APRIL 2022
networkingplus.co.uk

NETWORKING+

Beware of Russian ransomware

Russian ransomware is on the rise

Holly Andrews, KIS Finance
p6

Got backup, but is it enough?

Key tips on retrieving data

Ian Richardson, CSI
p7

Questions and answers

An old rocker shares his life

Steve Barber, Sepura
p16

Government urges businesses to boost cyber standards

Businesses and charities are being urged to strengthen their cyber security practices now as new government figures show the frequency of cyberattacks is increasing.

According to the *Cyber Security Breaches Survey 2022* report, published by the Department for Digital, Culture, Media and Sport (DCMS), almost one in three businesses (31%) and a quarter (26%) of charities suffering attacks said they now experience breaches or attacks at least once a week.

The number of businesses which experienced an attack or breach remained the same as 2021 levels. Almost a third of charities (30%) and two in five businesses (39%) reported cyber security breaches or attacks in the last 12 months.

Small businesses have been urged to adopt the Cyber Essentials scheme to protect against the most common cyber threats such as phishing attacks and use the Small Business Guide to improve cyber security practices. Larger organisations should use the Board Toolkit to get company executives to act on cyber resilience, the government added.

Cyber minister Julia Lopez said it is vital that every organisation takes cyber security seriously as more business is done online and in a time of increasing cyber risk.

"No matter how big or small your organisation is, you need to take steps to improve digital resilience now and follow the free government advice to help keep us all safe online," Lopez added.

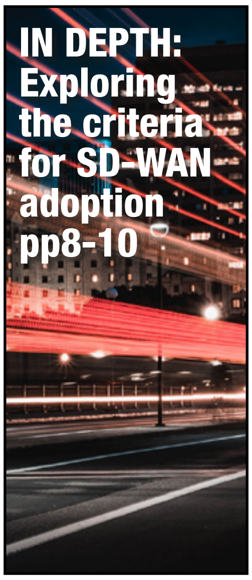
Following a wave of high-profile attacks over the past year including on Kaseya, Colonial Pipeline and Microsoft Exchange, there has been increased attention on the cyber security of supply chains and digital services.

Nigel Thorpe technical director at SecureAge, told Networking+ the statistics suggest that organisations are improving their defences against cyberattacks, yet "a sizable proportion" suffered the effects of some form of breach. "The advice given by the NCSC should certainly be taken, but organisations must recognise that individual people are not immune to making mistakes or poor decisions," he added. "And in our highly connected world, it might not even be your own employee who releases the ransomware."

The government said it is committed to protecting the UK from cyber threats, which is at the centre of its £2.6bn National Cyber Strategy. It is investing in cyber skills, expanding the country's offensive and defensive cyber capabilities and prioritising cyber security in the workplace, boardrooms and digital supply chains.

John Fitzpatrick, chief technology officer at cyber security firm Jumpsec added that it's important for organisations to be aware that the vast majority of attempted attacks "are typically not targeted" and most organisations will see these every day, because "they are relentless". He said: "Basic cyber hygiene steps like patching, anti-malware solutions and user awareness are still some of the best defences. Targeted attacks are far less frequent. Having a view of the attack paths within your business, including understanding who and why you might be targeted are important in planning your defences."

Martin Walsham, director of cyber security, AMR CyberSecurity said, "this is a useful report" and should act as a wake-up call for any business leaders in doubt about the level of business risk their organisation is exposed to through cyber threats. "I urge organisations to check they have robust cyber incident response plans in place, and that they are tested to ensure they are effective should they need to invoke them," he added. ■



IN DEPTH: Exploring the criteria for SD-WAN adoption pp8-10

LSE data centre migration helped by EXA

The London Stock Exchange Group's (LSEG) data centre migration is moving forward, with connectivity provider EXA hooking up the new facility with low-latency connectivity.

EXA will deliver on-network dark fibre, wavelength and ethernet services to LSEG for use by all the co-located users of the data centre.

The firm says its terrestrial and subsea network across Europe and North Atlantic is suited to trading venue connectivity, with all major European and North American exchanges being on-network and diversely routed.

It added that connectivity can also be extended beyond the facility and to other sites.

"There can be few cases in which the quality and speed of a network is more important than when connecting to the London Stock Exchange, so the decision to entrust EXA Infrastructure as connectivity provider to the new data centre is the highest possible endorsement of our capabilities," said Andrew Haynes, executive vice president of product and technology at EXA Infrastructure.

LSEG's data centre has been moved from the City of London to a newly built facility in the Docklands area, accommodating LSE, Turquoise and Turquoise Europe trading and market data platforms.

EXA is one of a handful of network providers with the Accredited Connectivity Partner status that is required to support connectivity to service subscribers on site. ■

First phase of 4G rollout on London Underground complete

BAI Communications has launched a permanent 4G mobile service on the eastern section of the Jubilee Line, which is a significant milestone in the rollout of mobile coverage across the London Underground.

Three and EE customers will be the first to benefit from the 4G and 5G-ready communications between Westminster and Canning Town, while the pilot services with O2 and Vodafone will continue while discussions with BAI on access agreements are finalised for a permanent service.

It follows a successful pilot scheme on the Jubilee Line since March 2020.

Last year BAI Communications was awarded a 20-year concession by Transport for London (TfL) to provide mobile connectivity on the Underground.

BAI Communications chief executive officer Billy D'Arcy said the service will "provide a massive boost to the passenger experience."

He added: "We're pleased to announce this first major delivery milestone on our journey to transforming London's connectivity. Customers of our launch partners, Three and EE, will be able to enjoy permanent access to uninterrupted mobile connectivity whilst travelling on the eastern Jubilee Line."

BAI is deploying an active distributed antenna system (DAS) from SOLiD Technologies, which is custom built for the challenging environment of the London Underground. This is an approach that has been proven in some of BAI's previous transport system deployments, such as New York City.

Coverage in tunnels is provided via a system of high-power radio units connected to circa 770kms of "leaky feeder" cable that are being laid throughout the London Underground tunnels.

In station ticket halls and platforms, a large number of low power radio units provide coverage.

The system connects back via new fibre connections to a series of data centres across London, which act as base station hotels and provide the interconnection points for each of the mobile network operators.

A permanent 4G mobile service is also expected on the Elizabeth Line and at Oxford Circus, Tottenham Court Road, Bank, Euston and Camden Town by the end of the year. ■

Nasstar to run new secure network for MoD

Managed services and self-styled "transformative" technology provider Nasstar has begun work on a new contract awarded to a facilities management services provider to run a new secure network required by the Ministry of Defence (MoD).

Last summer, Vinci Facilities was appointed by the Defence Infrastructure Organisation (DIO) to provide hard facilities management services. The South East Future Defence Infrastructure Services (FDIS) contract provides hard facilities management services for more than 6,200 buildings and infrastructure assets at 59 MoD sites in London and the home counties.

The initial seven-year term – there are three additional performance-related option years – is worth £1.1bn, comprising £423m for the core FM contract and a potential £732m for additional works. The FDIS contract represents a shift in the DIO's service delivery approach to better manage military built estate across the UK.

"We see this as the beginning of a strategic partnership between Vinci and Nasstar which will transform the performance and flexibility of our networks across various client sites," said Ben Paddick business solutions director at Vinci Facilities. "Clearly, for the MoD, security is a critical concern and Nasstar working with Fortinet [as an expert partner] has developed a solution that will enable us to run a more flexible and resilient network that enables us to take advantage of all the benefits that the cloud and IoT devices can bring, with security at its core."

The network and supporting applications will be delivered via a single control pane, with the aim of making it easier to manage. Nasstar is using SD-Branch technology, including a local area network, switches and wireless access points that have already been approved by the MoD. ■

Jisc updates cybersecurity policy for Janet

Jisc, the membership organisation representing UK academic research institutions, has announced policy changes aimed at strengthening cyber security in how colleges, universities and research bodies use the Janet Network.

The body that also provides technology services to the sector said the change follows consultation last summer and becomes effective from April 1, with three key updates.

Firstly, organisations using the Janet Network will have to undertake an annual self-assessment of their security posture.

Secondly, there will be an expansion of the existing geographic location IP blocking restrictions, going beyond remote desktop protocols to block high risk protocols and ports. The restrictions will also shift from an opt-in control to being by default.

Thirdly, the remit of Jisc's computer security incident response team will be extended to perform vulnerability scans across the network, effectively giving it a more proactive role rather than just responding to exceptional circumstances.

"We've made the policy changes against a background of increasing threats and on the basis that raising security standards at individual organisations will help the resilience of the whole sector," said John Chapman, head of Janet policy and strategy. "For example, ransomware, which, according to our 2021 cyber security response posture survey, is currently the number one threat to further and higher education institutions, can spread among connected organisations."

He added that "it's important that individual research and education organisations understand their cyber security strengths and weaknesses" and that an annual self-assessment will help achieve this result.

"For now, institutions can use whatever assessment methods works best for them, but we will be collaborating with members through our security community group to see if there is a consensus on which method works best or whether we should work together to develop a sector-specific model," Chapman said.

The Janet Network provides connectivity for information sharing between 18 million users in education and research. ■

EDITORIAL:

Editor: Robert Shepherd
roberts@kadiumpublishing.com

Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Holly Andrews, Amyn Jaffer, Ian Richardson, Brianna Boudreau, Toby Sturridge, Navinder Singh, Dean Watson, Ferran van den Berg, Tero Pesonen and Steve Barber

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 to upgrade school Wi-Fi connections by 2025

Education secretary Nadhim Zahawi said all schools in England will have "lightning-fast" broadband by 2025 as part of the UK government's efforts to "level up education".

The government also announced a £150m funding to support schools most in need to upgrade their Wi-Fi connections.

In the next three years, the department for education (DfE) intends to reach out to schools in priority areas to facilitate the introduction of "faster and more reliable connectivity".

"Upgrading schools to high-speed broadband, setting out clear standards so that schools know what technology they should have in place, as well as providing funding to support them in achieving this, is the latest way we are levelling up education across the country," Zahawi (pictured) said at the Bett Show in London. "We need to use our experience from the pandemic as a springboard to embed new and better ways of using technology in schools, and across education."

The department said it is also publishing its first set of technology standards, aimed at supporting schools and colleges in understanding which technologies they should have in place to support effective teaching.

Schools and colleges will be able to access advice on the most recommended technology infrastructure, which itself will support best practices in helping pupils learn, it added.

The £150m provided to help schools upgrade their technology will include those in the department's previously identified education investment areas.

These 55 areas were first set out in the Levelling Up White Paper in February this year and refer to areas of the country where school outcomes are the weakest. ■

WWL hospitals introduces new telephony comms

Wrightington, Wigan and Leigh Teaching Hospitals NHS Foundation Trust (WWL) has expanded its partnership with unified communications specialist Cinos to replace its telephony system with an IP (internet protocol) solution.

The group in the northwest of England has gone live with the Cisco-powered unified communications (UC) service, which has been designed to deliver "full resilience and critical communications" including the NHS 2222 emergency line, which will be supported using a hybrid approach, both on-premises and in the cloud.

The new Cinos service delivers scalable cloud-based telephony and UC solutions that utilise both Cisco and Microsoft technologies.

"There's an ever-increasing demand for digital solutions and the new service will provide the trust with a robust, fit for purpose and always-on communications platform that gives our staff more time to deliver the best possible safe patient care," said Malcolm Gandy, chief information officer at WWL. "The service has been designed in line with our newly announced digital strategy, which supports our investment in the latest digital and cloud technologies. It was so important that we selected the right solution and right supplier for this project to ensure positive outcomes for our staff and our patients."

The service is underpinned by the UK sovereign Cinos Cloud platform and will support communications for all WWL Trust's 7,000 employees.

Roll out of the project is already underway and the contact centre solution went live in December 2021. ■

Fluke Networks launches the first live fibre detector – FiberLert™

Fluke, the global technology leader in the manufacture of compact, professional electronic test and measurement tools and software, has designed the world's first live fibre detector called FiberLert™.

The one-handed tool allows anyone to perform basic tests on fibre and quickly identifies polarity issues and failed transceivers. The presence of near infra-red light is indicated by means of an audible sound and LED.

The FiberLert can detect invisible near-infrared (850-1625nm) wavelengths used in fibre-optic communication to troubleshoot cable, port, polarity and transceiver issues.

Designed for one-handed operation, the FiberLert is an easy-to-use troubleshooting tool that allows technicians and engineers to simply test for the presence of near infra-red light without the need for complicated setup or interpretation of the measurement data.

When placed in front of an active fibre optic port or patch cord, the tester emits a continuous light and optional tone. The tool is unique in the market for users to resolve the cause of the communications failure in fibre-optic networks.

Fibre Networks carry a significant amount of data, and issues that arise can impact many users making a quick resolution essential.

"There are a lot of network engineers and technicians who need to test and troubleshoot fibre connections on an occasional basis, but lack the tools and expertise to do so," said Robert Luijten, Training Manager and Test and Measurement Expert, Fluke Networks.

"They are forced to guess as to the cause of a communication issue and replace components such as transceivers and patch cords in the hope of solving the issue."

FiberLert removes the guesswork by clearly indicating where the signal is present and where it is not. This allows users to quickly pinpoint and remedy the cause of the problem, such as a failed transceiver or failed patch cord and replace it.

FiberLert supports single-mode, multimode, UPC/APC patch cords and ports and can test without contacting the port or patch cord, reducing the risk of contamination or damage.

FiberLert's LightBeat™ feature flashes the LED, indicating a powered-on condition and good battery.

A timer shuts the tester off after five minutes of inactivity to extend battery life. Rugged design includes a convenient pocket clip and is backed by a two-year warranty.

UK gov offers £5bn under G-Cloud 13 framework

The UK government is launching a set of deals for cloud services and software which could be worth up to £5bn, under the auspices of G-Cloud 13. The Crown Commercial Services (CCS) – a central government procurement body – has launched the tender for a range of technologies under the eponymous computing model. The contracting authority, a special unit within the Cabinet Office, has published two procurement notices which describe a framework agreement for G-Cloud services, an arrangement within which providers can offer services under a fixed set of prices and pre-conditions. The framework is divided into lots covering cloud hosting (£750m), cloud software (£750m) and cloud support (£2.5bn), according to a tender notice. Setup, migration, and security is advertised under a different notice and worth up to £1bn. ■

VMware offers fully managed storage-as-a-service

VMware is rolling out the technology it uses for its cloud disaster recovery service and selling it as a cloud storage service. Cloud Flex Storage is a cloud-native offering that is fully managed by VMware and delivered with pay-as-you-go pricing on the VMware Cloud on Amazon Web Services (AWS) infrastructure. Customers can provision the storage quickly in the VMware Cloud Services Console without adding hosts and adjust their storage capacity as needed. "This is about scalability and elasticity with scaling disaggregated so you don't have to add more hosts to get more storage capacity," said Mark Chuang, head of product marketing for cloud storage and data. ■

STL launches end-to-end 5G enterprise solution

STL, an integrator of digital networks, launched what it claims to be the first end-to-end 5G enterprise solution to address the growing demand for private 5G enterprise connectivity for campus, industrial and venue applications. This 5G Enterprise solution will comprise Garuda, STL's O-RAN 5G indoor/outdoor small cells, CYRUS, open distributed unit and centralised unit from ASOCS and VMware edge compute stack as the virtualisation layer and cloud management. STL's Garuda small cell radio is designed for small, medium and large enterprises, supporting more than 30 concurrent user devices per radio. "Enterprises will now be able to leverage a robust, secure 5G network that is easy to scale and upgrade and drives greater levels of service efficiency," said Chris Rice, chief executive officer, access solutions, STL. ■

Ark plans new Wiltshire DC

Ark Data Centres is looking to build another data centre at its Corsham campus in Wiltshire, to be known as P5 South. Situated at its Spring Park campus on Westwells Road, near Corsham, the company is also requesting to build a plant, highways works, vehicle access, infrastructure, enclosures, landscaping and other associated works. The building will have a total floorspace of 6,020 sqm (64,800 sq ft) over three floors. In its application, Ark said it has acquired the "Hawthorn Works" site to the south of their existing Spring Park Campus consisting of two factory units and car park. The company aims to demolish the two warehouse units and also build a connecting bridge between P5 North and P5 South. ■

'Firms have limited awareness of cloud native security'

UK organisations have limited awareness of cloud-native security despite considering cloud-native application security a critical priority, according to cloud-native security firm Aqua Security. A survey, conducted at Cloud Expo Europe in March 2022, found that 49% of the over 100 cloud professionals polled said their limited understanding of the risks and lack of know-how was among the highest concerns relating to cloud-native security. It also discovered that less than a third of respondents (32.7%) consider cloud misconfigurations to be their biggest security concern. Among others considered riskier were malware attacks (54%), social engineering and phishing attacks (56.7%) and insider threats (32.9%). "As more applications are built and run in the cloud, it's no surprise we're seeing threat actors shift their focus to target cloud-native environments," said Paul Calatayud, CISO at Aqua Security. ■

Perfect Image acquires Technique

Pixel Group, the parent company of the cloud centric IT services and data analytics specialist Perfect Image, today announced the acquisition of Technique, a Berkshire based IT Managed Services Provider (MSP). The addition of Technique follows the acquisition of cybersecurity specialist Cyphra in 2021.

Operating within the Pixel Group's group strategy, the acquisition will create a specialist MSP focused on providing secure end-to-end IT solutions to mid-market organisations and SMEs across the UK.

"The addition will create a powerful proposition to deliver secure, end-to-end IT managed services to mid-market organisations across the UK," said group CEO Kelly Simkiss. "We see significant opportunities ahead for organic growth as we take advantage of the cross-selling and up-selling opportunities within each customer base."

The group said the acquisition will allow the group to establish a foothold in the south of England (Thatcham), to complement the existing operations in the north of England (Newcastle), Scotland (Glasgow) and Northern Ireland (Belfast), giving greater geographical reach, broader market penetration and increased sales momentum across the UK. ■

RBS and SBRC in training partnership

The Scottish Business Resilience Centre (SBRC) and Royal Bank of Scotland (RBS) have formalised a partnership whereby the bank will offer access to SBRC-delivered cyber security workshops for its corporate and commercial customers. Already an SBRC member organisation for five years, the Royal Bank of Scotland has been keen to increase the knowledge it imparts to its corporate and commercial customers around key trends, including cyber security. RBS will promote the workshops and relevant resources through *rbsbusinesshub.com*

Word on the web...

Optimising your storage strategy

Florian Malecki, executive vice president, marketing, Arcserve

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

Now's the time for accurately communicating sustainability credentials

Amyn Jaffer, Ultima Labs director

Carbon reduction commitments are important for every business, no matter what industry or region. By 2023 all publicly listed companies and financial institutions will have to detail how they intend to meet the UK's 2050 net-zero carbon target. Right now, around half of smaller UK businesses fall within being 'Carbon Complacent' or 'Carbon Exposed'.

Previously, it's been too easy to pay lip service to the issue. Too often, businesses have put the cart before the horse – proclaiming environmental benefits or boasting better sustainability than their competitors before they have the underlying data. Regulators are becoming bolder in cracking down on such behaviours, which can amount to greenwashing, with moves such as the UK's Green Claims Code launched in September 2021.

We're already seeing customer choice being influenced by a company's commitment to the environment, and this is likely to grow in the future. Customers won't buy from companies unless they can demonstrate their commitment to the environment. It's an issue that binds all organisations – regardless of industry or size – and businesses need to show that they are taking sustainability and reducing their impact on the environment seriously.

So how can businesses take practical steps to reduce their impact on the environment?

The estimated total carbon emissions generated by IT is around 1.4% of the global greenhouse gas (GHG) footprint, and by 2040, this number is expected to hit 14%. Data centres make up the largest share of this percentage (45%). But a 2018 study found that Microsoft Azure is up to 93 per cent more energy-efficient and up to 98 per cent more carbon efficient than on-premises solutions. It's estimated that a greater reliance on cloud computing can reduce per-user carbon footprint by 30% for large companies and 90% for small businesses. Cloud brings flexibility around scalability and prevents wasted space and energy resources from being used by companies who rely on their own data centres.

While the cloud offers vast improvements in carbon performance compared to on-premises, continuous scrutiny of the digital tools we deploy is essential, and our consumption should be transparent. Sustainability calculators for the cloud provide businesses with a way of demystifying their carbon footprint and giving a solution-based approach to calculating their impact on the environment. At the same time, it allows them to demonstrate cost savings and the more comprehensive benefits of the cloud to the rest of the organisation.

There is now a specific carbon footprint calculator, for example, that will show customers how much they can reduce their carbon footprint by moving compatible workloads to Azure. This assessment tool enables businesses to assess their estates to help them evaluate which on-prem workloads would be suitable for Azure, the Azure VM types recommended for the target environment, the cost of hosting those workloads in Azure and the carbon saving they would achieve.

For example, the sustainability calculator demonstrates that a small business that has eight virtual machines running workloads in the cloud instead of on-prem would save:

- 12,913 miles per year saved.
- 5 acres per year saved.

This is based on:

- 7,800 CO2 kg per year - the amount of carbon footprint generated by purchasing and running similar physical servers through their entire lifecycle per year on-premise.
- 1,793 CO2 kg per year - the amount of carbon footprint generated by running these compatible workloads in the cloud through their entire lifecycle per year to compare with the on-premises figure.

Quantifying the carbon impact of each Azure subscription gives a business tangible data for reporting existing IT-based emissions. It allows a company to see estimated carbon savings from running those workloads in Azure versus on-premises data centres. It's also the first step in establishing a foundation to drive further decarbonisation efforts.

As well as energy efficiency, renewable energy, circular economies, asset disposal, and refurbishment of technology should all be areas of focus. From paperless offices with low energy lightbulbs and automatic power down to using specialist companies like N2S to recycle old equipment responsibly, every aspect of a business should be assessed to see how it can be changed to help reduce its carbon footprint.

The task of reducing global carbon emissions may sound challenging, but rather than be disheartened, it's vital to recognise that every business has a role to play while still being able to flourish. Investing in sustainability is good for business, good for customers and good for the planet. ■

Register for Networking+

Russian ransomware attacks are on the rise

By Holly Andrews, managing director, KIS Finance

In a joint review of cybercrime trends led by the UK, USA, and Australia, it was found that the number of sophisticated ransomware attacks originating from Russia, or being carried out by Russian speakers, has been on the rise over the last year.

Last October, the UK's cyber agency GCHQ also stated that UK ransomware incidents had doubled.

This threat is now being highlighted in government after chief of the defence staff admiral Sir Tony Radakin told the cabinet earlier this month that the UK needs to be ready for a wave of Russian based cyberattacks over its defence of Ukraine.

According to the National Cyber Security Centre (NCSC), the top sectors often targeted in ransomware attacks are:

- The NHS
- Universities and schools
- Businesses (including SMEs)
- Charities
- Law firms
- Councils

For example, at the start of February KP Snacks (makers of McCoy's crisps and Hula Hoops) suffered a ransomware attack resulting in a supply disruption which is expected to last until the end of March at the earliest.

Ransomware is a type of malware that employs an encryption software to the user's device in order to hold their information at ransom. The information or data is encrypted so that the user can't access or read their own files or databases. The criminals then demand a ransom (payment) in order to release the information back to you.

This type of attack can be crippling for organisations and businesses that hold and rely on large customer databases.

Most ransomware attacks happen via unsafe websites, text message links, or email attachments that are sent to an employee of the company or organisation. This means that every company and organisation that uses email services is a potential target.

Once the attachment or link has been clicked on, it activates the malware which then infiltrates the user's device and encrypts any data or information held. These criminals are smart and their attacks are usually targeted to a specific person that has access to important files and databases.

There isn't one single method that can be used to prevent ransomware attacks, so you need to implement good cyber security practices across your business in order to mitigate the risk and potential losses if you do fall victim to an attack.

1. Educate your employees

Your employees should be your first line of defence against ransomware attacks so it's vital that everyone on your team is educated on how to identify cyber threats. Your employees should know never to open email attachments from an unknown source or to download files or software from anywhere that isn't a known and trusted source.

It's also important to keep your employees updated on all the latest threats and any new tactics that these criminals are using so they know what to keep an eye out for.

2. Keep anti-virus software up to date

Just having anti-virus software in place isn't enough; it needs to be regularly updated in order to be effective.

Make sure that every device in your company or organisation is regularly updated with the latest anti-virus and anti-malware software. Having software that updates automatically and runs regular checks will give you the greatest level of protection against any potential threats.

3. Limit access

In order to limit the risk of ransomware threats, it's important that you limit access of important files to those who really need it. Giving employees access to databases and files that they don't need only widens the risk as criminals have more targets for their attack.

4. Backups are essential

It's absolutely essential to have backups of important files and documents. This is especially the case if your business can't operate without them as backups will allow you to still have access to your data in the event of a ransomware attack, lessening the impact on your business.

Backups should be stored either offline, or in a system that is entirely separate from your business' operating systems.

5. Have a response plan

Although taking these safety measures will mitigate the risk of an attack, nothing is 100% bulletproof and there's still a chance that a ransomware attack can happen. In which case, setting out a response plan ahead of time will ensure that you can respond quickly to a threat.

Make sure that all of your employees know who should be alerted in the case of an attack and what steps they need to take after a breach. ■

No PoE, No Problem
Don't delay a project!
Find DrayTek APs that ship with an external power supply.
Find Your Solution
DrayTek
web: www.draytek.co.uk | tel: 0345 5570007

You’ve got backup – but how safe are you?

Ian Richardson, head of innovation, CSI

Server room floods, ransomware, fires – however your data is damaged, lost or digitally encrypted – do you know how quickly you can retrieve it or even if you can? iland found in a recent survey that just 50% of businesses are testing their disaster recovery (DR) plans only annually or at less frequent intervals, while seven percent did not test their DR at all. Of the organisations testing less frequently, half said their disaster recovery plan may be inadequate based on their most recent DR test, while 12% encountered issues that would result in sustained downtime. Zero respondents said that their DR test was completely or moderately successful. Everyone reported experiencing issues.

So, with most companies remaining badly behind the curve, what steps are needed to ensure that you can retrieve your data after a data breach or disaster?

The datasets of organisations are huge, but the ability to retrieve 100s of terabytes in minutes is like having a spare car in your garage just in case your main one doesn’t work – it’s expensive to have it all waiting on the off chance you need it. And the faster you need it back, the more it costs.

Therefore, a core aspect of a DR strategy is to prioritise the data that is most critical to the business and focus your efforts around protecting that data first. To understand your data, look at your entire estate and define what’s critical to your business operations. Prioritise it in order of how it would impact customer delivery most if lost. It will give you a focus, and in turn, you can develop measures to minimise data loss in the event of a cyber-attack or disaster. You can also catalogue it by how much data can be lost by invoking a recovery (RPO) and its priority for recovery (RTO).

Obviously, there is a cost implication for any backup and with datasets increasing, it can be very expensive to store all your data in multiple, high availability data centres. In some cases, the costs are too prohibitive to justify. Virtualisation tools at the server or storage layer often use cloning or snapshot capabilities that serve as ‘back-up’, but these consume space in your production storage which is likely to be the most expensive in the environment.

Using one method for priority data backup and another for less important data can reduce costs here. Ideally, mixing disk, tape and cloud storage strikes the right balance between cost and speed. Archived data could sit happily on cheaper tape, but your essential systems, applications, and databases should really be committed to replicated disk. That way, you’ll be ready to restore essential systems rapidly if disaster strikes.

But it’s not just the process of backing up your data that’s important; it’s what happens to it after. Historically DR processes would have been slow. As datasets have grown, the emphasis has been more on cloud backup rather than disks. Here it’s prone to the same risk of cyber-attack – meaning someone could get hold of your backup as well as the company data, challenging a full recovery. So how do you ensure this data is safe?

There is no one-size-fits-all when it comes to data backup. Whether on the cloud, disk or tapes it’s critical to protect these backups as you would any other data. If using a physical backup, consider storing these offsite in another location, or at least a different building. You may have to qualify this to regulatory audits or your own security assessment. A fire or natural disaster could be all it takes to wipe out all your data along with your backups.

If storing digitally, use a separate file system or cloud storage service that’s located either on a physically or logically separated network. Minimise who has access to these login credentials and keep them on a separate enterprise directory to minimise cyber-attack induced risks. Keeping your data offline and inaccessible is also an effective way of keeping your data out of the hands of cybercriminals. This is known as an ‘air gap’.

Backup is an insurance policy for your businesses, but unfortunately, the process is often run on a shoestring budget and deprioritised over other more visible projects - until it’s needed. Most businesses don’t have a backup strategy and if they do, the error is that they’re not testing it. Cyber security frameworks strongly advise regular testing including who to tell if there is a loss, where the backups are stored, how long it’s going to take to recover and how to ensure these backups are stored safely. Automation technology can also locate new servers and applications that have been added to the network and provide notifications if it doesn’t look like it’s been backed up.

You can’t afford for that recovery to take days or weeks. Brands lose customers instantly when a data breach is reported in the media and it can take months or years to undo the damage. Proper governance of critical data can maximise revenue, customer satisfaction, and operational cost-efficiency leaving your business resilient against the threat of data loss. ■

Exploring the criteria for SD-WAN adoption

SD-WAN has gained a lot of traction over the years as enterprises look to modernise their networks. But what criteria do businesses use – in other words, how do they know they need it? Robert Shepherd investigates

SD-WAN deployment by enterprises has grown substantially over the last few years.

Indeed, a report by Dell'Oro Group published last year, forecasts worldwide sales of SD-WAN technologies to grow at a compound annual growth rate (CAGR) of 24% over the next five years, with the market expected to surpass $4bn in 2025. Much of that acceleration, the report says, will happen in 2022.

Additional highlights from the *Dell'Oro Group SD-WAN Advanced Research Report*, include: software accounted for more than 80% of SD-WAN revenue as of 2021, with its contribution expected to rise over the next five years.

Initially launched as a method of optimising data traffic across MPLS and IP-based connectivity, it's evident that SD-WAN has assumed a rapid pace of evolution.

Still, deploying SD-WAN might not be for every company – so, for those that are unsure, how do network geeks evaluate whether it's a necessity for their enterprise?

Dean Watson, lead solutions expert, professional services at IT specialist Nuvias,

says the business in question must consider the following questions: "Is our WAN footprint complex? Do we have branch locations that are difficult to service with high quality WAN links? Is our premise footprint dynamic? What are our current longest latencies and what would these look like with SD-WAN?"

For Toby Sturridge, chief technology officer, SDWAN Solutions, the list is endless.

"Where do we start?" he says. "There is an SD-WAN solution for every type of customer and requirement, from a single site that is perhaps moving to VOIP all the way through to enterprises with hundreds of sites. Any company that wants more network control, more visibility, more functionality, with less cost; or any company moving from MPLS to Cloud applications, expanding to new locations, opening more sites, or going through a digital transformation, using technology to the full benefit."

It's not just the vendors that (quite understandably) extol the virtues of and wax lyrical about SD-WAN. Brianna Boudreau, senior research manager at TeleGeography, the telecommunications market research firm, points to numerous reasons that have led enterprise customers to adopt this approach.

"Corporate traffic patterns and whether or not a team is already using a hybrid WAN are among the biggest drivers," she argues. "Covid-19 and the shift to hybrid work environments accelerated the adoption of cloud services and forced WAN managers

"The WAN today requires (a lot) more bandwidth. Particularly as enterprises continue to adopt cloud services and rely on bandwidth-hungry video/UCaaS tools to keep employees connected in today's hybrid work environment"

Brianna Boudreau, TeleGeography

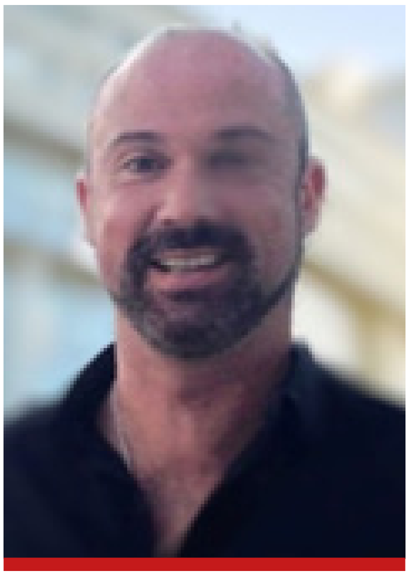
to permanently accommodate a remote-friendly, bring-your-own-device world. The drag on application performance due to indirect connections to cloud service providers has made traditional, all-MPLS networks less attractive."

Indeed, Boudreau says that "as a result", a majority of enterprise customers are pushing an internet-first WAN that integrates DIA and broadband alongside MPLS. "In fact, our latest WAN Manager Survey indicated that WAN managers had DIA running at 42% of their sites in 2021," adds. "For the first time, MPLS usage dipped below half of average sites—46% of sites were running MPLS in 2021."

Boudreau says another factor is network complexity in that while WAN managers can configure traditional CPEs to support these hybrid network designs, management can quickly become complex and burdensome as the network scales up. She says SD-WAN has been a major innovation in assisting enterprise network operators to manage this complexity.

"And third is the budget," adds Boudreau. "The WAN today requires (a lot) more bandwidth. Particularly as enterprises continue to adopt cloud services and rely on bandwidth-hungry video/UCaaS tools to keep employees connected in today's hybrid work environment. Our latest WAN Manager Survey also revealed that across MPLS, DIA, and broadband, the percentage of large port sizes being procured is growing, while port sizes 50 Mbps and under are declining 1-3% compounded annually. SD-WAN allows enterprise customers to integrate more cost-effective internet services into their WAN without sacrificing performance or security. For enterprises with increasing bandwidth requirements, but limited budgets, this makes SD-WAN appealing."

Speak to any business owner around the world and different approaches and cultures lead to different rationales when deploying new technologies in methods.



"There is an SD-WAN solution for every type of customer and requirement, from a single site that is perhaps moving to VOIP all the way through to enterprises with hundreds of sites"

Toby Sturridge, SDWAN Solutions

"Software is eating the world, and it also eats the WAN. SD-WAN, which brings programmability to wide area networks, is the logical evolution of enterprise networking technology"

Ferran van den Berg, Cerebo Networks

But what, historically, is the biggest selling point of SD-WAN?

For openers, Gartner estimates SD-WAN solutions (not Sturridge's company) can save 50% of both CAPEX and OPEX, compared to existing WAN routers. Meanwhile, Forrester's Technology Adoption Profile states "90% of network managers want to evolve their WAN using a software-define approach".

There are other biggest selling points, too.

"Originally, enterprise customers cited cost savings and leveraging multiple transport technologies as the main drivers for considering SD-WAN," says Boudreau. "While cutting costs is certainly still a motivation, customers are also looking at the agility, security, and superior performance that an SD-WAN enabled network can provide. In fact, when we

“The migration of legacy systems to next-generation technologies always poses a challenge and in this case may require a significant amount of effort”

Navinder Singh, In2IT Technologies

last surveyed WAN managers about their SD-WAN deployments, increasing site capacity, adding alternative access solutions, and improving network performance were the three most common reasons for adopting SD-WAN.”

Ferran van den Berg, managing director of Netherlands based MSP Cerebo Networks, adds:

Software is eating the world, and it also eats the WAN. SD-WAN, which brings programmability to wide area networks, is the logical evolution of enterprise networking technology. There are many different use cases for SD-WAN and enterprises must explore which use cases apply most for them, but any organization that still uses MPLS or traditional internet VPNs or needs to support the transition to the cloud, will gain benefits from SD-WAN.

As far as the UK is concerned, Sturridge says “it’s never been about cost, as there is not much difference in price between MPLS and DIA as an example”. He continues: “It’s always about performance, oversight and productivity, what the applications are and need, and being able to do more with less - be that less staff or indeed less costly connectivity technologies i.e. 4G or FTTx vs DIA. Add in covid-induced remote working or working from anywhere i.e. accessing corporate applications from anywhere and the business need for feature rich, simple, resilient and redundant SD-WAN is undeniable.”

Van den Berg argues that MPLS and hybrid networks have brought a lot of complexity to customers, but SD-WAN takes this complexity away. “Historically, SD-WAN sales have largely been driven by the increased adoption of SaaS applications, as enterprises want direct and optimised cloud access from the branch which is hard or impossible to realise with traditional solutions,” he says. “SD-WAN provides full control over the network via centrally configurable application policies, without the need for enterprises to worry about the complexity of the underlying network whatever WAN transport they are using.”

SD-WAN still has its detractors and critics. When researching for this feature, I was told:

“As remote work remains a part of everyday life, architectures like SASE are better suited for remote access than SD-WAN.”

With claims like that, does SD-WAN really stand up to scrutiny?

Sturridge says “we read scary statements like this every day”, which it claims are predicated based on fundamental misunderstanding of SD-WAN and SASE technologies.

“SD-WAN is a technology, SASE is a framework - they are not directly comparable,” Sturridge adds. “Anyone who is purporting to compare SD-WAN and SASE does not understand the terms well enough. SASE stands for Secure ACCESS Service Edge (the ACCESS part being SD-WAN) while SECURE SERVICE EDGE relates to multiple security technologies offered as part of the security framework. SSE is just SASE without SD-WAN and SSE does not have any resiliency or redundancy. Nor does it have any dynamic traffic management.”

When it comes to remote working – something many of us do now, thanks to Covid-19, Sturridge says his company’s products like SDWAN Remote and SASE Remote (both deviceless SD-WAN, one with and one without a full UTM security layer) fulfils work-from-anywhere criteria while still offering the benefits of SD-WAN at commercially attractive rates - with no VPN concentrator or manual VPN tunnel setup.

“Working from your home or from a coffee shop, using WI-FI or guest Wi-Fi and tethering from your mobile phone simultaneously to securely access the Internet or your corporate applications - over multiple connections, whatever they may be - and at the same time separating and securing your traffic from all other traffic on the same networks,” says Sturridge. “So if you’re at home in the middle of a virtual meeting and the kids decide they all want to watch 4k films simultaneously, it won’t degrade your meeting.”

Another accusation levelled at SD-WAN is cloud-native SASE offerings perform better and provide greater consistency than using SD-WAN. Again, Sturridge shoots this claim down.

“Cloud-native SASE doesn’t exist, but cloud-native security exists (SSE) and it works alongside SD-WAN for secure local internet breakout etc.,” he says. “But something has to route that traffic intelligently to the Cloud SSE – and that’s where the SD-WAN comes in.”

For Watson, “context is key here; many SASE offerings position a ‘backbone’ component to their solution to provide greater consistency than just sending international traffic over the internet’. He continues: “Some SASE vendors have built a dedicated infrastructure for the backbone, others piggyback over Azure vWAN or AWS inter-region links. This means that for international use-cases SASE solutions with a backbone can offer more consistent performance, but for domestic or regional use cases (Europe) where there is an inherent low latency between locations there would not be a tangible benefit to having a backbone as part of the solution.”

Businesses have fundamentally transitioned over the last two years, with working remotely or from home now firmly entrenched as both normal and desirable. This shift away from the secure networks of a closed office environment, toward more open networking using various cloud services and public internet, has been something of a challenge.

“The migration of legacy systems to next-generation technologies always poses a challenge and in this case may require a significant amount of effort,” says Navinder Singh, GM at In2IT Technologies. “It can also be a costly exercise to migrate existing networks onto an SD-WAN infrastructure, because this new protocol uses virtualisation extensively, which may not be supported by existing infrastructure. This would then mean that the entire backbone would need to be overhauled.”

However, Singh says that with any technology transition, having an experienced partner that understands both technology and business is instrumental. “The ultimate goal of SD-WAN is to enable flexibility and easier management, which requires a well-planned and well executed migration,” he adds. “A trusted IT partner will ensure that the promise of SD-WAN, including cost savings, improved performance, enhanced reliability and increased cloud readiness, are actually delivered.”

SD-WAN is certainly not going away – it’s evolving. In fact the Dell’Oro Group report also predicts that SD-WAN vendor consolidation is to continue over the next five years following a surge of acquisitions in 2020. That’s something worth looking at in the next SD-WAN feature. ■

“Is our WAN footprint complex? Do we have branch locations that are difficult to service with high quality WAN links? Is our premise footprint dynamic? What are our current longest latencies and what would these look like with SD-WAN?”

Dean Watson, Nuvias

How technology is helping the NHS

NHS and trusts are embracing the the latest technology. Here's how its helping day-to-day

Creating a simpler user experience for staff, patients and visitors

As part of the national response to the Covid-19 pandemic, the NHS Nightingale Hospital Exeter was opened to provide additional capacity to care for those with Covid-19. The 116 bed NHS Nightingale Hospital Exeter was purpose built at speed in just 8 weeks. A crucial part of the build was the requirement for a robust, scalable and reliable network to support IT teams and healthcare staff to deliver better patient outcomes. Secure Wi-Fi network was a top priority to ensure operational efficiency to provide critical equipment and responsive care.

Nightingale Hospitals were conceived in a crisis. They had to be built in a matter of weeks ready to deal with an unpredictable and dangerous pandemic. The Exeter hospital required a comprehensive, reliable wired and wireless network across the site within weeks. The ability to deploy a major IT solution so quickly could be genuinely lifesaving. There was a clear need for fast, reliable Wi-Fi throughout the new hospital as well as outside in the area where ambulances arrive. The presence of state-of-the-art wireless and wired medical equipment throughout the site also posed a challenge to the network designers. A high level of tailoring and flexibility was essential. The solution had to meet the diverse needs of many different users, accessing both their own and NHS-owned devices. This could range from medical staff using Wi-Fi enabled medical equipment to families talking to their loved ones by video (to avoid close contact). Simple, empathetic experience design tailored to the individual user's needs was, therefore, key to this project's success. With so many different users in such a data sensitive medical setting, robust network security was a must. A solution was required that would allow both registered and guest users fast, easy access on any device while offering a high level of cyber security across the network.

Deploying a major IT solution quickly and effectively could potentially save lives during the global pandemic and a number of solutions were put in place to make this a reality.

The Royal Devon and Exeter NHS Foundation Trust selected Qolcom and HPE Aruba, both well-known and trusted IT partners to the NHS. Many surrounding hospitals already depend on Qolcom's service and support experience, alongside HPE Aruba's network technology. This on-the-ground presence meant that the time to deploy was significantly reduced. Central services could be rapidly extended to the Nightingale Exeter for authentication–via Aruba ClearPass and for management, via Aruba Airwave. Qolcom's experience in the healthcare sector counted for a lot. In particular, its ability to devise a network strategy quickly to meet diverse user needs proved decisive.

Qolcom, together with HPE Aruba, worked in collaboration with the RD&E to deliver a robust, user centred network solution in a very short timescale. The solution was a tailored design based on a physical and logical extension of the RD&E LAN and WLAN to the NHE.

The network solution had four defining features, each contributing to meeting the Nightingale Hospital's precise requirements:

Granular security (for Wi-Fi and wired network)

With Aruba ClearPass, the Trust gains the robust cyber security features of a wired network in a wireless environment. ClearPass combines context-based policy management with next-generation AAA (Authentication, Authorization, and Accounting) services for highly secure mobile connectivity. This simplifies the management of network access policies, onboarding, guest user access and multiple device use - all from a single platform.

Dependable hardware, intelligent design

Every aspect of the solution was designed to ensure a secure, reliable network. For example, the Aruba hardware components selected by Qolcom for the LAN and WLAN solution included Aruba 8325 and 6300M switches, 515 and 365 access points and UXI Sensors. Qolcom designed a simple, resilient two tier topology based on a dependable collapsed backbone architecture. At the core/aggregation layer are two Aruba 8325 switches deployed as a high-availability cluster to maximise up time. In addition, Aruba's Virtual Switching Framework (VSF) feature allows multiple switches (up to 10) to be managed as one.

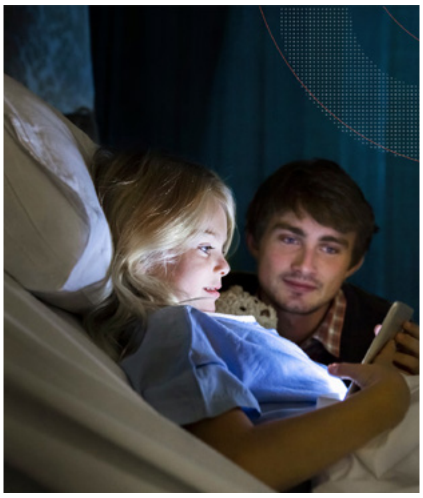
Wireless connectivity, centralised control

Fast, reliable Wi-Fi access is provided by several Aruba 515 series access points throughout the Hospital. A pair of Aruba 365 series external access points provide good Wi-Fi coverage to the area south of the building where ambulances bring in patients. The Aruba access points terminate on the mobility controllers hosted at the RD&E, with centralised management enabled via the Aruba Mobility Master. The new Hospital is connected to the RD&E network over two dedicated 10-Gigabit BT circuits via core/aggregation switches interfaced directly with the WAN equipment.

Collaborative delivery 3 4 and 24/7 support:

As with all Qolcom projects, the Nightingale project was delivered in three distinct phases - Plan, Document, Implement - all of which were accelerated to meet the time-critical demands of this project. Close collaboration between senior Qolcom team members and the Royal Devon & Exeter IT team confirmed the scope of the project. The working design was agreed quickly, followed by rapid sign off and implementation. Qolcom's engineering team worked closely with RD&E teams on all configuration tasks relating to the wired and wireless network. This was followed by full documentation and knowledge transfer. 24/7 tailored hardware/software support is now in place via a secure remote connection.

A fast, reliable and secure IT network was delivered for the Nightingale Exeter – to a very tight timescale and on budget. The network offers superb wireless and wired connectivity throughout the site, with context-based security, reducing the IT team's security headaches. Network management is greatly simplified, across a wide mix of users and devices. Healthcare workers can now quickly locate critical equipment through Wi-Fi enabled tracking, saving time and potentially lives, whilst patients are benefiting from a home-from-home experience to ensure they feel comfortable and can still speak to their loved ones through video chats (when close contact isn't possible). The role played by IT in delivering improved healthcare experiences at the NHE was critical and with the support of Qolcom and HPE Aruba, the NHE is ready to play its part in treating patients with coronavirus. Its highly secure, easy-to-manage network infrastructure means it is also very flexible – so it can adapt to changing requirements in a rapidly-changing healthcare emergency. ■



Bringing virtual and face-to-face consultations together at Buckinghamshire Healthcare NHS Trust

Nasstar has worked with Intouch with Health (part of VitalHub Corporation) to deliver a new system at Buckinghamshire Healthcare NHS Trust, enabling it to serve more than half a million patients annually with a virtual consultation platform that fully integrates with the two patient administration systems (PAS) used across the Trust.

The former was charged with delivering its customisable OneConsultation platform, providing secure, easy to access virtual consultations from a familiar interface based on Microsoft Teams. This has been combined with the Intouch with Health Flow Manager and Virtual Clinics applications, enabling a simple, single view of all patient appointments. By delivering a comprehensive patient flow management dashboard for all appointments it means those patients that have a virtual consultation can be managed on the same platform as those patients who present physically (face-to-face) at the hospital.

Due to the nature of its care delivery, Buckinghamshire Healthcare NHS Trust operates two patient administration systems. Integrating the virtual appointment pathway with both systems provides the Trust with a standardised approach to virtual consultations, and enables staff to schedule, manage and conduct virtual consultations as comprehensively as face-to-face appointments.

This partnership is a pioneering example of modern patient management and patient flow, as many NHS Trusts across the country increasingly look to offer patients the choice of consultation type post-pandemic. With the ability to manage both formats seamlessly, the unified system can assist in alleviating the ongoing pressures currently placed on the NHS.

Ross Fullerton, interim chief digital and information officer, Buckinghamshire Integrated Care Partnership comments: “Like most NHS organisations, Buckinghamshire Healthcare NHS Trust has a range of systems with service specific functions. What Nasstar and Intouch with health are doing is getting them to ‘talk’ to each other so that we are more prepared for the ‘new norm’ and can deliver the flexibility that the 500,000 patients we serve annually demand. It means we can be more efficient and provide patients with a fully ‘joined up’ experience, regardless of whether it is in person or virtually.”

Ben Mitchell, account manager at Nasstar adds: “Blended appointments will increasingly become the norm, but the delivery requires tight integration between various systems and the ability to provide a secure virtual consultation experience that is also easy for a patient to navigate. The joint offering between Nasstar and Intouch with Health provides this, showcasing an exciting future for healthcare.”

This digital system is now being piloted across Buckinghamshire Healthcare NHS Trust including hospitals at Stoke Mandeville, Wycombe, and Amersham with further plans to provide virtual consultations across all services including acute and community. In total, Buckinghamshire Healthcare NHS Trust has approximately 6,000 highly-trained, qualified doctors, nurses, midwives, health visitors, therapists, healthcare scientists and other support staff and cares for more than half a million patients every year.

Mike Sanders, CEO of VitalHub UK comments: “Covid-19 has fundamentally altered life over the last year. The global pandemic has, without doubt, been a catalyst for change. Our collaboration with Nasstar shows what can really be achieved with embedded solutions that are fit for purpose as we move forward, providing many benefits for staff such as a reduction in administrative workload, as well as an improved patient experience. Integrating the virtual consultation pathway with both patient administration systems creates a joined-up, sustainable, technological infrastructure at the trust level which can be scaled across geographical regions at ICS level, realising operational and experience benefits previously unobtainable.” ■

Emergency treatment at the Nightingale Hospital for patients suffering with Covid-19

Visbion is a specialist in medical image acquisition, distribution, management and display solutions. During the early planning stages of the UK’s response to tackling emergency treatment for patients suffering with Covid-19, they were approached to help provide solutions to offer screening for patient’s lungs, to help evaluate treatment strategies.

The Nightingale hospital, launched at the Excel in London on April 3rd, 2020, was constructed and operational in just 10 days, therefore there were significant pressures to deliver an operational and proven lung screening solution, within these time frames.

Encrypted transmission of scans direct from the scanning trailer within the Nightingale facilities are required for the trusts to ensure specialist reporting of the images and safe archiving.

Because of the time limitations and requirements for an extremely reliable and a highly secure method of data transmission, 4G cellular technologies were the clear choice to deliver on all technical, budgetary and rapid deployment criteria.

The Visbion Image Cube product ensures scans are transferred rapidly and securely to the hospital’s systems, ready for immediate diagnosis. Utilising the high speed 4G mobile networks provides highly efficient remote support and management of the system.

When the mobile unit is deployed, the Image Cube automatically connects to the approved network so that it is ready to scan and send data immediately, without the need for costly fixed line Fibre or Ethernet networks to be installed and avoid onsite installation delays, ready for immediate diagnosis. Utilising the high speed 4G mobile networks provides highly efficient remote support and management of the system.

By using a customised hardware solution, provided by Adey Electronics, comprising of an Advantech 4G router and a bespoke Mobile Mark dual 4G & GPS antenna, Visbion were able to ensure the communications were established to their screening kit immediately. The high-gain customised antenna provides a robust means of establishing external wireless communications to the mobile unit in a challenging and congested airspace within the busy Excel centre.

The Advantech industrial dual SIM 4G Libratum router means the best mobile network is intelligently monitored and selected to provide optimum throughput, reliability and performance, this is invaluable when connected to critical devices that need ‘always-on’ connectivity.

To provide full visibility and management of the solution remotely, Visbion also utilise the Advantech RSeeNet secure management platform to gain visibility of the 4G performance, connectivity statistics and get notifications to manage the communications system and provide the best solution to support the frontline team.

This was the first of the NHS Nightingale Hospitals to benefit from Visbion’s technology with the Image Cube solution now being used in subsequent NHS Nightingale’s in Harrogate, Bristol and Birmingham. ■

Securing IoT assets

Craig Price, SVP mobility products and marketing at Console Connect by PCCW Global

Already, 2022 is the year of Internet of Things (IoT). The widespread adoption of these devices shows no signs of slowing down. In fact, as revealed by IDC, IoT spend in Europe hit US$202bn in 2021 and will continue to grow in double-digits throughout the next four years.

The development and speed of adoption of IoT technology will also have an immense impact on businesses that are looking to improve cost efficiency and productivity. We've seen significant investments in IoT-related developments from the hyperscalers, such as Amazon's updates to long-distance wireless protocol and IoT RoboRunner. Strategic moves from big players sends a clear signal that the market will expand even further this year.

Inevitably, with greater reliability on IoT in the enterprise, the amount of collected data will also increase. But how can businesses ensure data safety and protect their network of connected devices?

Who takes responsibility?

With more devices added to the IoT ecosystem, there is greater exposure to a variety of threats. As the devices aren't patched regularly and come with default passwords that aren't often changed, threat actors can easily access these devices and use them as a backdoor into a network, and infect them with malware to create a botnet for the purpose of a DDoS attack. It doesn't come as a surprise that there is a growing pressure on IoT security, as governments and watchdog organisations continue to push new regulations. Much of this pressure is likely to fall on supply chain and device producers.

For instance, the UK's recent bill will require manufacturers and distributors to comply with new security requirements – for instance ensuring that consumer connectable products are more secure against cyber-attacks, protecting individual privacy and security. Although these legislations point in a positive direction, the change won't happen overnight. Enterprises can't simply sit and wait for more secure devices to enter the market.

Meanwhile, the massive volumes of data businesses produce and store via IoT can only be processed in the cloud. Therefore, securing sensitive information needs to be every enterprise's priority. With increasingly complex IT environments, end-to-end device connectivity will also pose more challenges, often involving a combination of local and international connections, public internet, mobile and Wi-Fi networks, and private and public clouds.

Risks of unsecure IoT

Unsecured IoT devices have been used as attack vectors for some of the largest DDoS attacks over the last few years, which shows that customers must be wary of not only having their network penetrated, but also being used as an attack surface.

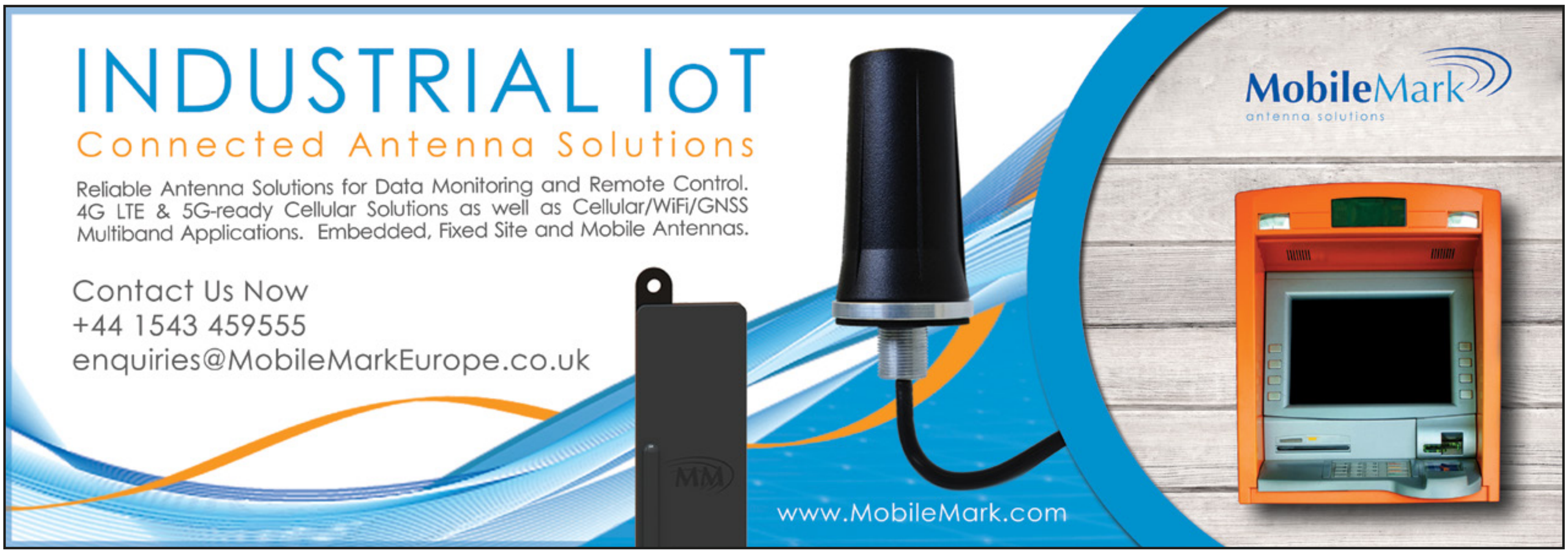
IoT networks are an extension of an organisation's network and typically need more security since IoT devices can physically be located anywhere. Compromised networks are costly, whether it be harm to reputation or worse. Attacks are becoming more sophisticated, to take advantage of how vast and physically dispersed IoT networks can be – security threats include IoT botnets and ransomware.

Furthermore, IoT system's attack surface can be significant with endless connections to data centres and clouds. To protect such an interconnected web, businesses need solutions that are scalable and grow along with an organisation's network.

Many IoT devices break into the internet using old security protocols. In an ideal world, the safest way to protect your IoT device is to get it off the internet. By doing so, this removes the ability to attack the IoT network from a random internet location. In fact, IoT devices can be connected directly to the cloud and back again, without going through any internet.

Companies can securely connect and transfer IoT data from device to designated data clouds or data centres over a private interconnection. By using a global connectivity platform that enables secure and flexible connection between assets, companies are empowered to activate (or deactivate) devices in real-time, have control over service configuration and traffic monitoring and gain better visibility over the IoT network.

It's likely that we'll see more and more IoT-driven enterprises in the near future. With complex ecosystems of devices and ever-increasing amounts of data generated, companies need solutions that will not only protect customers but also organisations themselves. By removing the IoT network from the internet, IoT security is greatly improved. Let's make 2022 the safest year of IoT. ■



Managing the deployment of mission critical broadband applications

Tero Pesonen, chair of the Critical Communications Broadband Group and vice-chair of TCCA

Around the world, the emergency services and other first responders are increasingly using broadband applications to augment existing mission critical voice and narrowband data services, such as those delivered by the Airwave network in the UK. This is catalysing a focus on the quality of 'mission critical' applications.

Unlike consumer apps, mission critical apps may be supporting users in life or death situations, and there can be no weak link in the ecosystem. This means that the successful implementation of mission critical applications will be a complex task. TCCA, the global representative organisation for the critical communications ecosystem, has published an advisory white paper that looks at the key considerations that need to be taken into account when developing and deploying true mission critical applications.

Authored by TCCA's Critical Communications Broadband Group (CCBG), the white paper provides guidance to Public Protection and Disaster Relief (PPDR) operators and users as they define their strategies for deploying and managing mission critical applications utilising broadband systems. In parallel, the paper aims to inform application developers on the specific requirements for delivering mission critical solutions over broadband systems.

Operators of public safety networks need to clearly understand users' requirements and the risks they are prepared to accept when deploying mission critical applications. Different user groups have different requirements – it is important that these are well understood and addressed by the operator's application strategy.

The paper emphasises the importance of the user experience. Users must absolutely trust their communications services, whether the network, the device or the application. Broadband technologies – the basis of the UK's Emergency Services Network (ESN) – will enable a wide array of new applications to greatly enhance the effectiveness, productivity and safety of public safety users and other critical organisations. However, the introduction and management of these new applications on to mission critical networks will require careful planning.

For users to gain trust and confidence in using mission critical applications on broadband networks, users first need to understand where they can expect the applications to be available. In the UK, the Emergency Services Mobile Communication Programme (ESMCP) has the 'ESN Assure' application that provides cumulative understanding of the broadband radio network coverage. This is an important step forward and helps the emergency services to measure and report on ESN coverage in their area, and report where improvements need to be made.

ESN Assure runs on a handheld ESN device and includes an app that monitors coverage while users are on the move, as well as offering a view of which areas are predicted to be covered. Extensive coverage testing is being conducted by the emergency services and ESMCP together, to ensure coverage issues are addressed and to build user confidence in the ESN coverage availability and performance.

To be truly mission critical, apps need to achieve end-to-end mission critical Quality of Service (QoS) levels in terms of priority, pre-emption, availability, security and resilience to ensure user trust. From secure hosting environments for the application servers, through the transport and cellular networks to the devices and their associated operating systems, each needs to be mission critical in its own right.

TCCA also highlights that to do their job effectively, first responders will typically require both mission critical and non-mission critical applications to be used on the same device. The white paper considers the use and potential misuse of device resources and how they are shared between the applications running on the device. As mission critical applications may depend upon services provided by third parties, the whole chain of device and application support must be carefully managed to avoid degraded operation.

Mobile application development moves very quickly compared to traditional government projects. Many applications provide new functionality every month, of which the users will want to take advantage. The validation and testing process should support this speed of development by, for example, having a lightweight process for minor updates of existing applications, or accepting validation or certification done by selected similar organisations.

Security and bug fix updates for the mobile operating systems (OS) are important and should be deployed without extra delay. Minor updates to mobile OS are also common, and major updates with large changes typically take place yearly. Validating applications for each user or agency separately would be cost prohibitive for many applications. Work under way by TCCA and the Global Certification Forum to establish common interoperability testing for Mission Critical Services (MCX) protocols will enable a vibrant competitive interoperable market, as has been achieved through TCCA's TETRA IOP process.

Although targeted primarily at the PPDR sector, the white paper will also be of interest to any organisation requiring or dealing with mission critical broadband applications. The full paper, 'Mission Critical Broadband Applications: A guide for deploying and developing mission critical applications using broadband technologies' can be read here. ■

TCCA
CRITICAL COMMUNICATIONS WORLD 2022
JOIN US IN VIENNA
SAVE THE DATE
21 – 23 JUNE 2022
MESSE WIEN EXHIBITION CONGRESS CENTER, AUSTRIA
SCAN THE QR CODE TO FIND OUT MORE
WWW.CRITICAL-COMMUNICATIONS-WORLD.COM/VIENNA
@CRITCOMMSSERIES
TCCA CRITICAL COMMUNICATIONS SERIES

NAS best practices

By Grant Caley, UK chief technologist, NetApp

In today's modern data centre, enterprise NAS plays an important role in not just providing highly scalable user file services, but also providing application file storage for a range of mission critical applications such as AI, VMware, Oracle, and SAP HANA. As a starting point, you should consider and ensure the following:

1) **Protocol:** Your NAS is the swiss army knife of file storage and should support as wide a set of protocols as possible. Essential are SMB (2, 2.1, 3, 3.11 (and legacy v1 to help with migrations)) and NFS (3, 4.1, pNFS). Also consider support for iSCSI, FC, FCoE, NVMe over Fabrics/RDMA and Object S3. Simultaneous file access, via both SMB and NFS, opens collaboration options and this is often needed in the Education and Engineering sectors.

2) **Performance:** As you look to deploy a NAS for not just file, but more importantly application usage, performance is a key factor. By default, today's NAS are usually flash based, and you have the option of SSD or low-latency NVMe disks. If you want to take application file performance to the next level, then look at NVMe End to End, this dramatically improves performance by optimising the protocol between NAS and server.

3) **Scale:** Whilst your NAS requirements may start small, it is worth considering your future expansion from day one. Having a NAS that provides a single OS, whatever the size of requirement, reduces management complexity and improves overall service management. Scale can be delivered in multiple ways:

a. Vertical scaling, which is where you can replace controllers, with larger versions, but keeping the underlying storage, as well as growing your storage capacity as you need to expand. You might need disk storage options such as NVMe, SSD, QLC or even still traditional HDD.

b. Choose an architecture that enables the clustering of controllers, such that you can expand by adding more controllers. Important here is the option to mix different controller types, different storage options and to be able to non-disruptively move workloads across cluster members.

c. If you require a scale-out filesystem, such as for HPC, EDA and other workloads, then ensure you choose a NAS that can deliver this potentially multi-Petabyte need, as well as still supporting your other workload types.

d. Being able to securely virtualise and multi-tenant your NAS enables secure scalability, this should also support RBAC, MFA etc.

4) **Cost:** When choosing a NAS, options such as deduplication, compression & dynamic thin provisioning should be starting stakes. But you can also enable tiering to S3 targeting either on-premises S3 or to any of the multiple public cloud S3 offerings. Tiering can reduce your on-premises storage capacity by often up to 80%. Another often overlooked factor for controlling costs, is through automation. Your NAS should be fully API driveable, integrate with whatever framework you want, whether that is via Ansible, Terraform or just an SDK.

5) **Protection:** Any NAS you deploy should offer High Availability protection, support redundant hardware, multipathing to shelves and disks and integrate features such as hardware backed write journaling.

- Enterprise NAS also needs to have at least zero performance, space efficient instant snapshots. These provide the 1st level of business continuity and should integrate into the likes of Oracle RMAN, SAP, Kubernetes and of course into user Windows desktops.

- Backups are the next requirement, these should be offsite and should either be a native NAS feature, for example to on-premises or cloud S3, or integrated via a backup tool such as with Rubrik & Veeam.

- Disaster Recovery is also essential with options to replicate either Asynchronously or Synchronously, such that you can select the service level you need to protect for. If you require zero data loss and near instant failover in the event of a site outage, then considering a metro clustering option is also essential.

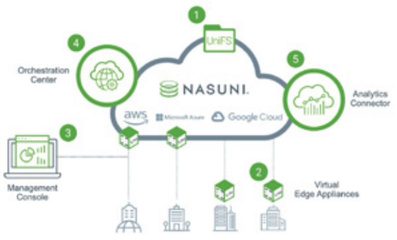
A final element to consider is whether the NAS can detect, protect, and alert to Ransomware attacks as well as offering immutability of files and importantly backups.

6) **Multi-Cloud:** If your NAS, with all its Enterprise features, were also available in AWS, Azure and GCP, then you also have options to replicate to the cloud, backup to the cloud and deploy your applications in the cloud, but with the same storage efficiencies, data protection, scale, and security, as they have on-premises.

7) **Management:** Finally, consider being able to manage your NAS across a hybrid multi-cloud environment, it should provide AI predictive risk analysis and recommendations, proactively, as well as offering integration into systems such as ServiceNow and other frameworks. You should also be able to deliver hybrid Multi-Cloud NAS provisioning, protection, replication and extending via a range of advanced data management options. ■

PRODUCTS

Nasuni delivers a file storage platform that leverages object storage delivering a simpler, lower cost, and more efficient SaaS solution for the enterprise, that scales easily to handle rapid unstructured data growth. Nasuni replaces on-premises file server, network attached storage (NAS), backup, and disaster recovery (DR) infrastructure with a cloud-native SaaS solution that saves money, scales infinitely, and is simple to manage. Better yet, it provides a file storage platform that allows companies to unify multiple sites worth of data. The combination of Nasuni with Azure, Amazon Web Services, or Google Cloud gives unlimited file server capacity on-demand, built-in backup, DR, and file sharing across any number of users and locations. "Whether Nasuni is deployed completely in the cloud, as a hybrid-cloud solution, or in a private cloud, an organisation's data is always protected and accessible with fast local performance," the company says. *nasuni.com*



The **TerraMaster F5-221** comes with an Intel Celeron J1800 processor (backed up by 2 to 4GB of RAM). This product is said to perform to a high standard with regards to file transfer and media benchmark tests. Its five trays are cooled by two 82mm fans. The fact users will unlikely need to fill all five at once, means the F5-221 is good for an upgrade at a later date. While TerraMaster's NAS software isn't as slick as Asus's or Synology's, it's quite well-designed, giving you easy access to the usual management tools and features, useful dashboards and an app store with a bewildering range of add-on apps. We did experience a few niggling setup issues, but assuming everything goes smoothly, this is a good NAS for big demands and small wallets. The F5-221 device relies on the following five data security layers: automatic scheduled backup, Btrfs file system and snapshot, RAID 1,5,6 array security, AES hardware folder encryption and network transport encryption, as well as cloud drive data backup. *terra-master.com*

The **QNAP TS-873A** 8-Bay Network Attached NAS Storage device features an AMD Ryzen V1000 series V1500B quad-core processor that delivers great system performance with up to quad-core / 8 threads and Turbo Core up to 2.2 GHz. It features two (2) 2.5GbE RJ45 ports and two (2) PCIe Gen 3 slots for you to flexibly deploy 5GbE/10GbE networks. Two (2) M.2 NVMe SSD slots (un-populated) for Qtier Technology and SSD Caching enable constant storage optimisation. The TS-873A supports QTS and QuTS hero, allowing users to flexibly switch operating system based on their requirements. This product also supports QuTS hero - QNAP's ZFS-based NAS operating system. Providing end-to-end data integrity, data reduction (inline data deduplication, compression and compaction), and much more, QuTS hero uses additional system resources to ensure an optimal environment for protecting business data. It's important to note that The TS-873A features two (2) PCIe Gen 3 x4 slots that allows for various expansion cards (sold separately, see accessories tab) for expanding application potential. *qnap.com*

This four-bay NAS is popular choice for businesses, not just home users. Powered by a quick quad-core Intel Celeron J4105 supported by up to 8GB of RAM, the AS5304T is supposed to be quick even when running over a standard gigabit ethernet network. It has space for four drives and supports a wealth of RAID configurations. There is also an HDMI port on the back allowing you to use it as a Linux desktop PC. It also comes with a hefty 92mm fan, which works with heatsinks on the major components to keep the heat under control. You can set up users and shared folders as you would on any other NAS, or set up iSCSI targets for virtualisation purposes. Asustor still provides tools for sync with OneDrive, Dropbox and Google Drive, or backing up Windows and macOS PCs. With the Brtfs file system, one can even use snapshots and the Snapshot Center app to safeguard the data on the NAS. *asustor.com*

Netgear says the **ReadyNAS 520 series** offers superior performance storage capabilities for up to 80 users, featuring 10Gigabit ethernet connectivity and superior streaming capabilities for multiple 1K or single 4K streams. It is available in four, six and eight bay configurations. It is an addition to the ReadyNAS family for small businesses needing to store, share and protect their growing company data. Campuses or universities need to protect their research data, regional branches need to gather and backup their local data and share them with headquarters. All ReadyNAS are built on the revolutionary ReadyNAS OS 6 operating system and next-gen BTRFS file system. A best-in-class 5 levels of data protection - X-RAIDTM, Unlimited Snapshots, Bit rot protection, real-time anti-virus and easy offsite replication work in concert to securely protect your data from common risks. Moreover, all ReadyNAS systems utilise proprietary ReadyCLOUD technology. No VPN setup, no port forwarding, no dynamic DNS required. Featuring an architecture powered by "blazing fast quad core hyper threaded Intel Xeon server processors along with DDR4 ECC memory", Netgear reckons "the RN520 is the no compromise, high performing data storage systems of choice for businesses that need the ultimate in capacity, performance and security". *netgear.com*

Please meet...

Steve Barber, CEO, Sepura and TCCA board member

Who was your hero when you were growing up?

Brian Clough, I really admired his straight talking and his ability to motivate and lead an average group of footballers, getting 110% out of them, making them believe in themselves. That is why I ended up supporting Nottingham Forest.

What was your big career break?

Having gone through an engineering apprenticeship at British Telecom in 1991 I was selected to take part in a new Management Cadetship Scheme, only 30 of us were selected out of more than 700 applicants. This gave me the confidence in my own abilities, as I was benchmarked against my peers, since then I have never looked back.

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

Transport Telematics – after leaving BT I moved into a fledgling industry providing real time location and information systems for buses, trams, light rail etc. At the time it was in its infancy but they were exciting times using new technologies like GPS, RF beacons and private mobile radio to deliver customer solutions. Nearly 30 years on and industry still uses GNSS and BT/WiFi for exactly the same purpose.

> **"While I can appreciate both, my main music era was 1975-1995 and more aligned to rock and post punk indie groups like the Psychedelic Furs, Faith no more, Sisters of Mercy, etc."**

What would you do with £1m?

Ideally I would build a triple size garage and fill it with vintage and new exotic British and Italian motorcycles. I have always been a keen biker, but my desire for the best bikes has always been limited by my bank balance and other commitments. The reality is that I would probably treat those closest to me.

If money was no object, where would you live?

I am very happy in the area I live now in the East Midlands, but I wouldn't mind a house by the sea down in Cornwall, it is a completely different pace of life. Having travelled a lot during my working life, usually to big cities, peace and quiet is very attractive.

What's the strangest question you've been asked?

Not sure anyone has asked me a question that I have found that strange, I seem to not be surprised by anything people say or do. If you expect the unexpected then nothing seems strange or should faze you.

In recent times I guess it would be from our current owners, who had just acquired Sepura in May 2017 and within one week, out of the blue, they just asked me whether I wanted to be CEO - as simple as that!

The Beatles or the Rolling Stones?

Neither for me. While I can appreciate both, my main music era was 1975-1995 and more aligned to rock and post punk indie groups like the Psychedelic Furs, Faith No More, Sisters of Mercy, etc I really am an old rocker at heart.

What is the most challenging aspect of your job?

There are many different challenges in my role, from managing upwards, managing different personalities or just being effective when spending time travelling. But I think there are two major challenges, the first is building the right team around you that can implement the strategic vision so that we grow the business, in parallel embracing new technologies and delivering organisational change. The second, as one of the new Board members elected in November 2021, is working within TCCA to ensure all members' views are represented as we deliver the Board strategy and promote the full breadth of critical communications solutions, whatever the chosen technology.

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

While there are many that I would like to dine with, there can only be one person, Brian Clough. He would be down to earth, humorous and unpredictable, there would not be a dull moment.

I would think though that we would not be going to a Michelin star restaurant, more likely he would settle for fish and chips wrapped in paper, sitting on a seafront bench.

I am 3DCIM
Say hello to two industry leading technologies available as one intuitive solution.
Wave goodbye to outdated legacy DCIM.
Ekko Sense
assetspire
3DCIM
Real-time optimization across your entire M&E infrastructure
Intuitive life cycle asset management for full data center management
DCIM
Ekko Sense
assetspire
ekkosense.com/ekkosoft-critical/3dcim
assetspire.co.uk/products/3dcim