead, EMR is also focusing on adding Network Access Control, Access Points for Category C stations and SOC services that can be extended to and integrated with the existing SD-WAN asset investments. ■

Northern moves toward intelligent trains

Northern's passenger WiFi service works by utilising the available cellular capacity in the geographical areas its trains pass through, to deliver data to those on board.

With over 340 trains travelling on its network, and an average of more than half a million users connecting to its WiFi every month, data usage (and, in turn, costs) could quickly begin to add up. What's more, this data expenditure was largely outside the transport operator's control, given that the provision of WiFi to rail passengers is mandated in the UK.

Snowballing data usage

Pre-pandemic, Northern was expecting to quadruple its data spend because of ballooning usage. When COVID-19 hit and lockdowns were enforced, Northern saw a sharp wind-down in data use; however, as lockdowns eased in the summer of 2021, and passengers began to return to public transport, data consumption started to rise steadily again.

Northern also noticed a shift in how its passengers were using the onboard WiFi service; more and more passengers were travelling for leisure, while the shift to hybrid working meant that business travellers were seeking to use the onboard WiFi network in different ways (e.g. for video conferencing).

Delivering a high-quality WiFi service was therefore more vital than ever for overall passenger satisfaction levels in the 'new normal'; however, due to the finite bandwidth available from cellular networks, the onboard WiFi connection could quickly become 'clogged up' when large numbers of Northern's passengers were seeking to use the service simultaneously. This could result in a less than optimal WiFi experience for its travellers, if left unchecked.

Given the substantial amount of data that it handles and the rising associated costs, Northern sought a solution which would allow it to control and mitigate its data spend, while still being able to offer the best possible experience for its passengers connecting to the onboard WiFi.

Enabling the modern railway

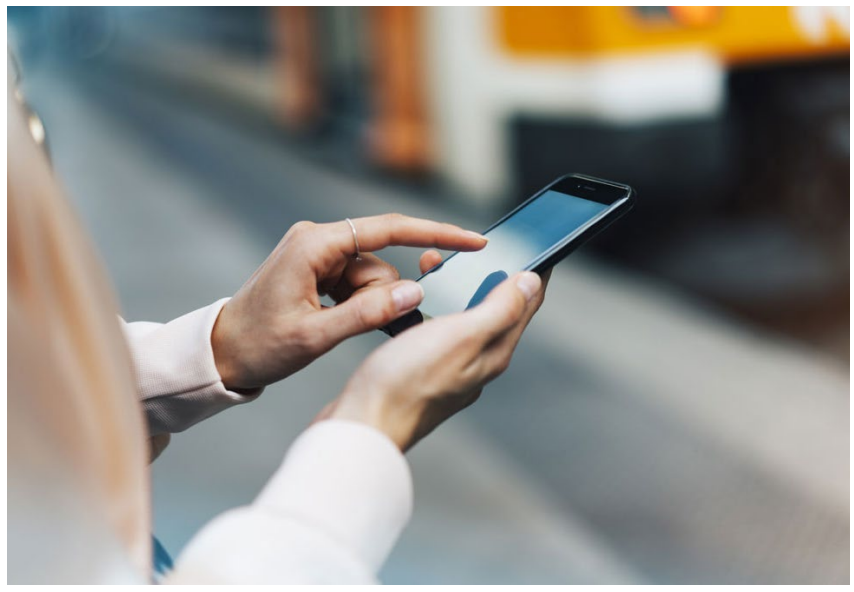
To help address these two aims, Icomera deployed its IcoShape solution as part of a competitive trial. By categorising network traffic, IcoShape allowed Northern to gain a deeper understanding of how data was being used, and to take the appropriate action. It was possible to monitor and analyse whether data spend was coming from passenger services or from operational systems, for instance.

Northern was able to configure WiFi usage rules using a web-based graphical interface integrated within ICONIC, Icomera's cloud-based monitoring software tools. Data traffic streams could be prioritised, throttled, or blocked depending on their level of importance, to better manage data usage and costs. For example, traffic for critical onboard systems such as digital video surveillance or real-time journey information could be prioritised, while still delivering the best possible WiFi for Northern's passengers.

"Northern was able to configure WiFi usage rules using a web-based graphical interface integrated within ICONIC, Icomera's cloud-based monitoring software tools. Data traffic streams could be prioritised, throttled, or blocked depending on their level of importance, to better manage data usage and costs."

The deployment resulted in no detrimental impact to passenger satisfaction levels; in fact, Northern saw an improvement in the overall passenger experience because it could provide a fairer, more reliable WiFi service for all (as opposed to a small number of passengers 'hogging' the available bandwidth).

Northern experienced a tenfold return-on-investment using IcoShape, as well as achieving an average 20% reduction in its data consumption.



"IcoShape has allowed us not only to better maintain our cost portfolio, but also to increase the customer benefit through delivering a more reliable WiFi service across our network," said Marc Silverwood, digital trains project manager, Northern.

As a result of the trial's success, Northern selected Icomera to rollout IcoShape fleet-wide; this was a simple task given that Icomera's connectivity solution allows for over-the-air deployment, in the click of a button.

"Northern continues to be one of the UK's most forward-thinking rail operators. We're thrilled that, thanks to our close working relationship, it has been able to reap the rewards of being an early adopter of innovative Icomera solutions, such as IcoShape," said Peter Kingsland, SVP UK, Australia & Asia, Icomera.

Icomera continues to work closely with Northern to leverage IcoShape's different use-cases, and to align the tool's feature roadmap to the transport operator's business goals. ■

Will your network let down your AI strategy?

Rob Quickenden, CTO, Cisilion

As companies start to evaluate how they can use AI effectively, there is a clear need for the network engineering teams to first ensure the network is up to the challenges of AI. AI applications are going to require data to be easily accessible and the network will need to be able to handle the huge compute needs of these new applications. It will also need to be secure enough at all points of access for the different applications to end users' different devices. If the network isn't reliable, readily available, and secure, it is likely going to fail.

In Cisco's 2023 Networking Report, 41% of networking professionals across 2,500 global companies said that providing secure access to applications distributed across multiple cloud platforms is their key challenge, followed by gaining end-to-end visibility into network performance and security (37%).

So, what can you do to make your organisation's network AI ready?

Enterprise networks and IT landscapes are growing more intricate every day. The demand for seamless connectivity has skyrocketed as businesses expand their digital footprint and hybrid working continues. The rise of cloud services, the Internet of Things (IoT), and data-intensive applications have placed immense pressure on traditional network infrastructures and AI will only increase this burden. AI requires much higher levels of compute power too. The challenge lies in ensuring consistent performance, security, and reliability across a dispersed network environment.

Use hybrid and multi-cloud to de-silo operations

According to Gartner's predictions, by 2025, 51% of IT spending will shift to the cloud, underscoring the importance of having a robust and adaptable network infrastructure that can seamlessly integrate with cloud services. This is even more important with AI as it needs to access data from different locations and sources across the business to be successful. For example, AI often requires data from different sources to train models and make predictions. A company that wants to develop an AI system to predict customer churn may need to access data from multiple sources such as customer demographics, purchase history and social media activity.

Network engineering teams need to make sure that they are using hybrid cloud and multi-cloud to de-silo operations to bring together network and security controls and visibility and allow for easy access to data. When businesses use multiple cloud providers or have some data on-premise, they need to review how that data will be used and how to access it across departments.

Install the best security and network monitoring

It's clear that as we develop AI for good, there is also a darker side weaponizing AI to create more sophisticated cyber-attacks. There needs to be end-to-end visibility into the network performance and security to be able to provide secure access to applications distributed across multiple cloud platforms. This means having effective monitoring tools in place and the right layers of security – not only at the end user level but also across your network at all access points.

Being able to review and test the performance of your SaaS based applications will also be key to the success of your AI solutions. AI requires apps to work harder and faster so tasting their speed, scalability, and stability, and ensuring they are up to the job and can perform well under varying workloads is important.

Secure Access Service Edge

The best way to ensure network security is as good as it can be is to simplify the tools and create consistency by using Secure Access Service Edge (SASE). This is an architecture that delivers converged network and security as service capabilities including SD-WAN and cloud native security functions such as secure web gateways, cloud access security brokers, firewall as-a-service, and zero-trust network access. SASE delivers wide area network and security controls as a cloud computing service directly to the source of connection rather than at the data centre which will protect your network and users more effectively.

SD-WAN connectivity

If you haven't already, extending SD-WAN connectivity consistently across multiple clouds to automate cloud-agnostic connectivity and optimise the application experience is a must. It will enable your organisation to securely connect users, applications and data across multiple locations while providing improved performance, reliability, and scalability. SD-WAN also simplifies the management of WANs by providing centralised control and visibility over the entire network.

As we head towards the new era of AI, cloud is the new data centre, internet is the new network, and cloud offerings will dominate applications. By making your network AI ready, by adopting a cloud-centric operating model, having a view of global Internet health and the performance of top SaaS applications, it will mean you will be able to implement your company's AI strategy successfully. ■

Can DCIM cope with the reality of GenAI workloads?

Dean Boyle, CEO, EkkoSense

With data centre management busy coming to terms with the realities of hosting high-density AI systems, it's clear there's going to be an increased pressure on data centre optimisation as teams work to make their operations as lean as is practical.

Generative AI applications present teams with some very practical engineering challenges. How do you continue to balance risk, capacity and cooling when you'll be running racks at 60kW – and potentially up to 100kW? That's a huge difference for halls that were originally designed to host traditional 3-5kW racks. What are you going to do about cooling? And how can you be sure you have the right solutions in place when you may be running multiple data centres worldwide?

Getting ready for GenAI workloads at 10x the power

Data centers are already looking to support 20% plus increases in workload levels even before GenAI. With this in mind it's clear that managers need a comprehensive and sustained commitment to data centre performance optimization. With AI compute workloads estimated to consume around 10x the power of standard deployments, the ability to either save power or release stranded capacity to increase IT loads will be critical.

Operations teams will need to unlock every possible area of improvement across their own data centres, those of colocation service partners, and edge facilities. Achieving this will require new levels of insight into existing thermal performance, power provision and capacity management – levels of insight that simply cannot be achieved by relying on traditional legacy Data Centre Infrastructure Management (DCIM) and Building Management Systems (BMS) tools.

What action should managers be taking?

So what needs to change? Unfortunately, many data centres aren't starting from a good place, and that's hardly surprising when so many legacy facilities are over a decade old and often still operating to their original design parameters. At EkkoSense we believe it's difficult to unlock the kind of cooling, power and capacity performance improvements that are needed to handle greater workloads and secure energy savings unless you know exactly what's happening in your data centre in real-time. We also believe that this won't be achievable unless data centre management commit seriously towards bridging the gap between their IT and M&E functions.

While the latest digital services and core business applications may run on leading-edge platforms, it's still the traditional facilities management teams that manage and maintain the building and the critical supporting infrastructure within it. However, most IT teams have little interest in the underlying Monitoring and Evaluation (M&E) infrastructure that provides the power and cooling that enables their services to run. Because of this, it's not unusual to see expensive power and cooling resources being used inefficiently. Excess energy usage not only gets in the way of corporate net-zero initiatives, but also potentially places organisations at risk when IT loads increase or critical resources suddenly become depleted or unavailable.

Need to make the invisible visible

This is perhaps why legacy DCIM data centre management tools, which largely come from the IT side, often fail to address the very real M&E needs of data centre operators – especially in terms of capacity management and overall energy efficiency. With rack load densities increasing, sites expanding, and expert resources stretched, the reality is that data centre teams with traditional DCIM systems in place may actually have very little time to react to problems that could be escalating quickly.

That's why EkkoSense is focused on complementing the capabilities of traditional DCIM-style data centre optimisation with a distinctive AI-powered approach that enables true real-time visibility of cooling, power and capacity performance. We believe that the only truly reliable way for data centre teams to troubleshoot and optimise performance is to gather massive amounts of data from right across their estates – and then leverage the power of machine learning and AI to help teams understand not just what's happening but also why.

The good news for data centre managers is that this latest generation of AI-powered data centre optimisation software can extend the potential of their existing BMS and DCIM investments – helping their operations teams to stay on top of their escalating workloads and ESG reporting requirements. ■

PRODUCTS

Raritan's Power IQ DCIM Monitoring Software enables data centre and facility managers to closely monitor and efficiently utilize their existing data centre power infrastructure.

Data centre health maps, power analytics, cooling charts, and reports alert the user to potential trouble, and help understand real-time power load, trends, and capacity at all levels of infrastructure. A configurable dashboard provides vendor agnostic views of power capacity, environmental health, and energy consumption.

A complete environment management solution that helps identify potential trouble areas, save energy, and maintain a safe environment for your IT equipment. Power IQ works with Raritan's PX intelligent rack PDUs and Smart Rack Controller, an all-in-one sensor management device, to support plug-and-play environment sensors that monitor temperature, humidity, air flow, air pressure, leaks, vibrations, and more. See trends, get alerts, save energy, and increase uptime.

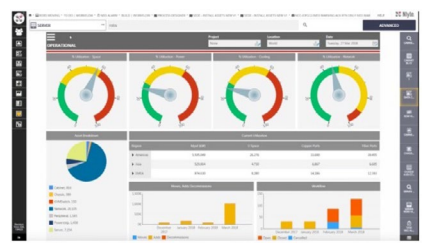
Power IQ monitors and measures all the energy usage in the facility including building meters, UPSs, Floor PDUs, RPPs, busways, rack PDU's, branch circuits, environment sensors, and IT devices. Increase data centre temperature without risk, calculate Green Grid's PUE Level, and drive green data centre and sustainability initiatives with bill-back reports.

Nlyte's DCIM software solution automates the management of all assets, resources, processes, and people throughout the entire lifecycle of the computer infrastructure.

DCIM software provides full visibility of all assets in a data centre, allowing IT teams to monitor energy usage and receive alerts when thresholds are exceeded. DCIM software also helps with data centre design and infrastructure planning, helping determine the optimum placement of new hardware. This translates to more efficient data centres, lower operating costs, and increased productivity.

Every asset in a data centre facility has a limited lifecycle. DCIM software enables the monitoring of the performance of existing assets over time and measure them against established benchmarks.

Benefits of Nlyte's DCIM include detailed information about assets and environment; robust dashboards and reporting; flexibility to work in any environment; support for goods receiving, provisioning, changes, tech refresh, and decommission.



Schneider Electric's comprehensive DCIM solution, EcoStruxure IT, addresses the challenges of DCIM 3.0 by modernising the software portfolio for monitoring and management of sprawling, hybrid IT infrastructure, which has become increasingly complex in the last few years.

The vendor-neutral solution enables resilient, secure, and sustainable IT data centres. It offers business continuity with secure monitoring, management, planning, and modelling from a single IT rack to hyper-scale IT, on-premises, in the cloud, and at the edge. Software services help implement the value of EcoStruxure IT solutions to drive business growth and achieve desired results.

Benefits of EcoStruxure IT include reduced OpEx and downtime while gaining instant visibility into infrastructure in the cloud or on-premises; increased resiliency and monitoring; and enhanced insights into the complete data centre, the big picture to individual devices.

FNT's Data Center Infrastructure Management (DCIM) solution is a central resource management and optimization software for the data centre, covering documentation, planning, and management of all data centre resources and facilities throughout their entire lifecycle.

Businesses that use FNT's DCIM software can streamline processes and optimize utilization of building infrastructure (power, cooling, floorspace), IT infrastructure (networks, servers, storage), connectivity (cables, patches) and services (software, applications). The solution provides consistent, up-to-date, and easily accessible data that is vital for informed decisions on deployment of data centre infrastructure resources and capacities. It is a field-tested solution based on the powerful FNT Command Platform that delivers a comprehensive and integrated view of all data centre resources. From recording and monitoring live power consumption and temperature values to planning the entire data centre, FNT's DCIM software will keep a data centre operating with maximum efficiency.

The needs for data centre management are evolving constantly and the move to colocation, virtualization, and hybrid infrastructure adds new aspects to management processes. DCIM should therefore be selected not just by looking at todays' needs, but with the future of data centre operations in mind. Features such as planning, including cable management and network aspects, or vendor-agnostic support for all equipment models are critical for the long-term value of a solution.

Please meet...

Hubert Da Costa, CRO, Celerway

Which law would you most like to change?

I'd like to make it easier for people to access any country they want. It'd give people better opportunities to take their lives in the direction they choose, whether that's working, living, or studying abroad. We live in a global world, so it makes sense to have that flexibility.

What was your big career break?

My big break came when I joined Symbol Technologies as Global Alliances Director back in 1999. It was about more than just the sales and relationship-building skills that I learned while I was there, my whole perspective changed. I went in as a do-er and came out as an enabler. I've been building on those leadership skills ever since and being in the position I am now, where I can inspire others, is something I highly value. There's so much more to business than the metrics you're accountable for. The real value comes with the outcomes you enable for your customers and the difference you make to their lives with the solutions you create for them. These values are at the heart of how I see my role as Chief Revenue Officer at Celerway.

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

Coming from an Indian heritage family, if you'd asked my traditionalist parents, they'd have said I should pursue a career in medicine or law. But I knew from an early age that I was interested in tech, and I spent many happy days as a boy playing with Pentium computers, which were cutting edge at the time. I was fascinated by how they worked and the things you could do with them, and from that point my direction for a career in tech was set. Having said that, I'm also a people-person, so working in sales has always come naturally to me. I'm so lucky to have found a career where I can bring these two passions together and I get real enjoyment from the work I do.

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

Ah, that's an easy one, it'd be Tim Peake. I admire people who have that adventurous spirit and the courage to break new ground. I'm always challenging myself to push my limits because that's how you grow as a person. Tech is a great enabler in astronomy, and I'd love to find out what it's really like to brush your teeth in zero gravity.

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

When I was just starting out in my career, someone once said, "be true to yourself". The wisdom of these words didn't truly resonate with me until I was a few years older, and I realised that if you do what you enjoy rather than what someone else thinks you should be doing, you'll always find happiness. I can hand-on-heart say that I enjoy every day at Celerway because I'm working with talented people to deliver transformational technology into the hands of our customers.

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

Working at NASA would be incredible. I can imagine there's an amazing vibe in a company that exists to take humans into new and previously undiscovered spaces. It'd be great fun to brainstorm around new space missions or how to embed the latest tech into rockets. It'd feed my innate curiosity as well as my drive to find new and exciting ways of doing things.

The Rolling Stones or the Beatles?

That's a tough one because they were both such pioneering bands, but if I have to choose, it's the Beatles. I admire the way they brought different musical genres together and paved the way for future artists, they're even influencing songwriters now. Listening to Paul McCartney on the piano always takes me to a happy place.

What would you do with £1 million?

Beyond taking care of my family and making our lives financially secure, I'd set up an educational trust fund for people who wouldn't otherwise have the opportunity to learn. Education is the single most powerful hope for our society because it advances our ways of thinking so we can meet today's challenges and be ready for tomorrow's. As a dedicated fan, I might also treat myself to a Liverpool FC season ticket.

What's the greatest technological advancement in your lifetime?

The internet. I remember Tony Blair labelling it as the "information superhighway" and that was a great metaphor, although now we could maybe even take that into an intergalactic sphere too. The internet is still revolutionising everything in the world, from the ways we work to how we communicate and even interact with everyday objects. It's mind boggling. We've come so far from the early days of popping into the library to use a computer to where we are now with smartphones in our pockets and wearables on our bodies. Now we have entire generations of digital natives who have never known life before the internet. Even my four-year-old niece is a tech whizz – I guess it must be in the genes. ■