JUNE 2022
networkingplus.co.uk

NETWORKING+

The IoT data deluge

Effective data storage management tips

David Keegan, DataQube Global, p13

Pushing the boundaries

Making the most out of solutions

Terence Ledger, Sepura, p14

Questions and answers

'Why I would love to live in Chile'

Chris Dyke, Allied Telesis UKI, p16

Government launches consultation on data centre, cloud security

The UK government has begun a consultation on data storage and processing to strengthen the security and resilience of local data centres and cloud services.

Companies that run, purchase or rent any element of a data centre have been asked to detail the types of customers they serve.

The Department for Digital, Culture, Media and Sport (DCMS) is seeking views from data centre operators and their customers, cloud providers, equipment suppliers and cyber security experts – to help the government understand the potential risks that data storage and processing services is facing.

This includes detailing what measures are in place and what steps they are already taking to address any vulnerabilities.

"We legislated to better protect our telecoms networks and the internet-connected devices in our homes from cyberattacks and we are now looking at new ways to boost the security of our data infrastructure to prevent sensitive data ending up in the wrong hands," said Julia Lopez, minister of state for media, data and digital infrastructure.

It also seeks feedback on putting in place processes seen in other regulated sectors – these include incident management plans, having to notify a regulator when an incident impacts their services, or a requirement for someone at board or committee level to be held accountable for security and resilience of the infrastructure.

Based on the evidence collected, DCMS said it will then decide whether any additional government support or management is required to minimise the risks to data storage and processing infrastructure.

Jon Anthony, founder Adappt.ai and the Hub.ai told *Networking+* that "in the world of cloud data security, every dependency is an opportunity for a back door". He added: "Even in the vaunted world of Open Source, compiled code, back doors are hidden in plain sight. The only true solution is a standards-led approach. Personally, the most effective hardening technique I have seen is the automation of hacking tools such as Kali Linux and Metasploit to perform high volume combination exploit testing."

Jason Sabin, CTO with DigiCert, added: "The UK government is doing the right thing seeking counsel from security experts. Protecting data centers and cloud assets is complicated and includes stringent physical and network security, continuous monitoring and compliance with industry regulations. Achieving digital trust through proven means like PKI is essential to secure data centres and the cloud assets."

The DCMS stated that any new protections would build on existing safeguards for data infrastructure, including the Networks and Information Systems (NIS) Regulations 2018 which cover cloud computing services.

Nigel Thorpe, technical director at SecureAge, said a focus on maintaining and improving the cyber-resilience of data centres and cloud services is clearly very important. "However, we must not lose sight of the fact that it is often the endpoint which is the weakest link," he said. "It is the point at which the least cyber-security aware people operate, and, until we all install the modern equivalent of the old 'dumb terminal' on our desks, potentially sensitive information is frequently downloaded to the local PC."

Martin Walsham, director of cyber security, AMR CyberSecurity, added: "Recent complex attacks such as the widely publicised Solar Winds hack demonstrate how supply chain and IT providers are both vulnerable and actively targeted by well-resourced and capable adversaries."

The consultation will run until July 24. ■

Alexander Stadium gets ready for the Games pp8-10

Yodel disrupted by cyberattack

Delivery service company Yodel has suffered a "cyber incident" resulting in widespread disruption across its network.

Customers awaiting deliveries noted that the company's systems went offline the weekend before last and that they have been unable to receive updates since then.

In a message posted on its website, Yodel said: "We are working to restore our operations as quickly as possible but for now, order tracking remains unavailable and parcels may arrive later than expected."

Although the company is still able to make deliveries, it has advised customers to expect delays across its network.

Yodel has not revealed how it was attacked, but early reports suggest that it was targeted by ransomware. The damage appears to be primarily related to service disruption, as opposed to the exfiltration of personal data.

"Reports of a cyberattack against Yodel causing disruption to its services demonstrates the importance of cyber preparedness," said Lawrence Perret-Hall, director, CYFOR Secure. "Having an incident response and forensic readiness plan in place, deployable at any time, is crucial in the event of a business-critical attack. And with business continuity playbooks readily available, disruption can be kept to a minimum. This is even more important when considering Yodel was targeted at a weekend, a common tactic cyber criminals use in an attempt to avoid immediate detection.

It could take weeks to fully restore systems. Yodel is still required to fulfil its data breach notification requirements. ■

Surrey, Sussex Police use Motorola's Pronto for INTERPOL

Surrey Police and Sussex Police are using Motorola Solutions' Pronto to secure immediate access to the comprehensive international criminal database of the world's largest police organisation, the International Criminal Police Organization (INTERPOL).

Officers will be provided with important information to protect national security and enable daily productivity gains.

Pronto is the most widely deployed mobile policing solution in the UK, improving public safety through features that enhance situational awareness including mobile biometrics and federated searches.

The new service will equip 4,500 police officers across both forces with the INTERPOL database, ensuring instant and secure access to millions of international records including warrants, stolen property and threats related to weapons.

"Pronto has been a part of the digitalisation of our police force since 2009", said Amber Kingshott, mobile development manager, Surrey Police. "With access to INTERPOL, our officers no longer need to call a colleague or return to a police station to run a search, saving minutes in everyday operations and emergency situations."

Steve Boniface, detective chief superintendent, Sussex Police, added: "It takes an average of 1.2 seconds to run a query through the INTERPOL database using our mobile device. "Officers can run a search from any location at any time, leveraging INTERPOL's vital source of intelligence to increase safety for themselves and the British public."

Motorola said secure access to INTERPOL is now available to all Pronto customers at no additional cost. Furthermore, the solution is fully compliant with INTERPOL's commitment to privacy and data protection. ■

Secure I.T. Environments completes phased DC upgrade for Three Rivers District Council

Secure I.T. Environments, the design and build company for modular, containerised and micro data centres, has completed a multi-phase major upgrade project for the main data centre at Three Rivers District Council.

The site, at the main offices in Rickmansworth, provides essential digital services to public sector staff and those used to support the local services that the district council provides.

The multi-phase project covered the following areas: server room UPS upgrade (phase 1), server room flooring replacement (phase 2), energy efficient AHU upgrade (phase 3) and fire suppression (phase 4).

"At each stage of our major upgrade project, Secure I.T. Environments has delivered professionally in its consulting and on-site implementation of the work," said Gary Cook, data centre manager at Three Rivers District Council. "Our project involved, multiple areas of works in a live data centre, and the team at Secure I.T. completed all the works on time and to our expected standards."

Chris Wellfair, projects director at Secure I.T. Environments added: "Whether building a new data centre, or undertaking major upgrade projects, we work very hard to ensure consistent standards and a minimum of disruption for our clients, with particular care and attention to those data centre services that need to remain live throughout the works." ■

North wins £7m contract with City of York Council

IoT service and solutions provider, North, has secured a £7m contract to transform digital connectivity and network security for City of York Council.

Under the terms of the deal, North will work with the City of York Council to future-proof its facilities to enable faster and safer access to digital services in line with requirements following the Covid-19 pandemic.

Council buildings and schools across the city of York will now benefit from a digital transformation contract that puts flexible working, safety, security and connectivity at the heart of operations.

North will oversee a range of new security measures across the network, new digital tools to allow both internal and external threats to be monitored and faster and more flexible Wi-Fi to support a mixed working environment.

Local schools will be able to enhance their learning environments and operate more efficiently, both parties said.

The project places security at the heart of City of York Council's operations, both within corporate workplaces and in educational establishments, to ensure a safe environment following an increased use of online services and flexible working policies during the pandemic.

"Our digital infrastructure has transformed multiple council services, improving efficiency, effectiveness and informed decision making," said councillor Nigel Ayre, executive member for finance and performance at City of York Council. "It helped us to very quickly adapt to the pandemic, allowing us to continue working in a secure way, as we supported residents and businesses whilst having to work from home."

Mark Lowe, business development director at North, added: "Digital services have become the essential foundation to deliver enhanced public services across local government with a blended-online approach now commonly adapted in workplaces. Therefore, to ensure businesses are able to operate effectively these structures must be kept up-to-date and secure." ■

EDITORIAL:
Editor: Robert Shepherd
roberts@kadiumpublishing.com
Designer: Ian Curtis
Sub-editor: Gerry Moynihan
Contributors: Simon Michie, Terence Ledger, Florian Malecki, Alan Jones, Jonathan Bridges, Norman Rice, Simon Wilson, Sam Durrant, David Keegan, Martin Riley, Nicolas Roussel and Chris Dyke

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

Gov publishes response to Data Reform Bill consultation

The government has pledged to make several changes it claims will boost businesses, protect consumers and seize the "benefits" of Brexit, in its response to a consultation on the impending Data Reform Bill.

At their core, the reforms hinge on the government's belief that the European Union (EU) General Data Protection Regulation (GDPR), which transposed into UK law as the UK GDPR after Brexit was finalised, held organisations back from using data in a dynamic way.

It said there was a lack of clarity in the GDPR that led to an overreliance on box ticking, and that the regulation was overly reliant on a one-size-fits-all approach that failed to account for the unique needs of disparate organisations, placing a particular burden on small and medium enterprises (SMEs) and startups. It is these burdens the government is set on removing.

Outlining how it plans to diverge from European Union-based data protection rules, the government's proposals include clamping down what it perceives as red tape around privacy and data protection to save an estimated £1bn, while strengthening data protection standards and reforming the Information Commissioner's Office (ICO). Along with giving innovators and researchers more flexibility in how they use data in their work, the government wants to increase fines for people who misuse data.

Outlining its response at the end of London Tech Week, the government said that data was core to the UK economy, with data-driven trade generating 75% of the country's services exports and revenues of £234bn in 2019 and touched how businesses operate.

"Today is an important step in cementing post-Brexit Britain's position as a science and tech superpower," said digital secretary Nadine Dorries. "Our new Data Reform Bill will make it easier for businesses and researchers to unlock the power of data to grow the economy and improve society but retains our global gold standard for data protection." ■

NHS Digital launches £9.5m innovation framework

Technology companies can tender to provide digital services to help healthcare professionals as part of a new NHS GP tech innovation framework.

NHS Digital says any supplier can bid to become part of the framework, which has been designed "to encourage new ways of working" for doctors and other primary healthcare professionals. Up to £9.5m has been ringfenced as part of the framework.

Interested companies can submit a tender for the tech innovation framework if they can provide a solution that delivers at least six core functions of an electronic health record. These are: patient information maintenance, appointments management, recording consultations, prescribing, referral management and resource management.

GPs and commissioning groups will be able to access these technologies in a bid to deliver "better care and work effectively", according to NHS Digital. This is the third framework to launch under the Digital Care Services Catalogue and will run alongside GPIT Futures and Digital First Online Consultation and Video Consultation frameworks.

NHS Digital said this new framework will help expand the core clinical systems available in the GP IT market by encouraging innovation and moving towards an open cloud-native.

The tender invitation says that by using public cloud-based solutions, GPs and commissioning groups can offer significant usability and accessibility improvements, making systems "easy to use, intuitive and compliant with latest standards".

Suppliers can apply from August 15. ■

Vertiv Releases First Environmental, Social and Governance Report

Columbus, Ohio [June 28, 2022] – Vertiv (NYSE: VRT), a global provider of critical digital infrastructure and continuity solutions, today released its inaugural environmental, social and governance (ESG) report, the company's first public report of its ESG activities.

The report outlines Vertiv's approach to energy and water efficiency; diversity, equity and inclusion (DE&I); employee health and safety; and other ESG-related topics. The content covered in the report serves as a baseline upon which the organization will build future efforts.

"We all know how critical connectivity is to our daily lives and the global economy. The world's appetite for data continues to rise, and our solutions keep data systems on and connected. At the same time, we recognize the current and potential impacts of climate change," said Rob Johnson, Vertiv CEO. "We are seeking to meet the growing demand for critical digital infrastructure, and simultaneously mitigate environmental impacts from our operations and products. As a result, we're innovating to come up with more efficient and effective ways to support critical digital infrastructure."

Vertiv's ESG Executive Steering Committee, made up of senior leaders from across the organization, is driving a company-wide evaluation of ESG performance. Some of the activities and results highlighted in the report include:

- The introduction of new and upgraded products with high energy and water efficiency attributes, with others planned for release in the coming months and years.
- Participation in several industry partnerships aimed at addressing data center efficiency and emissions, including the EcoEdge PrimePower Project (E2P2), the Sustainable Digital Infrastructure Alliance (SDIA), the European Data Centre Association (EUDCA), and the RISE Partnership Program.
- An internal review of Vertiv's Scope 1 and 2 greenhouse gas emissions.
- Development of performance and improvement benchmarks to help the organization reduce operational greenhouse gas emissions.
- A 12% year-over-year reduction in recordable injuries based on the U.S. Occupational Safety and Health Administration's total reportable injury rate (TRIR).
- The introduction of training opportunities to support the organization's global focus on diversity, equity and inclusion.
- The appointment of multiple women to executive positions within the company within the last two years, including Sheryl Haislet, Chief Information Officer, and Stephanie Gill, Chief Legal Counsel.

For more information or to download the full report, visit Vertiv.com

Nearly £250k worth of devices stolen under LSE's watch

London School of Economics and Political Science (LSE), a leading research institution, has recorded nearly £250,000 in stolen electronic devices, including laptops, tablets and phones, over the past five years according to official figures. The data which was retrieved via the Freedom of Information Act (FOI) and analysed by the Parliament Street think tank, observed the number of stolen electronic devices from LSE year on year from 2017 to 2022, as well as the total cost of devices lost.

In total, £242,744 worth of devices were listed as stolen, with laptops, tablets and phones accounting for 78 per cent of the devices. Overall, the 208 stolen laptops, tablets and phones totalled £189,934 worth of lost devices, with 126 laptops, 61 phones and 21 tablets reported as stolen. The news comes following the government's Cyber Security Breaches Survey, revealing that an alarming 92% of universities have been targeted by a cyber-attack in the past 12 months. ■

Prysmian connects Colchester with super-dense fibre cable

Colchester is the latest city to get super-fast fibre connectivity with an innovative FTTX system that will place one of England's oldest towns among the best-connected places in the UK.

The brand-new Prysmian cable system provides customers with speeds of up to 1Gbps, both upstream and downstream. This technology will allow local businesses and enterprises to upload and download digital assets much faster over a more reliable, safer connection and therefore improve productivity. To make this possible, Colm Coyle, managing director of Rio IT and designer of the installation, 'searched high and low' for a cable that was up to the task.

"The challenge was that we needed to find a way of bringing the existing cable infrastructure forward more than 20 years, in a way that would not be outdated for a long, long time – if ever," he explained.

Coyle specified 26km of 552 Sirocco HD fibre cable for the project, supplied by Fusion Utilities, to be installed by Scotech in a ring around the city. This particular cable is made up of 552 individual G657A2 fibres, with a fibre density of up to 10.5 fibres per mm2. It utilises Prysmian's BendBright-A2 200μm single-mode (ITU-T G.657.A2) bend insensitive fibre, allowing it to retain enough flexibility to be bent around tight corners without being damaged. ■

Extreme's new suite of solutions

Extreme Networks has introduced a suite of new solutions, creating new ways for customers to drive better outcomes from their networks in the era of the infinite enterprise. The company has extended its ExtremeCloud portfolio to include new SD-WAN and AIOps with digital twin capabilities – enabling customers to deliver secure connectivity at the edge of the network, speed cloud deployments and uncover actionable insights – all from within a single platform. With Extreme's new SD-WAN offering, enterprises can, among other things, simplify management by enabling customers to manage wired, wireless and SD-WAN from a single platform. ■

Corel adds zero trust tech following Awingu acquisition

Corel, the creativity and productivity solutions vendor, has acquired Awingu, a provider of secure remote access technologies, adding the acquisition to the Parallels brand portfolio. The acquisition brings zero trust security at the browser level to customers who need to access the cloud, legacy and workspace-based apps and resources. Adding Awingu to the Parallels Remote Application Server (RAS) tech stack also solves clients' challenges of securely working with legacy apps, on-premise assets, hybrid cloud architectures and the fast-growing base of software-as-a-service (SaaS) applications all organisations have. Awingu is a browser-based Unified Workspace that allows users to work and collaborate virtually anywhere using any device compatible with HTML5 browsers. ■

Teledata to open new Manchester DC

Cloud hosting and data centre operator TeleData will open a new data centre facility in South Manchester later this year. The new facility will see the firm open up to 10 more data halls with 25,000 sq ft of floor space and 4MVA of power, designed to accommodate over 500 new server racks. Since 2020, the operator has opened three new data halls at its Manchester campus, taking the total number of halls up to five. "As a data centre provider we have a responsibility to our clients to ensure that continuous capacity is available," said Matt Edgley, director, Teledata. ■

Green Mountain enters UK

Norwegian sustainable colocation provider Green Mountain is expanding into the UK through the acquisition of Infinity SDC's last remaining data centre in the London Borough of Havering. In a statement announcing the acquisition, the buyer's parent company, Israeli public real estate investment firm Azrieli Group, said it had agreed to acquire the data centre and some adjacent land with a view to using that to expand the existing facility further. The site will also be upgraded to meet Green Mountain's "strict sustainability standards", confirmed the statement, although it is already 100% renewably powered. ■

Hibernian signs security pair

Scottish Premiership club Hibernian has signed a multi-year partnership with data protection and security business Acronis and connectivity provider Dunedin IT. The former will provide hybrid cloud solutions for backup, disaster recovery, secure file sync, and data access, to become Hibernian's Principal Cyber Protection Partner. This partnership will be supported by the expertise of Dunedin IT, which will deliver Acronis cyber protection solutions to improve data storage and access, creating a more efficient and collaborative workflow. "Acronis is trusted with the cyber protection of some of the biggest institutions in European football, namely Manchester City, AFC Ajax, Atlético Madrid and Inter Milan," said Hibernian's commercial manager, Murray Milligen. ■

Funding boost for planned DC campus

The panned development of a 700,000 sq ft data centre campus in Sutton, Cambridgeshire, is set to become a reality after the site's owners agreed a new funding package. Property investment company, Topland Group, has agreed to refinance Camro Data Park on behalf of owner Lasercharm through a £9.25m, two-year facility from its structured finance division. Anish Vora of Topland Group said Camro Data Park has "an exciting future", and with an ever-growing demand for data storage, we are pleased to have helped bring it one step closer through our senior facility". ■

Word on the web...

Digital transformation is about more than just WFH

Sergio Budkin, director of market development, Virgin Media O2 Business

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

Edge computing moves service-providers to the centre of enterprise transformation

By Simon Michie, CTO, Pulsant

Edge computing's radical departure from the standard cloud model presents service-providers and application-builders with new markets and a platform for innovation.

Bringing computing power to the edge of the cloud, close to where organisations generate and use it, accelerates digital transformation, regardless of an organisation's location. In the UK, the edge gives businesses beyond the South East, where the hyperscalers are situated, access to low latency digital services, enabling them to use a vast arsenal of powerful new SaaS applications.

For SaaS vendors, the edge opens the door to millions more customers and latest subscription and delivery models. Application-builders and providers can orchestrate the network functions and computational infrastructure needed for secure delivery to their end consumers. Content providers are able to offload from their central servers, transforming access and efficiency.

We already see exciting use cases supported by 5G-enabled edge computing. Including remote monitoring and diagnostics in healthcare along with 3D medical imaging, while the availability of low-cost, easily-deployed sensors extends the internet of things (IoT) and Industry 4.0 applications that include artificial intelligence (AI) and flexible automation requiring near real-time responses. In manufacturing, automated, high complexity production will be possible in new locations. In port management and logistics, edge computing delivers major gains in efficiency across expansive campuses and along supply chains. Multi-party gaming, advanced drone use, AR and VR applications are all enabled by edge computing.

The potential is such that Statista estimates the worldwide edge market will grow to $250.6bn as soon as 2024. By 2030, the number of devices connected to the internet could reach 125 billion according to IHS Markit.

This dramatic growth depends on low latency. Augmented reality, virtual reality and most Industry 4.0 IoT implementations require latency as low as 1ms to 10ms. Edge-located machine learning (ML) models also require low latency once they are trained on masses of data in the cloud. As well as enabling organisations to deploy ML when they otherwise could not, edge computing reduces the costs of backhaul to the main hyperscalers' hubs.

However, the success of edge computing requires service-providers and end-users to have access to a scalable national network of edge data centres to ensure that, regardless of location, they have low latency, high-bandwidth connections. The more advanced edge platforms achieve sub 5ms latency, using a networking approach that spreads the load across several regional data centres. They not only process data closer to each end-user but reduce the congestion in backhaul that undermines performance.

Edge data centre networks must have high-speed connectivity to cloud services so transfers of data to the central hub are seamless, with route diversity to ensure resilience in the event of outages. And as more enterprises use edge-reliant applications, there must be sufficient capacity to meet future demand for bandwidth.

Partnering with one provider with a nationwide network of cloud and data centres, rather than a collection of multiple providers will also deliver benefits in terms of security and remove the complexities of integrating IT services. If solution-builders and service-providers are serious about expanding into all corners of the country their customers will also need access to a platform that has a good geographical spread of strategically-located sites that are purpose-built, and which maximise coverage in any area.

Since many organisations will balance their workloads between the public, private clouds and the edge for reasons of flexibility, security and cost, edge data centres need to facilitate hybrid patterns of use and multi-cloud models. They should sit between the on-ramp to the public cloud and network-to-network interfaces with the telecoms providers. This functioning edge ecosystem also needs to include specialists in microservices, containerisation, virtualisation and related fields.

We can see how ecosystems are developing, as telecoms and hyperscalers form partnerships with existing edge computing platforms. Last year, for example, Telefonica Germany partnered with AWS and Ericsson to virtualise its 5G core network. The purpose is to enable quick integration of new applications, removing the need for time-consuming hardware set-ups while reducing costs.

The edge also requires partnerships between the big-name public cloud vendors and edge providers so that organisations deploying advanced applications have the flexibility to locate workloads where they work best. Service-providers should be looking out for edge providers that have these relationships in place as well as the vital attribute of ubiquitous low latency coverage and high-speed fibre connections between centres.

For service-providers and solution-builders, the new maturity of edge computing opens the main gateway to new markets and the ability to create new products and business models that deliver higher levels of service and increased revenues. Yet to be successful, it still requires a smart selection of partners. The right edge computing platform will transform the fortunes of SaaS providers and put them at the centre of digital transformation for thousands of new customers.

The bottom line is that through edge data centres, businesses can easily power their growth, their entry into new markets and delivery of new services to almost anywhere, therefore meaning solution-builders can provide products and services built on analytics, AI and machine learning. ■

Pushing boundaries for critical communications

Terence Ledger, worldwide sales director, Sepura

Public safety organisations are increasingly being challenged for resources and time, so users need to make the most of the powerful communications solutions that have been invested in.

Modern digital radios are capable of much more than just voice communications, although this remains their primary mission critical capability. Two critical areas for deploying advanced communications solutions are sharing mission critical data and enabling wireless radio programming.

Sharing mission critical data

The ability to communicate both voice and data on a secure, encrypted device opens the door for the deployment of intelligent applications to support users.

This plays an important role in helping to ensure better situational awareness for team leaders, enabling smarter operational decisions to be made.

Data can be shared from a variety of sources, dependent on an organisation's operational procedures. Examples can include:

- Health data from attached devices, such as heart rate monitors
- Location data, based on Bluetooth or Wi-Fi connected geofences. Team leaders can see where operational staff are located and what their status is, and can assign tasks according, improving efficiency
- Job dispatch information, sent from the control room to specific individuals or teams. Radio users can quickly accept roles, or indicate if further resources are required.

Data can also be manually entered by the radio user and sent over the network. This can be used to confirm routine maintenance tasks have been completed and that specific messages have been received.

Benefits of Data Sharing

Organisations that share this key data over existing networks can reduce costs by maximising the use of their existing hardware, while improving efficiency by enabling improved situational awareness. Voice channels are kept clear for emergency communications while field users can use data sent to their radio to refer to when required.

Enabling over the air programming

Lengthy, resource-heavy procedures such as re-programming radios can be a significant logistical challenge, with radios based in multiple locations and shift working affecting when they can be made available for upgrades.

Improved connectivity options on modern TETRA radios via secure Wi-Fi makes available the option to update radios remotely as a fleet or in controlled groups, as and when suits the operation.

This is significant as it makes the reprogramming and radio update much simpler, more efficient and more flexible around operational needs. Using Sepura's established Radio Manager programming tool, administrators can upgrade all SC Series radios across a fleet, whether they are used in vehicles, based in control rooms or hand-held models.

Over the Air Programming enables organisations to change many aspects of a radio's setup; options include amends to a radio's configuration, phonebook or talkgroup updates, enabling feature licenses, installation of AppSPACE applications or the upload of crucial data.

Wireless programming vastly reduces the risk of radio downtime; rather than requiring every fleet radio to be in one central location for the process, the fleet programmer can programme multiple radios, at a set time.

Radios can be based in disparate locations such as satellite offices or vehicle parking lots. As long as they are connected to a trusted and approved secure Wi-Fi connection, the update can be deployed. By synchronising the fleet upgrade, organisations can avoid the operational issues that may arise due to out of step configuration between radios normally faced via the wired programming method.

Downloading data to the radio does not interrupt any communication and does not require user intervention. Users can continue with their duties while downloads run as a background task. Once downloaded, the user is still in control and triggers the installation process at the next radio switch off.

These solutions are available for users of Sepura's advanced SC Series TETRA radios, used by major public safety and other mission critical organisations around the world. ■

Healthcare is now the industry most targeted by hackers: here's how organisations can defend themselves

By Florian Malecki, executive vice president marketing, Arcserve

Healthcare data breaches reached a record high in 2021. Indeed, healthcare now sees more cyberattacks than any other industry. Fully one-third of all cyberattacks are aimed at healthcare institutions. Why? Because healthcare is a valuable and vulnerable target.

Hackers go after healthcare because patient data and hospital systems are lucrative prey. Hackers know they can demand a high ransom if they compromise patient data or healthcare systems. They also know healthcare organizations will likely pay the ransom — and fast because compromised data and systems can cost lives in a hospital setting. Hospitals, of course, rely on constant and immediate access to patient data to deliver care. If they don't have that access, people may get sicker and die. Almost one-fourth of healthcare institutions hit by a ransomware attack in 2019 and 2020 reported increased patient death rates after the attack.

Unfortunately, attacks on healthcare will only increase in the years ahead. Indeed, some hacking groups focus solely on attacking healthcare organizations. In April, the Department of Health and Human Services warned the healthcare industry about "an exceptionally aggressive" ransomware gang called Hive dedicated to targeting healthcare and favours double extortion. It demands one payment to unlock data it has encrypted and another payment to prevent the data from being publicly released.

Ransomware works by traversing through all copies of your data, including primary, secondary, and backup data. Attackers then encrypt or exfiltrate the data. One of the most practical and effective ways to secure backup data against a ransomware attack is air gapping.

There are two types of air gapping. The first is traditional, physical air gapping, in which an organization disconnects the digital asset from all other devices and networks. This air gapping is the ultimate cybersecurity measure because it creates a physical separation between a secure network and any other computer or network. Using a physical air gap, organizations store backup data on media such as tape or disk, then disconnect these media entirely from their production IT environment.

The second type of air gapping is called logical air gapping. A logical air gap relies on network and user-access controls to isolate backup data from the production IT environment. It's like a one-way street on which data is pushed to its intended destination, whether a storage device on-premises or a custom appliance. The key here is that the control and management of that data, such as how it is retained or who can modify it, is not available through that same system or path. Anyone who wants to manage or alter the data must go through entirely different authentication channels.

The beauty of air gapping is that it makes it nearly impossible for ransomware to compromise your data backups. It's almost as if your data is wearing a cloak of invisibility, making it impervious to any malware that manages to enter your network.

Healthcare organizations can deploy a second measure against ransomware, 3-2-1-1 data protection. It means maintaining 3 backup copies of your data on 2 different media, such as tape and disk, with 1 of the copies placed offsite to enable quick recovery. Further, you should have 1 immutable object storage copy of your data and 1 air-gapped copy. Immutable object storage protects data continuously by taking a snapshot of it at 90-second intervals. So even if a ransomware attack occurs, you can recover your data right away.

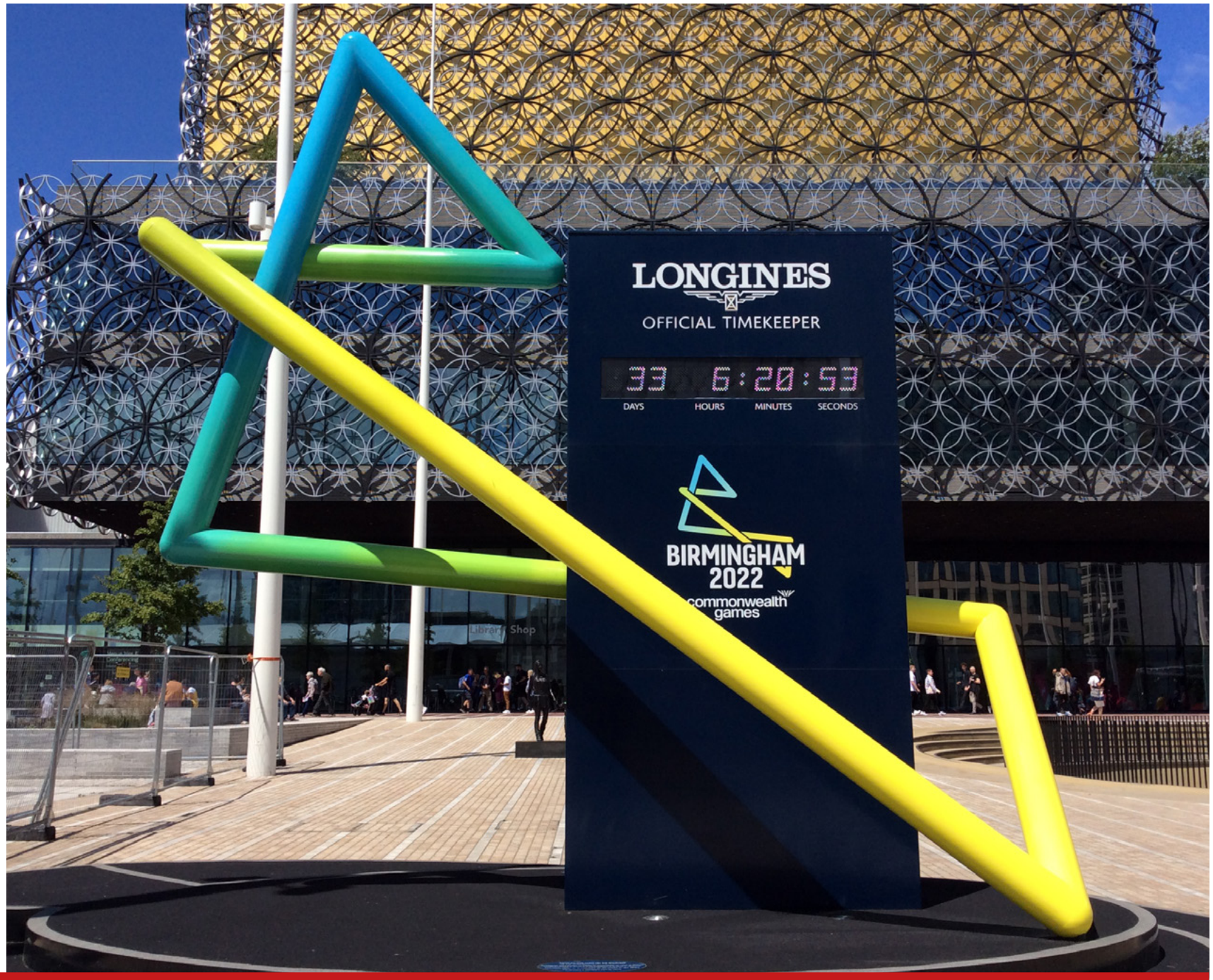
If there is an attack—or downtime or natural disaster—your data snapshots enable you to return to a very current file state. Snapshots can't be changed, deleted, or overwritten, so they secure data against ransomware attacks, human error, and hardware failure. Healthcare organizations that deploy immutable snapshots can maintain the seamless continuation of their operations even in a ransomware attack or other calamity.

For years, companies could rely on a cyber strategy of safety in numbers, figuring that the bad guys would attack someone else. That strategy is now out the window. Healthcare organizations must assume that they will, sooner or later, be the target of a ransomware attack.

The impact of a data breach in healthcare can be catastrophic since all aspects of healthcare are now digital, from diagnosis to long-term care to every event in between. Healthcare generates vast volumes of data at all levels of care and engagement—and that data could not be more critical because human lives depend on it.

Given the quantity and value of healthcare data, implementing a multi-layered protection and recovery strategy is urgent. It is not whether such a strategy should be implemented or even when. It is a matter of, "How fast can we do it?"

Healthcare institutions must quickly implement air gapping and other data protection initiatives to protect themselves. It is indeed a matter of life and death. ■



Let the Games begin

The XXII Commonwealth Games is set to welcome 54 countries and 18 territories to Birmingham. Robert Shepherd asks the experts what Alexander Stadium needs to have in place for the perfect sporting spectacle

Most stadia across the UK were built in the last century – some were even erected in late 1800s. As you can imagine, networks, Wi-Fi, fibre, data and IoT were not considered when the various clubs secured planning permission for a home ground.

That's why, in recent years, stadia have been knocked down and re-built – even moved from residential areas to wasteland to embrace a digital world. After all, the fan experience has changed – it's not just about watching the on-field action anymore. Now it's almost as much about connectivity and the sharing of data.

"Stadiums and other large sporting venues have become notorious for their poor connectivity," says Alan Jones, marketing manager, D-link UK &I. "The stadium environment concentrates a large volume of users, causing existing cellular networks (3G/4G) to slow and leading to woefully inadequate coverage, with expensive data rates for accessing content. This isn't just an annoyance for fans, but also a missed marketing opportunity for free 'word-of-mouth' advertising for sports teams, as fans often like to share their experiences on social media."

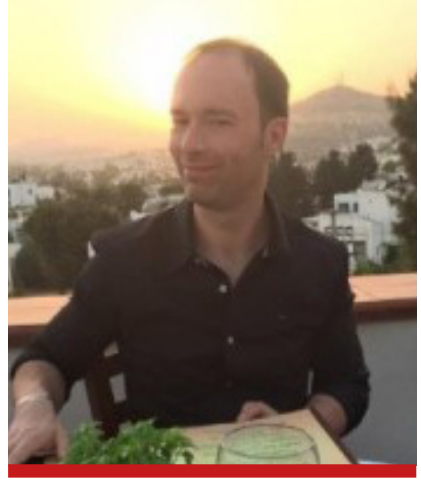
Jones says, "some clubs do try to implement Wi-Fi in their stadiums, but finding a solution that is both fit for purpose and reliable is a step too far for most", with numerous technical and logistical hurdles to overcome.

Scheduled to begin later this year, Extreme Networks and Verizon Business have joined forces to roll out wireless connectivity for Manchester United at Old Trafford.

Additionally, Extreme will outfit

"Stadiums and other large sporting venues have become notorious for their poor connectivity"

Alan Jones, D-link UK &I



"The communications needs are vast and multifaceted with providers, meaning the confinement of sporting locations and the logistics required to get established must be built into every delivery plan."

Jonathan Bridges, Exponential-e.

Liverpool's Anfield stadium with Extreme Wi-Fi 6E access points to deliver the latest generation of wireless connectivity and enable fans to take advantage of digital amenities. The wireless network will be managed by ExtremeCloud IQ, which helps stadium officials monitor and control Wi-Fi capacity and efficiency, configure devices and gain visibility into real-time analytics.

"This implementation will provide fans of these two clubs with fast, reliable Wi-Fi capabilities and increase the clubs' ability to deliver high-performance, low-latency and secure digital services such as mobile ticketing and touchless transactions," says Norman Rice, chief operating officer at Extreme Networks. "Extreme Venue Analytics will also provide Manchester United with actionable insights from the Wi-Fi network, providing information such as app performance and usage, foot traffic flow and effectiveness of concessions, among others. Similarly, with ExtremeAnalytics, Liverpool FC will gain real-time data, including fan foot traffic, popular concessions and points in the match when fans are most digitally engaged."

Birmingham's Alexander Stadium, located within Perry Park and Perry Bar, is the main athletics venue for the multi-sport event.

When the world is watching, you must up your game (pardon the pun) and the event organisers of the Commonwealth Games are acutely aware connectivity needs to be up to scratch.

Still, that doesn't mean it's going to be easy, according to Jonathan Bridges, chief innovation officer, Exponential-e.

"One of the biggest challenges when it comes to delivering and establishing such projects comes down to logistics and confinement of locations," he says. "The communications needs are vast and multifaceted with providers, meaning the confinement of sporting locations and the logistics required to get established must be built into every delivery plan."

Bridges says that another obstacle relates to collaboration with third parties and the complexity of working with and designing the project to support multiple broadcasters. "As with any deployment and service establishment, collaboration with third parties is critical to success, so it's critical to map these out and build contingency plans for delays, especially in getting connectivity to difficult locations," he adds. "Finally, typically these projects have short set up windows due to the locations, especially when they are city-based like the Olympics and the Commonwealth Games. This means the speed at which we need to work is hugely increased and requires larger teams to rapidly deploy, test and establish the service and its security."

As far as Alexander Stadium is concerned, Rice has some advice to impart to the network manager and their team when it comes to moving, securing and storing data.

"Firstly, install a solution that ensures maximum connectivity and performance," he says. "Secondly, it's important to know your fans better so that you can customise elements of the experience for them. Tighter engagement with fans, particularly through an app, i.e. app-based ticketing, instantly adds value and encourages people to engage."

Bridges adds that scalability and resilience are everything. "Existing networks are rarely – if ever – designed to operate at the kind of capacity an event like the Commonwealth Games demands," he continues. "We would therefore strongly advise working with a network provider that can offer high-quality, uncontended connections for each key element of the event. They should also be able to connect to points of presence (PoPs) around the world, to ensure consistent global coverage, with minimal jitter, packet delay, and packet loss, without compromising the quality of on-site connectivity."

Aruba is a company that's worked with many sports and events locations to help provide the latest and best network infrastructure it can. The company was selected by Tottenham Hotspur to help create what is widely viewed as the most technically advanced stadium in the world. Everything apart from the fire systems relies on the Aruba network. It came as no surprise then when the vendor was selected by Brum 2022 as part of a strategic partnership to provide secure

"Firstly, install a solution that ensures maximum connectivity and performance. Secondly, it's important to know your fans better so that you can customise elements of the experience for them"

Norman Rice, Extreme Networks

and flexible connectivity at the games.

"Aruba, using their expertise as part of Hewlett Packard Enterprise, are the ideal company to provide a complex and flexible network connection, enabling a seamless experience for our workforce, volunteers and athletes," says Adrian Corcoran, chief information officer at Birmingham 2022.

Aruba says it will be providing a full network experience to the Games family, deploying a programmable edge-to-cloud solution using Wi-Fi 6, 6E and wired connectivity. "The solution not only provides an exceptional experience, but it will also allow for AI-driven security and management in the cloud via Aruba Central," Simon Wilson, chief technology officer for Aruba UK&I.

"The biggest challenge for us has been the pace of the project and the temporary nature of the games. We only get access to many of the venues very close to the games kick-off, which means everything must be set up, tried and tested in a much shorter timeframe than most IT projects." Wilson says this could not have been without the capabilities of Aruba Central and the skill and dedication of everyone involved. "The Games setup is also temporary with a clear mandate of the Commonwealth Games Federation that there should be a legacy," he continues. "In fulfilment of that, everything we supply for the games will be repurposed into local schools, hospitals, and other public sector projects."

Carl Jarvis, customer services manager at Pro-networks explains how his company has provided League Two football club Tranmere Rovers with day-to-day IT support since September 2004. He explains how the relationship works on an ongoing basis.

"IT upgrades would involve PC, laptop & server supply including setting up the AD infrastructure, security permissions, user administration etc.," he says. "Data is stored securely on the server, backed up locally onsite and backed up to a secure offsite location. From a comms point of view, the club would use its social media channels to share important messages with supporters / customers and we have nothing to do with this."

Of course, the most important thing is crowd safety. Thankfully, technology has moved on a lot since, for example, the Bradford City stadium fire of 1985 and the Hillsborough disaster in 1989. Alexander Stadium first opened in 1976 and then the facility became the home of UK Athletics in 2011, following a refurbishment that saw the creation of the 5,0000-seater East Stand on the backstraight.

For Birmingham 2022, it will be modernised with a post-Games permanent capacity of 20,000 – up from the current 12,700.

Jarvis explains how Pro-networks keeps the crowd moving. "Finally, we helped Wi-Fi connect the stadium, including turnstiles which was vital for them when the ticketing system changed from a "buy the tickets at the club shop and present to a steward to gain entry" to a "print you own tickets at home" solution, which are scanned, giving the club data on turnstile use/attendance etc.".

Sam Durrant, head of security at Plextek says many factors come into play when managing a crowd.

"Critical communications and the use of IoT have come to be key players in a wide range of safety-critical activities and will be of vital importance for the upcoming Commonwealth Games held in Birmingham," he adds. "One way of ensuring crowd safety is through the use of sensors for people counting – an approach recently used by Plextek involved the use of a combination of ultrasonic and infrared proximity sensors. These can be fixed to the entrance of the venue and used to count how many people are entering at any point and feed this data back to the event security to ensure they do not exceed capacity."

Hugo Read, head of engineering at Landways, says the emergency systems deployed by his firm comprise the surveillance camera network, the voice alarm system and the emergency phones, are all enabled by the power and data network. All these connected systems run on the DC power network that includes a three-hour centralised battery back-up that covers all the systems.

"The use of highly visible emergency phones that are simply 'lift to connect' allows people in need to instantly connect to the control room without any need to dial or carry out any action," Read says. "The voice alarm system is naturally highly resilient and extremely customisable, allowing emergency announcements and alarms to override the PA audio and to be 'addressed' to either individual speakers, different grouped zones or to the whole stadium."

Read adds that due to the improved reliability of the overall network, including the phone system, plus the very fast and easy way people can connect back to the control room, allows for easier overall communication with the emergency services.

Of course, there's more to safety than just getting people through the turnstiles. Should an individual want to smuggle in a dangerous item, it's a lot more difficult to do it than it once was.

"Concealed object detection is another element to consider when working on a large-scale event," Durrant continues. "The use of microwave imaging, capable of real-time detection of hidden objects, provides a non-intrusive approach. Microwaves, due to their low frequency, are intrinsically safe to use on people and can discriminate against a range of threats, including explosive devices and weapons. Such technology can be capable of screening people at close range in a short time which is ideal for sporting events such as the Commonwealth Games. "We are lucky that we now live in a society where we have multiple technologies at our disposable and that we can use these technologies to ensure the safety of others."

Running the network is no mean feat at such a huge event and Hugo Read, head of engineering at Landways said, that whilst his company focuses on the infrastructure, rather than the data and application layer, there are inherent benefits of taking fibre to the device.

"Fibre is more secure, not restricted by bandwidth, not subject to electrical and environmental degradation and is not confined by distance," he adds. "This means that the traditional intermediary comms rooms that are often vulnerable, can be removed."

Furthermore, Read says that with the 'cloudifcation' of data and services, "dual fibre backhaul is a must, but of equal importance is the IP Transit arrangement which needs to be flexible to allow bursts of traffic at peak periods and fast upgrade paths, such as WDM equipment ready to be deployed at a moment's notice."

With so much data flowing around the networks, security is an obvious consideration – and that goes for employees as well as the thousands at the stadium.

Read says that using full fibre deployment directly from the core unit to all end points, data capacity and network reliability were both significantly increased, enabling all servers to be stored either in the core unit or in cloud storage, with very low latency download and upload times of data including very large analytics and video files. "This greatly improved the operations of the site, allowing users to access data wirelessly at high speed from all areas included in the coverage," Read adds. "Allowing the data servers to be stored in the highly secure core unit also improved the data security. Full fibre connectivity in low-profile inconspicuous containment out of reach of the public without unnecessary breakout points and cabinets also increased security and reduced the risk of tampering and hacking. A variety of VLAN networks with their own security protocols for office use, conference, fans, EPoS, ticket scanning and media use also provided data separation and security for the different networks."

Bridges Security is also a major concern as these large-scale events are a primary target for cyber attackers, particularly DDoS attacks, so it's critical to ensure we have effective cyber controls deployed on top of the service."

For Wilson, any network, controlling access and protecting peoples' data is paramount. "We achieve this through a zero-trust security model based around Aruba ClearPass," he says. "By doing this we ensure no user or device has access until we know who or what they are and then only grant access to that which is appropriate for their role. We also use AI to help identify clients and essentially this is to ensure they are who they say they are."

Wilson adds that when events occur across locations, the only way to operate at this scale is with cloud-based services delivered right to the edge. "By managing the network in the cloud, teams no longer have the heft task of shipping as much equipment between events or storing equipment when the games aren't taking place," he concludes. "The NaaS model enables the team to make it as simple as needed."

Games on.

"One way of ensuring crowd safety is through the use of sensors for people counting – an approach recently used by Plextek involved the use of a combination of ultrasonic and infrared proximity sensors"

Sam Durrant, Plextek

"The Games setup is also temporary with a clear mandate of the Commonwealth Games Federation that there should be a legacy"

Simon Wilson, Aruba UK&I

Five-star treatment

One of the world's most famous hotels and an independent luxury hotel get the perfect upgrade

Puttin' On the Ritz

The five-star Ritz London hotel is situated in the heart of Piccadilly overlooking Green Park. Over the last 115 years it has earned a reputation as one of the finest hotels in the UK and become a benchmark by which other hotels are measured. The Ritz boasts 136 Louis XVI-style rooms and suites, a world-famous Afternoon Tea and the Michelin-starred Ritz Restaurant.

The Ritz is a luxury hotel that welcomes a discerning clientele who expect world-class service. The hotel's IT network is no different. The Ritz London's in-house IT team consists of six people and there are three members of the IT staff who monitor the IT network constantly. They need to maintain visibility of the health of the hotel's core network, IT systems, building and cameras 24-hours a day. The IT team found that other solutions they had tried weren't fulfilling their needs. As Richard Isted, IT manager, The Ritz London explained: "We were not getting useful reporting from our previous monitoring systems because they were either hard to configure, difficult to maintain or lacked the feature sets to configure the more complex or unusual systems for monitoring."

As a result, Isted and his team turned to Paessler's PRTG Network Monitor, initially taking out a free trial. They mainly use PRTG to monitor the health of the hotel's core network and IT systems in order to get more visibility and control.

Some of the main motivations for Isted and his team in choosing PRTG was that it is feature rich and easy to set up: "There are numerous extensive blog articles on the Paessler website that help you to configure common devices for monitoring. We haven't had to log a single support case because everything is so self-explanatory. As we operate on a "Windows Server" based system, it is easy for my team members to help manage, as opposed to Linux-based monitoring systems which have a much steeper learning curve." Setting up sensors and connecting them to PRTG was also very straightforward. Isted added: "PRTG made configuring custom SNMP sensors much easier than other systems I've worked with."

The business benefits

Hotel security and maintenance is a key priority for the IT team. After they first started using PRTG, the IT team discovered some useful insights into how well the systems and buildings were functioning. Isted explained: "We found out that our air conditioning fails more often than I had anticipated. Before we installed PRTG one of our servers was damaged due to overheating. Now temperature alerts are instantly escalated to a 24-hour on-site team who take corrective action."

The PRTG alerts are invaluable for the in-house maintenance team who operate around the clock. "There's a separate escalation group for them. We're a 24-hour operation, but the IT team is not necessarily always on site, that's why we have plugged PRTG into our email system and linked escalation alerts to the telegram messenger service as well. The alerts tell the maintenance team the exact location of the problem. It's a good way to make sure that we don't have any issues to sort out in the middle of the night when we're not actually on site to monitor things ourselves, and this has proved useful on several occasions."

The use of PRTG has also led to a much more proactive approach by helping the IT team spot issues and needs much sooner, which has been a major benefit so far. Isted said: "PRTG's alerts are extremely useful and give us a heads up on potential issues before they escalate" This has allowed us to be more proactive, as opposed to being reactive. We have also used them to look at traffic patterns when our network is busy, allowing us to adjust our backup jobs to work around any peaks. Overall, PRTG has helped us improve service up time by highlighting important alerts that would result in a system failure or downtime if action was not taken."

Isted and his team have strong ambitions when it comes to upgrading the hotel's tools and technology to create a cutting-edge IT network and system. "Thanks to PRTG we have been able to analyse our need for further IT equipment. The data that we have collected gives us figures on resource utilisation which in turn helps back the business case for further investment in IT infrastructure. In the future, we're planning on investing in more IP cameras and physical security, access control devices as well as switches and servers. We'd also like to integrate our system with physical security devices such as door locks and electronic door controllers using the PRTG maps feature and to have better integration with our cameras so we can track their health and utilisation. This would enable us to create a personalised dashboard for our security team so that they can have greater insights into our security equipment and respond quickly when there's an issue. So far, we've probably covered 33% of what PRTG can do as it's such an extensive system. We have lots of ideas that we haven't had a chance to implement yet." ■

"I would recommend PRTG because it has helped us significantly improve service up time by highlighting important alerts that would otherwise result in a system failure or service disruption if action was not taken. Thanks to PRTG we can ensure that The Ritz London's network and IT systems are five-star, just like the hotel"

Richard Isted, IT manager, The Ritz London

Beyond Wi-Fi

Barnsdale Hall Hotel is an independent luxury hotel with a range of accommodation including lodges and apartments. Popular among corporate and leisure clients, the hotel facilities include a spa and leisure club facilities, restaurant and bar, business conference services and wedding packages.

Wi-Fi is provided to guests wherever they may be within the buildings, grounds, accommodation, spa facilities and conference suites.

The hotel management recognises that good quality Wi-Fi is key to guest experience.

When Ian Stone took up his role as estate manager at Barnsdale Hall Hotel, the Wi-Fi infrastructure – provided by Novahub – was already in place.

However following installation of the system, it had not been substantially upgraded.

Seeing no reason to replace the existing infrastructure or find alternative supplier, Stone contacted Novahub in order to understand and familiarise with the configuration and layout of the Wi-Fi network and to plan a roadmap to evolve the Wi-Fi provision around the hotel.

"I don't give recommendations lightly, but if anyone in this industry were to ask me for a recommended WiFi service provider, I would tell them to go and talk to Novahub without hesitation"

Ian Stone, estate manager at Barnsdale Hall Hotel

Stone knew from his previous experience – part of which was with a large international hotels group – that business and leisure hotel guests expect good quality Wi-Fi.

Wi-Fi not only influences or impacts on the experience of guests while at the hotel; it can also be a driver of return bookings.

At the Barnsdale, Wi-Fi is provided not just to guest accommodation, but in areas such as the leisure centre reception, bar and snooker room and for business guests, throughout the conference facilities.

In order to continue providing free, high-quality Wi-Fi to all guests, Stone saw the need to survey, assess and upgrade the Wi-Fi infrastructure in key areas of the hotel.

Of particular interest, Novahub added value by offering insights beyond the Wi-Fi technology to the business value of Wi-Fi and how and where it could be deployed around the hotel site and grounds.

When asked for support, the Novahub team proved highly responsive, for example being willing to help out at short notice following a power outage in part of the hotel.

Novahub can also offer anonymised insights and reporting into Wi-Fi location and traffic usage around the hotel. ■

The IoT data deluge in industry and manufacturing

Effective data storage management is a critical component of the IoT ecosystem

By David Keegan, group CEO, DataQube Global

Internet of Things (IoT), from a top-level standpoint, refers to a network of physical devices such as embedded sensors, driverless vehicles, smartphones/tablets, wearables, or home appliances, that create and share information without human intervention. Even though there is currently a strong drive towards IoT and digitisation, the concept has been around for the last 10 years at least, with interconnected devices and applications prevalent in industry and consumables.

What has recently changed is the augmented capabilities of said devices, faster comms networks, the standardisation of communication protocols and more affordable IT, which is giving the IoT phenomena a turbocharge. As such, it is transforming operational processes and product lifecycles across a range of markets and applications. That said, the detailed level of information current IoT devices are capable of capturing should be empowering manufacturers to leverage the benefits of Industry 4.0 to operate truly automated production lines/assembly lines, but this isn't happening as quickly as you might expect. Whilst some of the barriers may be cultural or finance-related, a much bigger barrier, in many instances, is highly intelligent devices versus substandard data handling and storage management infrastructure.

An unavoidable consequence of IoT and the devices and applications it powers, is the colossal amount of constantly changing data that is generated as a result. This data needs to be processed in real-time if meaningful conclusions are to be drawn and swift decisions made to avoid bottlenecks and keep production lines operational, as smallest of delays can have major repercussions further down the line. This is particularly important for manufacturers reliant on artificial intelligence (AI) and machine learning (ML). Both disciplines are data intensive, bandwidth hungry and require robust storage management processes that enable parallel processing at scale. Indeed, the value of any IoT derived data is incredibly short lived, and unless the associated storage management infrastructure can keep pace with the constantly changing data, an IoT investment can very quickly become an expensive white elephant.

So, what happens to all the IoT data?

1. Data sources

IoT gathers data from an array of devices and/or embedded sensors and the information can either be processed locally, depending on the availability of appropriate infrastructure, the sensitivity of the data, or the nature of industry, or transported via an edge gateway to a colocation facility or the cloud for processing and handling.

2. Data storage

The data captured by the embedded technologies then needs to be appropriately stored for long-term and short-term applications. Some of the data might require immediate processing depending on the application (the operability of an industrial robot for example), whereas some might need to be securely transported and/or stored for future applications.

Data storage is a small cog in a big IoT wheel

Storage is just one element of the IoT data processing ecosystem. BUT it is an element that is becoming increasingly integral as insufficient storage capacity is detrimental to operability. The storage capabilities of any IoT network must assure data integrity, reliability, and safety. Moreover, they must be agile to support a range of environments, technologies, and applications, whilst facilitating seamless interconnectivity between edge gateways, other edge devices and the cloud. Substandard storage is the Achilles heel for many manufacturers, with outdated comms rooms not allowing them to harness IoT data to its full potential. Insufficient storage capacity is such an issue that, according to industry research, between 60% and 73% of machine generated data goes unanalysed.

The IoT data that powers Industry 4.0 needs to be processed as close to the source as possible for operability and safety reasons and organisations reliant on mission critical data are quickly realising that conventional colocation facilities cannot always assure the ultrahigh speed and litra low latency needed. In paradox, many on-premises facilities are not fit for purposes as far as IoT data storage management is concerned because they are unable to house the specialist IT needed. And even if they are, there is seldom room for expansion as capacity requirements escalate. High performance computers (HPC), because of their sheer magnitude, GPU-based processing power, associated cooling technology, and high energy consumption, need specialist facilities that are fireproof, weatherproof, comprise seamless connectivity to the cloud and support dynamic power consumption.

Commissioning a bespoke facility robust enough to meet the demands of IoT data is a non-starter for many manufacturers because of the high costs involved – anything between £7-£12m per MW and lead times in excess of 18 months. What is needed is a viable means of providing centralised data centre capabilities locally without the associated expense of building a bespoke facility that assures HPC processing. This has not been possible, thus far, however, due to financial constraints, complex project management requirements and excessive deployment times. However, the IoT data handling quandary in manufacturing is about to be transformed thanks to a disruptive approach to edge date centre infrastructures.

Recognising the need for data handling at source, the company has developed a portfolio of podular data centres for internal and external usage that assure high-speed, high-performance, low latency processing needed for IoT data. Installs are possible from less than 10 watts to +100 MW and individual pods can operate independently as a mini data centre or merged in stacks, depending on the size of a manufacturing facility or the storage capacity needed.

Without a cost effective and viable means of delivering HPC at the edge, IoT data will remain untapped regardless of the accuracy or sophistication of the associated embedded sensors. Edge data centre infrastructures must adapt to meet this changing data processing landscape. ■

Why consolidating security tools is key to improving ROI and decreasing cyber risk

By Martin Riley, director of managed security services at Bridewell Consulting

With high-profile cyber attacks on the rise, enterprises are under pressure to strengthen security. As organisations transform and their attack surface grows, many make the mistake of investing in more and more security tools. However, not only is this costly, often there is usually little consideration for the integration between technologies and gaps in the coverage this creates. And if not managed correctly, this can actually increase risks and hinder the security teams' progress in the long-term.

There's no silver bullet when it comes to cyber security. Many enterprises are prepared to spend big to acquire security technologies, but often neglect investing in the ongoing development of people required to maintain, operate, and continually improve these technologies. Not only does this cause security teams to be stretched too thinly across disparate and poorly developed solutions, but it makes it difficult to keep up with changes in technology and new features.

It also increases the complexity of monitoring, managing, operating and optimising a technology stack, making it harder to secure crucial business data. The average time to detect and contain a malicious attack still remains at 315 days - often a result of disjointed security architecture and noise levels from traditional security monitoring, meaning IT teams cannot respond effectively.

Having too many disconnected security tools also impacts data and processes. Each tool produces large amounts of data, and if all are acting in silo, can cause challenges over visibility, integration and control of data. According to new research from Panaseer, the shift to cloud and remote working has driven a 19% increase in the number of security tools organisations must manage.

Also, the more integrations and endpoints an organisation has, the greater number of things to secure, making it easy for security holes to creep in. Enterprises do not want new technology to be the entry point for a data breach so correct controls need to be put in place to secure the data while it flows across the network and to also protect it where it resides.

With complexity and management of multiple tools high, many enterprises recognise the need to consolidate. However, to effectively bring security tools together, there are some key considerations.

First, time needs to be set aside to ensure technologies are consolidated safely, and that capabilities and content created in existing tools are retained and ported across where appropriate. Security Information and Event Management (SIEM) technologies are a prime case where organisations do not want to lose existing custom use cases and analytics.

Second, the right technology needs the right people to use it effectively. It takes time to transfer skills from one technology set to another and additional training may be required to explore and develop new skills.

Finally, legacy methods of working need to be left behind. Consolidation presents an opportunity to identify where technology can relieve operational challenges by using automation to drive efficiency and streamline security operations. For example, old-fashioned technology stacks often produce multiple alerts, which in-house teams have to review and apply their own intelligence to before arriving at a response. With the right technology stack, like Extended Detection and Response (XDR), enterprises can automate detection and increase the ROI of security operations while also strengthening cyber resilience.

MDR combines human analysis, artificial intelligence and automation to rapidly detect, analyse, investigate and actively respond to threats. It can be deployed rapidly and cost-effectively as a fully outsourced service or via a hybrid security operations centre (SOC) and helps to develop a reference security architecture that enables organisations to safeguard on-premise systems, cloud-based applications and SaaS solutions. It also enables companies to quickly respond to new threats, reducing cyber risk and the dwell time of breaches.

If organisations are smart in their choice of solution - for example, choosing a Microsoft-based solution - enterprises can leverage existing investments in Microsoft 365 licensing to consolidate vendors and technologies, such as SIEM, endpoint protection, cloud security and identity-based solutions. Each solution on its own incurs significant costs and can lead to over £100k a year in costs savings.

The most effective MDR services are those that utilise Extended Detection and Response (XDR) technology to enable detection and response capabilities across network, web and email, cloud, endpoint and most crucially, identity. This ensures that wherever the cyber-attack comes from, users, assets and data remain safeguarded.

To be effective in today's modern environment, security teams need a solid grasp of all technologies used, whether hybrid, on-premise or cloud-native, and understand how to implement effective security controls across all environments. The problem is many enterprises lack security professionals with the depth of security knowledge and technical capability to develop more advanced capabilities required for effective MDR or running a cloud-native modern SOC.

By working with a security partner to implement MDR and consolidate security vendors and tools, enterprises can reduce complexity and simplify operating processes, leaving security teams free to expedite their knowledge and skills growth and maximise cyber security ROI. ■

Fibre termination in different environments

By Nicolas Roussel, technical manager, Siemon

Fibre optic cabling is emerging as the dominant media type for data centre infrastructure but also in the LAN market fibre is on the rise. The increasing bandwidth needs of buildings that result from new developments including Wi-Fi 6, the Internet of Things (IoT) or intelligent building devices, demand fibre in the backbone. In harsher, industrial environments fibre cabling also has its place, especially in locations that require extended distances, in spaces with close proximity to heavy sources of EMI, or where fibre active equipment is used.

When it comes to deploying fibre links, there are several different termination methods available, ranging from pre-terminated and fusion splice options, to field-terminated connectors. Whilst it's important to consider the immediate applications and equipment interface requirements, future scalability plans, available budget, insertion loss performance and the level of expertise of those doing the installation, the environment in which fibre installations take place will play an important role in determining which termination method applies best.

Pre-terminated solutions

Whilst pre-terminated solutions are largely deployed in the data centre, they can turn an installation in an office environment around quickly when pathways allow it. These plug-and-play solutions don't require specific tools especially when MPO connectors to support higher bandwidth needs are installed but the installation must be carried out carefully and good testing methods must be applied. Pre-terminated solutions are available in multimode and singlemode fibre types and multi-fibre MTP, LC, SC, ST connector interfaces.

Splice-on pigtails

These solutions are ideal for transitioning from 250µm OSP to 900µm indoor cable and are therefore frequently used in entrance facilities for incoming fibre, for example in cloud and colocation data centres where there is fibre coming in from various service providers. In the LAN environment splice-on pigtails are also widely used in the vertical cabling backbone where they terminate in the telecommunications room or at the floor distributor. In these installation environments, splice-on pigtails are the more durable option since they are able to withstand the cable pulling process.

Splice-on pigtails offer a strong, repeatable low-loss connection, typically around 0.1dB, cost less than pre-terminated solutions (excluding labour) and offer the benefit of not needing to plan exact lengths or deal with longer lead times.

However, the splicing process – where a short fibre stub that protrudes from a pre-polished connector is fusion spliced to the incoming fibre using an electric arc - can be expensive for anyone who doesn't own a splice machine and there is also the added cost and space required for the splice trays and sleeves to house and protect the splices and a decent workspace is needed to accommodate the process.

Splice-on pigtails are generally available in multimode and singlemode options and various connector types, including duplex and simplex LC, SC and ST, and multifibre MTP.

Splice-On connectors

Splice-on connectors are used in LAN environments in a similar way as splice-on pigtails, but they add a good practice in the horizontal distribution as there is no need for splice trays and protective splice sleeves since the splice is protected within the connector housing itself. This reduces material requirements, conserves space within fibre enclosures and can save up to 30% on installation time compared to pigtails.

Like splice-on pigtails, splice-on connectors offer a strong, low-loss connection without the need to predetermine lengths and they require a fusion splicing machine and a quality cleave. Splice-on connectors can terminate 900µm and 250µm fibre. Pre-polished fusion splice-on connectors like Siemon's OptiFuse are available in multimode and singlemode and with LC or SC simplex PC or APC connectors.

Mechanical splice connectors

Mechanical splicing is an easy and friendly installation method for fibre-to-the-desk or any installation where space is a concern, or where a decent workspace is not available. These field-terminated connectors are perfect for lower fibre counts, repairs and reconfigurations, especially for situations where installers do not have the luxury of planning lead times or do not own an expensive fusion splicer as required for splice-on pigtails or splice-on connectors.

Mechanical splice connectors are a frequent choice in industrial environments too. Because the splice is protected within the connector housing itself, the risk of contamination by dust moisture, and harmful substances which are commonplace in these harsher environments is lower.

Pre-polished mechanical splice connectors like Siemon's Lightbow are available in multimode and singlemode and with LC or SC simplex PC or APC connectors. ■

PRODUCTS

Connectix Cat6A SFTP RJ45 patch leads are designed to complete the Cat6A Channel, providing support for extremely high-speed applications including 10GBASE-T, the company says. These patch leads are made from shielded Cat6A cable and are terminated using high performance modular plugs. The fully shielded cable increases signal isolation and helps to prevent contaminant noise from entering the lead. These SFTP patch leads are complementary to the Connectix Cat6A Cabling System and will provide support for future bandwidth-hungry applications. Features include the fact they are independently tested to Cat6A and 10GBASE-T channel performance standards and they conform to ANSI/TIA 568-C Category 6A. Leads are available from stock in lengths from one to 10 metres in a number of different colours. *connectixcablingsystems.com*

Excel Networking Solutions offers one of the market's most comprehensive ranges of copper cabling solutions, supplied in 100% plastic free packaging. Inclusive of Category 5e, 6, 6A, 7A and 8 copper cable classes, Excel's structured cabling products constitute an end-to-end solution where performance and ease of installation are prerequisites.

Having evolved to face industry challenges, Excel offers high density designs as a space saving solution, such as the 0.5U patch panel and reduced diameter cabling. When a system is installed by an Excel Cabling Partner, a 25 year warranty can be awarded, covering product and applications assurance of compliance with industry performance standards appropriate to the class of copper cabling being installed.

Excel also offer a pre-terminated copper solution as part of their Specialist Support Services, which are carried out by our specialised, knowledgeable technical staff and go through a rigorous quality check before delivery.

The full portfolio of Excel's copper cabling products is also available in the dedicated Excel Copper Catalogue. *excel-networking.com*

HellermannTyton says it has "a connectivity solution for every phase of your network infrastructure, from cable entry in to the building, distribution across the building to the data outlet at the desk". The company says its S5 MDU enclosure will distribute any incoming fibre to the comms room or to multiple zones in the building. From the comms room, HellermannTyton have a number of copper and fibre solutions that can then be used to connect offices, active equipment and hardware to the outside world. HellermannTyton manufactures a wide range of solutions designed to provide connectivity to different zones within a building. The new Zone Cabling brochure highlights the new HTC range of products in both Cat6A and Cat6. The Category 6A solution includes the new Category 6A Jack, panels, cable and patch leads. The new Jack is designed to be 'tool-less' and does not require any specialist termination tools. For Cat6 there is a new range of panels, outlets along with a selection of 6C and Euro modules, faceplates and back boxes. Additionally, there is a 6C and Euro module designed for Fibre to the Work Area applications. *htdata.co.uk*

"Carefully checking each cable takes too much time and carelessly unplugging the wrong cable can take webshops, apps or transactional sites offline," says **Brady Corporation**. It offers labels that are designed to reliably identify any data centre cable, server, component and rack to take the guesswork out of troubleshooting.

Brady's labels with adhesives for curved and flat surfaces stay attached to every cable and component. As a result, identification will be in place when fast troubleshooting is necessary to avoid downtime." Label sizes and shapes are available to easily identify any rack, server, component, STP, UTP and COAX cables and Brady also offers a flag shaped label designed for minimum fibre optic cable contact with maximum available space for identification data," the company says.

The Brady Workstation app platform offers an array of label design capabilities that cover almost every data centre identification need. Cable, component and rack labels, and even facility signs and identification can be designed in a few steps. Designs can easily be sent to a Brady label printer for on-site printing so the new label can be applied immediately. *bradyid.com*

Please meet...

Chris Dyke, Allied Telesis UKI

Who was your hero when you were growing up?

As a as a child, it was always my dad. He was an extremely hands-on parent, and we were always doing stuff together: him, me and my two sisters. Whether it was taking us to the seaside to go swimming or diving; or camping or fishing he was always teaching us new things and helping us to be as self-sufficient as possible. I always admired that in him, and it seemed that most of my friends didn't have that kind of relationship with either of their parents, as most of my mates were drawn to our house to hang out. Being hands-on is something that I've always tried to ensure that I replicate where possible with our kids because I admired it so in my dad, but that said, he was a terrible cook, so I've improved on him there as I learned to cook from my mum.

What was your big career break?

That was escaping from Somerset on a train to Bracknell. When I finished university, I applied for over 100 jobs in Somerset but never even got an interview. Then I went to Bracknell and had an interview with an agency on a Monday lunchtime and started work for a catalogue IT reseller the following day. So, I escaped on the Monday and started work on the Tuesday on 50% more money than I would have got from the jobs I was applying for in Somerset! That was really the big career change as it allowed me to get into IT.

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

Respect your elders. To be honest, I know this is probably a bit boring, but from school I was always encouraged to have meaningful conversations with adults, even as a kid, and to show them respect (but not in the way that kids consider to be respect these days) and it's always served me very well.

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

I'm sure you hear this all the time, but I would choose to work with animals in a rescue centre or a wildlife park. Not sure I'd be much good at healing them if they were hurt because I'm not awfully good at blood, but animals just bring so much joy and they don't ask for anything in return.

What would you do with £1m?

If I had a million pounds, I would buy somewhere in the Alps, so that I could enjoy skiing with my kids. The mountains have always been my happy place, having been a skier since my early youth and I'd really like to enjoy the snow with my kids before it disappears for good. It would need to be the Alps because then we could hop there, which is what I'd like to do as often as possible.

Where would you live if money was no object?

Bit off-the-wall, this one, but I would love to live in Chile, which is probably not an answer that you've had before. Chile has some lovely beaches for my wife, and you can get to the mountains in less than an hour and a half for skiing in the Andes, which is fantastic. This means we could both have the holiday that we always wanted without having to argue too much, and we could still meet up for dinner in the evenings. I've got a basic smattering of Spanish, so that would also help.

The Beatles or the Rolling Stones?

Beatles, for sure. The Rolling Stones were a little bit too rock-n-roll for my family, so as a youngster I'd listen to The Beatles because they were much more family friendly. Also, for the last 15 years or so, I've been told loads of times that I look like a fat Paul McCartney! And I'm still not sure whether that's something to be proud of or not - you can make your own mind up as to if you agree or not.

Which law would you most like to change?

I don't really have a law that I'd like to see changed. What I would like to see is some attempt for the law to keep up with changes in technology because we seem to have loads of laws governing our lives that really aren't fit for purpose in the age of computing, advanced connectivity, AI and other technology. It seems that most of the people involved in making laws and assigning punishments are far too out of touch with tech. So, a wholesale review of law for the modern age would be great to bring it into the 21st century.

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

It would be David Attenborough, who you probably hear as an answer all the time. He's just had such an amazing life and career and he's changed the way that so many people think around the world about nature and the planet. I'd just be happy to sit there and listen to him while I eat loads of food. That would be perfect for me. ■