OCTOBER 2020
networkingplus.co.uk

NETWORKING+

The power of IP networks

Here's what the owners of the buildings should know

Mike Hook, LMG, *p7*

Cloud-driven networks

About the fuel powering the 'new normal'

Dahwood Ahmed, Extreme Networks, *p13*

Questions & answers...

Networking+ sits down with the Colt CCO

Paula Cogan, Colt, *p16*

BT and Toshiba launch 'unhackable' network

BT and Toshiba have launched the first quantum-secure industrial network to be installed in the UK.

The 6km network in Bristol uses standard Openreach fibre to connect sites belonging to the National Composites Centre (NCC) and the Centre for Modelling & Simulation (CFMS) across the city.

The project was chosen because of the sensitive nature of the data sent between the two organisations. Both firms have interests in the aerospace, energy and automotive industries and deemed standard networking and security technologies to be insufficiently secure. Instead, data was stored and transported on physical storage – a much more inefficient, time-consuming and inherently insecure method than what quantum networking promises to deliver.

Whereas classical computing architectures store information in binary (one or zero) bits, quantum computing uses subatomic particles' ability to exist in multiple states at the same time. This means quantum computers can store significantly more information and compute issues much more quickly.

Furthermore, quantum computing has huge implications for the financial, military and healthcare sectors among others as it can expediate research projects. While some have concerns that this increase in computing power could render most encryption measures obsolete, it also opens the door for even more powerful security measures through quantum cryptography.

This network is protected by quantum key distribution (QKD), an apparently 'unhackable' technique for sharing encryption keys between locations using a single stream of photons. Multiplexing compatibility allows both data and keys to be transmitted on the same fibre, essentially doubling network capacity, and allows for the distribution of 1000s keys per second.

BT and Toshiba say the new network demonstrates a tangible benefit to industry and the viability of QKD to transmit sensitive data across fibre. "For the deployment with NCC, we have tailored our QKD system to operate with standard Openreach optical fibre solutions," said Andrew Shields, head of quantum technology at Toshiba Europe. "We were delighted to see that Toshiba's QKD technology works well in Openreach's multiplexed environment, which can serve as a model for deployments elsewhere. We see most interest from the government, finance, telecom and healthcare sectors."

The UK government has expressed a desire to be at the forefront of the field, believing it can play a vital role in the connected economy and accelerate Industrial Internet of things (IIoT) deployments. A National Quantum Computing Centre (NQCC) is expected to open in 2022 as part of the £1 billion National Quantum Technologies Programme.

BT has alrwady constructed a commercial-grade test network link that spans 125km between its Adastral Park R&D facility in Suffolk and the University of Cambridge, linking to the wider UK Quantum Network (UKQN) – a collaboration between industry and academia.

continued on page 2

IN DEPTH:
Connectivity in old buildings
P8-11

BT and Toshiba team up for quantum-secure network launch

Continued from page 1

Imran Shaheem, a consultant at Cyberis, says the partnership between BT and Toshiba "is a massive first step for the UK" as the nation moves towards a quantum safe future.

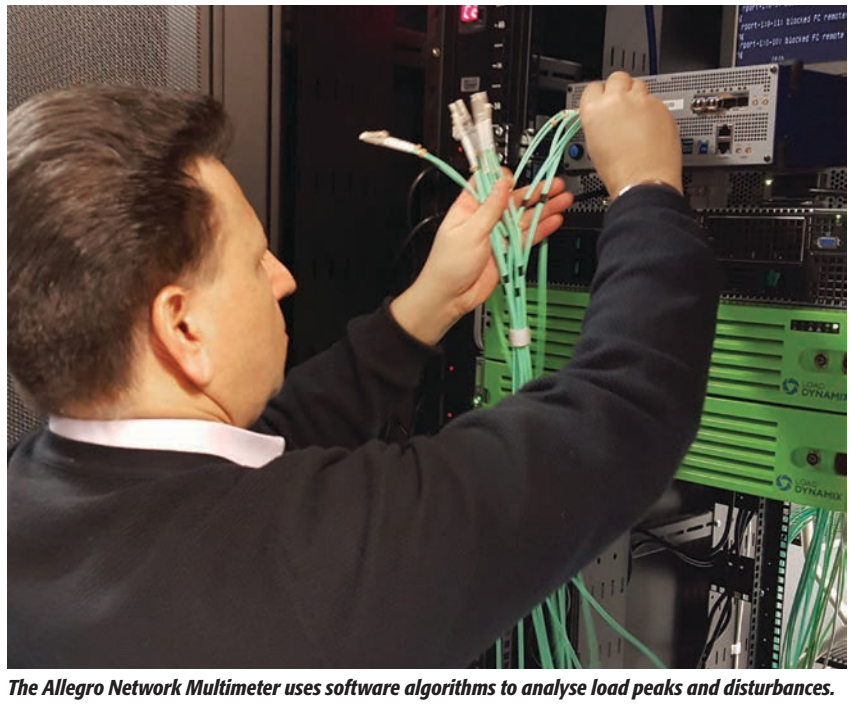
"Toshiba continues to be a global leader in the quantum cryptography field and as lead of the AQuaSeC project they're perfectly positioned to facilitate such a network, with BT's experience alongside their extensive fibre optic networks making them an ideal partner," he told Networking+. "This is an important milestone in securing our economy and its sensitive data as the nation, alongside the world, becomes more interconnected and continues to adopt smart technologies."

Shaheem added that "we can expect to see more developments like this" as the UK prepares for a post-quantum future. "The ability to utilise existing infrastructure in terms of currently laid fibre optic cabling significantly reduces what was traditionally a large obstacle in adoption, that being the requirement for dedicated infrastructure," he continued. "With continuing breakthroughs happening in the field of quantum cryptography, the technologies that are starting to take their first steps to safeguard industry may one day contribute to protecting all of us digitally at home. Watch this space." ■

Network analysis expert expands reseller network in the UK

Allegro Packets GmbH, a specialist in and provider of network analysis and troubleshooting appliances, has extended its UK partner network with the appointment of GCH Test and Computer Services.

The former's network diagnostic tools include the Allegro 200, 500, 1000, 3000, 5500 and from this year, the latest Allegro x300 Series. These Allegro Network Multimeters are available for mobile or stationary use with 1 to 100 Gigabit analysis rate. Allegro Packets' troubleshooting tools are deployed by network administrators around the world to analyse network traffic in real-time and to store previous network events to allow high granularity, detailed analysis. As a result, network problems, performance bottlenecks and packet losses can be quickly identified. The Allegro Network Multimeter uses software algorithms to analyse load peaks and disturbances. At the same time, it acts as a network monitoring tool to ensure high network quality.



The Allegro Network Multimeter uses software algorithms to analyse load peaks and disturbances. At the same time, it acts as a network monitoring tool to ensure high network quality

"We are delighted to partner with Allegro Packets," said Laky Hothi, sales and marketing director of GCH. "Their range of network appliances are easy to use, extremely powerful and cost-efficient. They meet the needs of small organisations up to the largest multinational enterprises, Telcos and ISPs. The combination of their leading-edge solutions and our market and technology experience will help all our clients and prospects maintain trouble-free communications during this challenging time as organisations increasingly adopt work-from- home policies."

Klaus Degner, co-founder and managing director of Allegro Packets added: "We are really pleased to enter into this relationship with GCH, and are confident that their many years of experience and success will be a great benefit to their expanding customer base and prove to be a mutually beneficial future for our two companies. I have no doubt that the combination of their excellent UK reputation and our state-of-the-art appliances and support will be a winner." ■

Slough authorities to decide on Zurich data centre plans

Local authorities are set to decide whether to approve Zurich Assurance's bid to build a one million sq ft data centre in Slough.

The firm has applied to build the facility on the site of the Langley Business Centre, approximately five miles east of the Slough Trading Estate, the UK's data centre capital. This proposal would see the demolition of the business centre next to Langley Station, and build a mixed-use development which would include some 60 homes, shops and pubs, and could include an energy centre and district heating system alongside the 93,000 sq m (1m sq ft) data centre.

It is not clear at this stage whether the planned data centre is for Zurich's use, but the application talks of "market demand" which suggests a commercial use for the data centre space. Officers of the Slough planning committee have recommended the application be approved, saying its proximity to the existing Trading Estate hub means it would "take advantage of the site's proximity to digital infrastructure in form of high-speed cable that links London, Slough and Berkshire, the west of England and Wales," according to local media.

The application was filed in December 2019 and includes a power substation for the data centre. Premises, both houses and shops, would be on a strip of land along Station Road, while the data centre would take the vast majority (up to 90%) of the land, away from the road. ■

It is not clear at this stage whether the planned data centre is for Zurich's use, but the application talks of "market demand" which suggests a commercial use for the data centre space

An edge solution for visual inspection and observation

Two tech specialists have forged a partnership to offer an edge solution for automating visual inspection and observation.

The new end-to-end offering will merge the edge computing technology of Advantech with the BrainMatter platform for intelligent automation based on AI, which allows the former to execute automated tasks on-the-edge of innovative IoT devices ideal for industrial environments.

BrainCreators is a Netherlands-based firm that specialises in turning artificial intelligence (AI) technology into accessible software. Advantech is a computer manufacturing player also in the industrial IoT space, headquartered in Taipei, Taiwan.

Furthermore, the companies said this collaboration allows organisations to significantly increase their margins, improve customer experience and optimise operational efficiency. The technology can be employed in a range of instances such as for the automatic inspection of products and objects, the anonymisation of video images for pattern recognition and the observation of materials, terrains and buildings.

This collaboration allows edge solution ready packages to be used in the cloud, on-premise and on the edge. The packages can be created by the BrainMatter platform to the platform based on examples. Through this transfer of knowledge, the platform can learn skills and perform reality checks against a provided standard or objective.

"Our partnership with BrainCreators represents an important strategic partnership for Advantech," said Jash Bansidhar, managing director of Advantech Europe. "The partnership allows us to better roll out our AI solutions in the Netherlands and beyond. As Edge AI becomes increasingly important, it is vital that we work with partners who are able to combine domain knowledge with a practical mindset to deliver successful projects. We are convinced that BrainCreators can help customers get the best out of Advantech's NVIDIA technologies."

Glenn Brouwer, co-founder and CRO of BrainCreators, added: "As a company, we are continuously improving BrainMatter. Advantech has an enormous amount of knowledge and technology in the field of edge computing. By combining their edge technology and knowledge with BrainMatter, we have developed together an end-to-end solution that enables visual inspection and observation in almost real-time." ■

EDITORIAL:

Editor: Robert Shepherd
roberts@kadiumpublishing.com

Designer: Sean McNamara
seanm@kadiumpublishing.com

Contributors: Gerry Moynihan, Mike Hook, Dahwood Ahmed, Paula Cogan, Hugo McGuire

ADVERTISING & PRODUCTION:

Sales: Kathy Moynihan
kathym@kadiumpublishing.com

Production: Suzanne Thomas
suzannet@kadiumpublishing.com

Publishing director: Kathy Moynihan
kathym@kadiumpublishing.com

Networking+ is published monthly by:
Kadium Ltd, Unit 2, 1 Annett Road, Walton-on-Thames, Surrey, KT12 2JR
Tel: +44 (0) 1932 886 537

ISSN: 2052–7373

HMRC warns universities about cyber scams

The HMRC has urged institutions through Universities UK to warn new students of cyber scams as they are more 'vulnerable' due to their limited experience of the tax system.

In August, the government department received reports of more than 74,800 scam emails, text messages and phone calls. Nearly 41,300 of these specifically offered bogus tax rebates.

"We are concerned that the new academic year and remote working in academia will see another wave of email and text tax scams, targeting a new and potentially vulnerable university intake," said Mike Fell, head of cyber operations, in a letter to universities. "These scams often offer fake tax refunds or help with claiming Covid-related financial help," said Mike Fell, head of cyber operations, in a letter to universities. We also see frauds offering spurious support with reclaiming council tax, purporting to be from TV Licensing, the DVLA or 'GovUK'."

Thousands of the scams were targeted at students and the criminals had obtained their personal university email addresses by unlawful means, an official statement said.

Students who provide personal details in response can end up inadvertently giving access to important accounts, like email or online banking, leaving scammers free to commit fraud and steal their money.

"We are concerned that remote working because of Covid-19 could lead to more tax scams targeting a new and potentially vulnerable university intake," added Jesse Norman, financial secretary to the treasury. "HMRC are doing everything they can to clamp down on cyber fraud, but students also need to be vigilant. We would urge university principals to take a lead in helping to protect their students from these cyber criminals by raising awareness of what to look out for."

Alistair Jarvis, chief executive of Universities UK, said: "The message to students is to remain vigilant and question anything that seems unusual. Any student who fears their account may have been misused is encouraged to speak to either university support services, their bank, or to the police via Action Fraud."

Criminals also use phone scams to threaten taxpayers into handing over cash. Some 651,600 scams have been referred to HMRC since August last year. Of those, more than 215,660 were voice or telephone scams, the statement further said.

Hacking universities and students data has been a common occurrence of late, as students get to grips with working and studying from home during the Covid-19 pandemic.

University of York, Oxford Brookes University, Loughborough University and University of Leeds are just a few institutions that were targeted during the summer months. Cyber security experts are working with schools, colleges and universities across the country to help them keep their data secure. ■

Charity deploys 8x8 platform

UK charity Age Scotland has deployed the 8x8 Open Communications Platform to help them work remotely during the pandemic while continuing to provide vulnerable older people with support services.

The Covid-19 pandemic has led to Age Scotland experiencing a surge in call volumes, increasing by 500%. As a result, the charity needed to more than double its contact centre team. It also needed to fast-track the deployment of a technology solution that would enable a mobilised workforce and allow them to communicate and collaborate with the community, and effectively manage high call volumes through improved queue management and routing. Working with its telecom partner, Frontier Group, Age Scotland selected 8x8's integrated voice, chat, video conferencing, and contact centre solution, which was deployed in five days.

"8x8 surprised us with extra functionality that we now realise we need," said Laura Stenhouse, telephony manager at Age Scotland. "8x8 Meet has added a whole new dimension to our teams, community groups and veterans' projects. We can host friendship circles online and enable people to interact via video. Platform features such as call recording and analytics have helped us gain valuable customer insights and identify trends to shape policies and give older people a voice in the community. The 8x8 Open Communications Platform is incredibly flexible and a step closer to providing the best possible experience for both our employees and older people."

The Charity Digital Skills report showed that now two thirds (66%) of charities are delivering all work remotely. ■

Working with its telecom partner, Frontier Group, Age Scotland selected 8x8's integrated voice, chat, video conferencing, and contact centre solution, which was deployed in five days

FROM THE COVER

Making the case for an RMM

Remote monitoring and management software is a core tool in the IT management technology stack designed to monitor the health and performance of devices and provide tools for managing those devices effectively. RMMs are packed with functionality and overlap with many other technologies such as mobile device management (MDM), unified endpoint management (UEM), and remote control tools. Because of this, contextualizing everything an RMM can do – and providing a big picture of your ROI can be difficult.

With employees wasting 8+ hours per month on IT issues, IT efficiency has a direct impact on businesses. For SMBs, it can make or break their success. Find out how remote monitoring and management software helps IT leaders monitor the health of devices and drive efficiency through remote tools and automation.

Improve end-user productivity

Employees, on average, waste 22 minutes per day on IT issues – with one-third spending at least 8 hours per month on IT issues outside their normal duties. An RMM allows you to proactively identify issues and – in many cases – remediate them before the end-user is impacted, leading to 20 – 30% reduction in tickets and a significant boost to end-user productivity.

Server and network outages impact entire organizations' productivity levels, costing business on average $427 per minute. With proactive monitoring, IT leaders can identify warning signs of server health or network instability, quickly remediate or avoid issues, and reduce incidents of unplanned downtime by up to 80%.

Make technicians more efficient

On average, ticket remediation work times range from 12–20 minutes and cost $15.56 per ticket. With service desks on average receiving 429 tickets per month, IT leaders need to drive technician efficiency to keep costs in check. Facing ongoing pressure to support more endpoints per technician, IT leaders can turn to an RMM to increase capacity. In addition to reducing the overall number of tickets produced by end-users, RMMs significantly reduce the time it takes to remediate issues, from 50% - 70% through automation, access to critical device data, data-rich tickets, and hands-on tools built to solve IT challenges.

Improve security

Endpoint security should be a priority issue for all business. A breach costs, on average, $3.92 million. Even with businesses spending tens to hundreds of hours per week on managing the vulnerability response process, breaches happen regularly. While OS patching is possibly the most effective form of device hardening, 57% of data breaches could have been avoided if patches had been installed on time.

Patch management is a cumbersome process if its not centralized and automated due to a lack of transparency and end-user interference. Automated patch management, as part of a remote monitoring and management tool, reduces the time it takes to patch endpoints by more than 90%. With an RMM, Windows patching has been shown to decrease from 90 days to just 18 days.

Crossword gains acceptance to G-Cloud

Crossword Cybersecurity has been accepted onto the UK Government G-Cloud framework version 12 in the 'cloud software' and 'cloud support' categories.The framework enables public sector organisations to procure Crossword's Rizikon Assurance and Consulting cyber-risk management tools via the digital marketplace run by Crown Commercial Services. "Our Rizikon Assurance cloud-based service is already used by a number of organisations and the digital marketplace will make it even easier for others that want to mitigate third party risks in areas such as cybersecurity, GDPR and diversity, to get up and running," said Sean Arrowsmith, the group sales director at Crossword.

TeleData brings in diverse fibre routes

Manchester data centre operator TeleData is working with Zayo to bring diverse fibre routes to its Manchester facility. The latter will provide resilient high capacity network options ranging from 1 Gbps to 10Gbps wavelengths, to dedicated dark fibre circuits. Zayo's routes into TeleData's facility will be completely independent from other fibre providers' routes and will also widen the availability of diverse links to other connectivity hotspots, such as major national data centres and various connectivity-heavy technical and commercial hubs. Services are expected to be live in Q3. The news of additional carrier diversity comes as TeleData announced its £2m data centre facility expansion in September.

Tech boss makes tracing app warning

The boss of a British tech company has warned the government of potential serious flaws in the security of personal information and data used in the new contact tracing app technology, announced by health secretary Matt Hancock. VST Enterprises CEO Louis-James Davis said the scanning technology's reliance and use of QR codes exposes it to "attagging" or cloning. This is where a 'genuine QR code' is replaced by a cloned one, which redirects the user to a similar website where personal data can be intercepted. "When you are dealing with the public's personal information and private data, security is of paramount importance and crucial to public confidence," Davis said.

Ivanti swoops for MobileIron and Pulse Secure

Ivanti has entered into a pair of agreements to acquire MobileIron and Pulse Secure as part of an effort to create a zero-trust platform that can be delivered as a service. Acquired for $872m (£665m) MobileIron gives Ivanti access to a set of tools for securing mobile computing applications deployed on devices running Apple iOS or Google Android. Pulse Secure's VPN will allow workers to securely connect to corporate networks from home. The financial details for the latter deal have yet to be disclosed.

Ribbon launches robocall-fighting managed service

Ribbon Communications, real-time software and packet and optical transportation solution provider, has announced two new managed as-a-service features to its Ribbon Call Trust portfolio: STIR/SHAKEN-as-a-Service and Reputation Scoring. These services will help reduce robocalls and phone-based fraud attacks. STIR/SHAKEN is an acronym that stands for secure telephony identity revisited (STIR) and signature-based handling of asserted information using toKENs (SHAKEN), a caller authentication, signing and verification process required in the US and Canada to prevent call spoofing. The new service aims to help service providers comply with its namesake regulations without the cost of implementing it in their own networks. The reputation screening offering improves upon STIR/SHAKEN-as-a-service with real-time, multidimensional scoring of calls to help mitigate fraud and nuisance calls.

AEWIN collaborates with Altran to enable enterprise uCPE solution for SD-WAN

Taiwanese firm AEWIN, a supplier of networking equipment for enterprises, is using Altran's SD-WAN uCPE Operating system framework to enable cloud/virtualisation. Through this collaboration, Altran's SD-WAN uCPE operating system (OS) leverages AEWIN's uCPE Whitebox Hardware solution, a general-purpose platform that integrates computing, storage and networking on an off-the-shelf server to provide various network services as virtual functions to any site on the network. Altran's uCPE solution is pre-integrated with vRouter & Firewall virtual network functions (VNFs) and Altran Orchestrator, as well as a cloud-native OS that supports containerized, low-resource footprint workloads for cost-effective uCPE deployments. "AEWIN's collaboration with Altran enables us to build uCPE for enterprises to share resources, reduce costs, innovate more quickly and automate operations," said Charles Lin, chief executive officer at AEWIN. "As both the SD-WAN and uCPE markets continue to strengthen, this solution will enable savvy enterprises to integrate virtualization and establish market leadership more quickly and cost effectively."

Firm delivers new data centre

Secure I.T. Environments, a design and build company for modular, containerised and micro data centres, has completed a new data centre for Opus Trust Communications in Leicestershire, the omnichannel communication specialist working in heavily regulated industries. The new modular data centre, which further increases the security rating of Opus Trust's operations, began construction in April 2020, during the UK Covid-19 pandemic lockdown. The nature of Opus' operations gave the project key worker status, and despite the many challenges created in the supply chain, logistics and onsite management of the project, it was fully delivered in just 15 weeks. Opus operates in sectors such as telecoms, utilities, financial services providers, as well as the NHS.

'Cloud services increase PKI adoption'

Organisations are rapidly increasing the size of their data protection infrastructure, 'causing a dramatic rise' in the adoption of public key infrastructure (PKI). Research by Entrust shows that PKI is used in almost all IT infrastructure providing security for certain digital initiatives. The main growth in uses are authentication, cloud and IoT. As companies become more dependent on digital information, they face more threatening cyber-attacks, calling for higher security. IoT is the fastest factor in the growth of PKI usage, up 26% over the past five years to 47% in 2020 with cloud services as a second highest driver, according to 44% of respondents.

Word on the web...

Sanjeev Verma, managing director of Squire Technologies calls for clarity and leadership re 5G

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

ARE YOU READY
FOR THIS MUCH POWER?

DATA CENTERS

HEALTHCARE FACILITIES

INDUSTRY

The KOHLER 4 MW industrial generator
featuring 4 500 kVA at 50 Hz
and 4 000 kWe at 60 Hz.

kdseries.com

100 YEARS OF POWER KOHLER EST. 1920

KOHLER SDMO

Securing the healthcare sector

Experts discuss how Covid-19 has impacted the healthcare sector and what needs to be prioritised going forward

Now, in 2020, technology and healthcare become increasingly intertwined every day. The ongoing pandemic has highlighted the real need to embrace data driven technologies and even accelerated the rate at which digitisation in the healthcare sector is adopted.

"Much has been said about the need for public sector organisations – particularly those within healthcare – to adopt progressive technologies to enhance citizen service", says Cleveland Henry, director of Cloud at UKCloud.

He states: "Prior to Covid-19, there was movement towards it with the NHS publishing its long-term strategy and introducing NHSX in 2019, but the pandemic has undoubtedly accelerated the need to adopt digital strategies throughout healthcare and we are already witnessing the positive effect. From streamlined patient care to remote GP consultations, technology has been at the forefront of the response and cloud technology has been at the centre of it all.

"As we move forward, cloud technology will become more entwined with our healthcare. Whether it's front-line services or allowing support staff to work from home, the cloud will play some role – it is the enabler. Therefore, there needs to be more education to lift the myths that still exist around its use.

"Firstly, the 'perfect setup' is incredibly difficult to find and those that wait for it will be waiting a while. There's no one-size-fits-all setup and each workload may be suited to a different type of cloud. As such, a multi-cloud approach is ideal for healthcare organisations. Providing the benefits of public and private cloud deployments, it enables organisations to host workloads depending on what is truly most important and the appropriate data classification requirements.

"Secondly, the concern that the cloud is less secure than on-premise infrastructure. Data is a national asset and healthcare organisations possess a lot of it, but when engaged in the correct way, the cloud offers so much protection. Cloud environments are built with security at their core, and that means they're always running and – vitally – scalable. Moreover, the apprehensions around vendor lock-in, solution incompatibility and working with a sole partner can all be addressed through the adopting a multi-cloud approach."

"Healthcare systems everywhere are facing an increasingly demanding and complex patient population with a diminishing healthcare workforce that can barely keep up. Add in the new pressure of a global pandemic, and technology-based solutions become a point of focus,"

Joost Bruggeman MD, PhD, co-founder and CEO of Siilo notes. "Healthcare professionals need secure ways to flexibly communicate with each other in real time. The advantages of messenger communication are widely apparent both personally and in the workplace, but most commercial solutions are not designed for the data security requirements in healthcare. A survey by the German Data Protection Institute has shown that over half (54%) of all medical professionals are using insecure messenger applications such as WhatsApp for work. Sensitive patient information, as well as photos and videos, are stored on unprotected commercial servers which is not in patients' best interests."

Bruggeman further argues, "European governments are seeking to regulate messenger communication services. In Germany, for example, data protection authorities have defined the technical requirements for messenger services in the healthcare sector in a November 2019 whitepaper. Such requirements include anonymity tools, PIN code protection, and isolated data storage on devices.

"Establishing clear recommendations and criteria is only the first step in keeping patients safe. Officials are still learning how software is being used in practice, and there are risks to setting strict guidelines. Striking the balance between keeping patient data safe and empowering practitioners will take time. Shaping technological solutions and security standards for the future of healthcare is a complex and ongoing conversation but a necessary one as we face ongoing healthcare crises."

"Had this pandemic happened 50-years-ago, it would have been a very different story. Technology's transformed our ability to respond to a crisis," Chris Boyd, lead malware intelligence analyst at Malwarebytes stated.

He continued: "Now, more than ever, data is power – and money. Facial recognition technology, DNA testing kits, period tracking apps: the value of health data is matchless. Biometrics in business has almost become mainstream; banks use voice recognition on phone calls; Disney uses your fingerprints to grant access to its theme parks. In this pandemic, some organisations and governments are harnessing the power of biodata to help curb the spread of Covid-19, such as contact-tracing apps.

"But, the commercialisation of healthcare data is like walking a tightrope. In the future, where do we draw the line between privacy, commerce, and safety? Especially as biometrics are big business, and third-party contracts generate significant profits?

"The issue of privacy cannot be overstated – think of the damage done if data ends up in the wrong hands. Just this month, Interserve, which helped build Birmingham's NHS Nightingale hospital, and Bam Construct, which delivered the Yorkshire and the Humber's, reported cyber-attacks. Large scale ransomware on hospitals and businesses that hold sensitive bio-data is not such a far stretch.

"The most worrying thing about this sensitive data being breached? Once it's compromised, there's no going back. For prevention over cure, businesses, governments, and citizens alike must treat their data like the vital asset it is."

There are many moving parts to ensuring the healthcare sector undergoes the digital transformation it needs, and many things to be considered – from secure methods of communication and working from home on the cloud, to assessing the dangers of commercialising health data. The pandemic has been a catalyst for the industry's digitisation, however, we must not get ahead of ourselves. Going forward, it's evident that security must be a priority at every turn.

Unleashing the full power of IP networks

Mike Hook, executive director, LMG

As we have witnessed the rise of the IoT and the increased digitisation of the built environment, building owners and managers have come to recognise the primacy of the IP network rather than any one individual system. Indeed, the IP network is now firmly established as the central plank of the future of the 'smart building'.

This is down to the fact that the IP network is the critical piece of the puzzle that brings all of the various building support systems onto a common platform – eradicating technology siloes and unlocking a far more detailed and sophisticated data-centric view of buildings. That data is the vital fuel you need to deliver operational efficiencies, increase sustainability, maximise health and well-being, and enhance security in buildings. Without this data, and the IP network that delivers it, buildings will never be truly smart.

However, while it is welcome that the value of IP networks is being recognised, there remains an issue that is holding back building owners from realising the full potential of the IP-based approach. All too often the deployment models for building technology – even for IP-based systems – are firmly stuck in the past.

What do I mean by stuck in the past? I mean that the delivery of the networks, and the systems based on them, remains incredibly siloed.

In the vast majority of cases virtually every aspect of the network is managed by separate specialist contractors. So, the initial cabling install will have a dedicated contractor, whereas the ongoing management will most likely be handled by a different firm. Each of the security, AV and other systems that rely on the platform will all be installed, and potentially managed, by another raft of separate companies. There may even be multiple layers of project managers and consultants involved attempting to manage this complex arrangement.

This model cannot possibly be sustainable. When IP networks promise to remove technology siloes the deployment and management model cannot continue to be so fragmented.

If we are to truly transform the built environment through technology, boost occupant satisfaction and maximise property values then we need to reduce this complexity.

There seems to be an obvious answer to this challenge – if IP networks support standardisation and interoperability, then surely the technology supplier should be able to deliver on all of the aspects of the platform? Would it not make sense for there to be a converged approach to the network, devices and services – from communications and security to AV, digital signage and even operational technology systems – for a building?

This converged approach has huge potential to simplify processes, ensure interoperability and functionality, and increase the speed of deployment. Rather than the scattered, inefficient deployment models that are typical, a converged technology deployment approach can deliver efficiency and cost benefits throughout the whole lifecycle of the building.

For example, during construction and fit out, a 'master systems integrator' should take on the commercial risk of delivering full interoperability, security and managing programme clashes/overruns. Having this central supplier also gives main contractors one point of accountability – de-risking projects by keeping sites safe, secure and running efficiently.

Similarly, once the building is occupied, having a truly converged IP backbone to the building doesn't just greatly increase process efficiency, but it gives access to a far richer pool of data than would be otherwise possible. This allows cross-referenced insights from multiple sources that empowers predictive maintenance, optimised use of space and resources, and hyper-personalised services. Indeed, with the right partner on board, building owners can create a host of tailored IoT-enabled services to boost occupant satisfaction and maximise property values.

This is just a tiny snapshot of the sorts of benefits a converged approach can deliver. Although it may appear to be a small change to the current state of affairs, it really can have an outsized effect on the success of any smart building project.

If we are to make the full potential of IP networks a reality then more intelligent and joined-up tech infrastructure is essential, not a nice to have. Rather than the headache of dealing with and synchronising work across multiple suppliers at every stage of the deployment, the converged approach gives building owners the chance to go from blueprint to operation, and beyond, with one partner.

And this is to say nothing of the additional challenges that COVID-19 is presenting to building owners. Rather than limit the reliance on IP-enabled buildings, the pandemic has supported the business case for more smart buildings systems. Having total control and flexibility in how a building is managed and operated is likely to be more important than ever before.

Of course, the transition to a truly converged operational model isn't going to happen overnight. There is a huge amount of work to educate the industry on the advantages of this approach, engineers need training to be able to handle all of the different technologies involved competently, and 'end users' need to have the trust in this model that they really will see the benefits.

However, I believe this absolutely has to be the future of the industry. Without the full convergence of building management and IT systems, it will not be possible to deliver the reduced operating costs, sustainability benefits, and occupant experiences that smart buildings promise.

Connectivity in old buildings

Many period buildings were not designed for the offices that now sit in them. Robert Shepherd finds out how new comms equipment navigates old brickwork

Internet connectivity problems are common in old houses. After all, the likes of John Nash, Decimus Burton and architects who plied their trade in the last century didn't have internet connectivity in mind when they were commissioned to design property.

However, many businesses in the UK face this challenge, too. Think about it: lots of companies now operate out of – well, they did before the Covid-19 pandemic – Georgian townhouses that ordinary folk can no longer afford to live in.

For context on what "old" means, all buildings erected before 1700 that 'contain a significant proportion of their original fabric' is listed under the listed building status in the UK.

So, you've moved your offices to a beautiful period building in Bath or a Georgian townhouse in London's Mayfair. However, its unforgiving design is not conducive to 2020 network infrastructure and your internet signal is for want of a better word, poor. Yet you have committed to an eye-watering rental agreement. Now what?

Glyn Brice - principal systems engineer at Extreme Networks, says that due to the way that Georgian townhouses are built - with thick walls filled with rubble - they can be more challenging to deal with. "This is why we look to the flooring area," Brice says. "With floors in Georgian townhouses often being made of oak, our teams can be imaginative and flip the entire installation on its head. This means that rather than running cabling through walls, we can go through the floor instead. As a team, we also need to be somewhat flexible and quick to problem solve when kitting out any older or listed buildings in case any other design challenges arise along the way."

Alex Shuker, CTO at DrayTek, a manufacturer of broadband CPE, says the installation of traditional access points (where each access point is hard wired back to the network switch) through a property is the optimum configuration for a wireless deployments, but this is an expensive choice if it involves building work to run the network trunking and install the wall plate

Don’t think...

...how much you want to reduce your environmental footprint and total operating costs with one standalone solution.

Act!

Get the highest active power needed for your IT applications, with sustainability built in.

Liebert® EXS 10-80 kVA UPS:

- Reduced TCO
- Compact footprint
- Installation flexibility
- High efficiency operation

Vertiv.com/LiebertEXS_N

VERTIV™

and data point. What if the property is listed?

"For listed building, planning considerations may be another reason this is not an option," he adds. "A viable alternative choice is to install a mesh based wireless solution where each access point communicates to the next hop over wireless and only the root node is connected to ethernet cabling."

However, each listed property may have unique restrictions, prohibiting engineers from carrying out the desired work. Brice says that if this is the case, "you can get creative" – this is where looking at other specific technology solutions comes in. "For example, we can explore using a wireless mesh device which only requires a three-pin socket," he adds. "This technology offers comprehensive mesh networking features to create secure, flexible and scalable networks without the need for any cabling. However, probably the biggest benefit regarding the use of meshing technologies within listed buildings is the ability to provide services without needing to interfere with the fabric of the building. This reduces cost and speed of deployment, whilst maintaining the original fabric of the building."

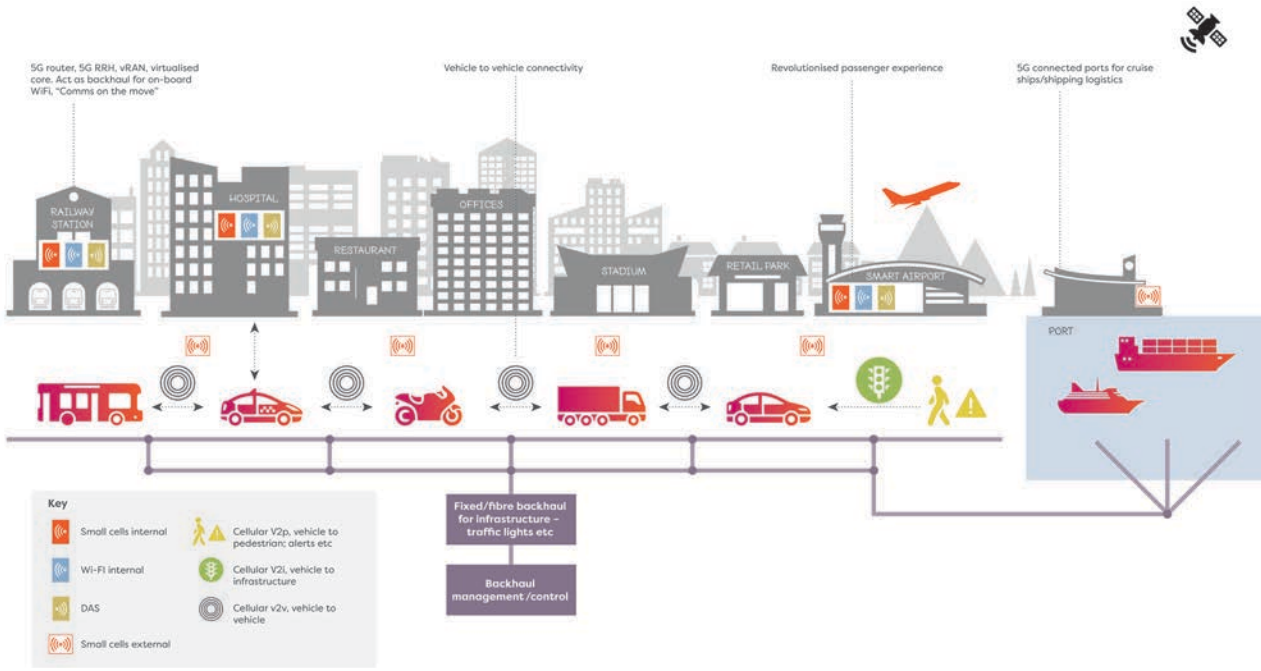
Being creative is one way of achieving the desired goal, but there are other ways, too.

Shuker says "a really convenient option with this are small form factor access points that have an integrated plug socket and plug directly into a wall electrical socket". He cites an example – the DrayTek VigorAP 802, which can act as a mesh node to a mesh root, such as the wall-mount DrayTek VigorAP 903 or ceiling-mount VigorAP 1000C.

Of course, unless the premises are part of a uniform terrace, no building is exactly the same as the next, even if they were built at the same time. Lewis White, managing director infrastructure and networking, CommScope says each will come with its own connectivity challenges - whether it's the size, density and volume of people and traffic, 'green design' or even buildings with lots of glass windows blocking radio signals. "So, it's not necessarily a question of old and new and more whether the building is set up to deliver for the expectations of those using it," he says. "Many office-spaces aren't properly setup to deliver wireless mobile connectivity, for example. Indeed, CommScope research found that nearly half of UK office workers admitted having to step out of the building to make a phone call or access 4G data services on their mobile device due to a lack of coverage indoors."

Then you have to factor in cost. Basic economics dictate that in most cases, the bigger the job, the bigger the cost. I ask how that works with old and sometimes crumbling buildings.

White says all buildings are assessed on a case-by-case basis so it's hard to provide a specific answer to this.



Each and every building will come with its own connectivity challenges - whether it's the size, density and volume of people and traffic, 'green design' or even buildings with lots of glass windows blocking radio signals

"What we can say is that we rely on our partners – many of which have been installing telecoms infrastructure into these types of buildings for many years – to advise as to the right infrastructure," he continues. "Of course, with a wireless deployment, there may be less of a requirement for expansive cabling with more connectivity provided wirelessly. This will likely have a positive effect on the impact of IT infrastructure in older properties."

Regardless of building style and size, solid walls inhibit Wi-Fi signals so can cause an issue with how much coverage a single Wi-Fi router or access point can provide. Shuker adds that the latest wireless standards often rely on the 5Ghz frequency range which although it offers higher network speeds does have lower penetration capabilities compared to 2.4GHz. "The speed of the wireless network is influenced by the quality of the signal being received by the access point, so solid walls can pose a deployment challenge," he adds. "The solution to this is to plan out the positioning of the access point and check that each mesh node is receiving a decent signal from the next hop. Built-in access point setup tools will often provide a speed or signal checker so that the optimum position of the access point can be determined and to help identify any areas which would benefit from further coverage."

Talking of solutions, another well-known supplier in this space is Huber+Suhner. Its range of SENCITY small cell/DAS antennas are designed "to be simple and attractive to seamlessly fit into any office or home" to provide wide wireless coverage, according to Cristina Olimpieri, the firm's product manager RF antennas.

"To generate the same high-quality connectivity with thick walls in the way, the network needs to be dense by installing multiple antennas that offer both capacity and coverage within a given space."

Cristina Olimpieri, product manager, Huber+Suhner

"To generate the same high-quality connectivity with thick walls in the way, the network needs to be dense by installing multiple antennas that offer both capacity and coverage within a given space. These kinds of antennas are coming on to the market to address similar challenges of network," she adds.

Although it's clear, indeed obvious, that thick walls will only provide resistance to fluid connectivity, Brice warns that the worst material to work with is in fact…paper. "Given the amount of moisture it holds, it absorbs anything it bonds with," he says. "Stone is also particularly tricky to work with for a number of reasons. Old stone walls are often protected so can either not be disturbed, and if they are, they must be handled carefully which takes money, time, and resources. In older buildings, a stone wall may be upwards of 30cm in depth while marble floors can require diamond drilling."

Having spoken to a handful of enterprises to find out how they have adapted to working in older buildings, it would appear that one way to navigate the connectivity challenge is to use powerline extenders. Roy Castleman, founder and managing director of EC-MSP, a London-based IT support company focusing on small and medium-sized businesses, says his company has deployed this technique, which works by essentially passing the ethernet over the power. "In other words, the exact opposite of power over ethernet," he says. "Firstly, one extender needs to be plugged into a power socket close to the entry point of your internet connection. Then an Ethernet cable should be connected from your router to the extender. Next, plug an extender into another power socket near a device you wish to get connected to the internet. You should then be able to plug an Ethernet cable into the device and the adapter. As long as both sockets are on the same ring, the Ethernet connection will be passed over the power line to the device."

Sounds reasonably straightforward, right? However, there are some factors to bear in mind. "There are some drawbacks to this solution, mainly that they can be impacted by electrical interference, some speed is lost using this method and finally the more extenders in use the less reliable the solution will be," adds Castleman.

While the focus of this feature is on the buildings themselves, it's important to consider the surrounding area. For example, older cities where the Romans set up home, such as London, have underground tunnels. Can these incredible feats from ancient times be put to good use in 2020?

Brice says that from his firm's experience of working with underground tunnels, "we cannot generalise" and say whether all can be put to good use, or if they are a hindrance. It is all circumstantial based on the tunnel's location as well as date of creation.

"With underground tunnels in older cities, such as London, the first question we ask is whether there is access to building plans," says Brice. "Once we have the building plans, we can then identify any potential restrictions, and make a call on whether a tunnel can be put to good use. Generally, the newer the tunnel, the easier it is to navigate. Firstly, as building plans will be available to view and secondly as we would be confident that the tunnel would have been lined correctly for cabling (as per the latest building guidelines). Having said that, we have worked with older underground tunnels and there are a number of ways to handle these.

White says that "we all read countless reports and industry research discussing the critical role of superfast broadband as a business enabler" - and CommScope absolutely agrees that it's a necessity for any organisation committed to delivering a first-class service.

"Yet, despite this, I still find it challenging to access the Internet or make calls consistently while I'm taking the train," adds White. "And it's even more of a challenge underground. The good news is, it is possible."

White explains how CommScope has been involved in innovative projects across Europe, including the world's longest rail tunnel which runs underground for 57 kilometres, with trains traveling at 250 kilometres per hour.

"Bringing the available network from the track side into the train - especially underground in tunnels - is probably the biggest challenge faced by operators when looking to provide seamless mobile coverage to rail passengers and CommScope have solutions that can solve this challenge too," he says.

The challenges are evident, but not insurmountable. However, surely there must be situations where a vendor has been unable to complete a job owing to the tricky working conditions?

Brice says a pre-survey to evaluate the customer's needs and the complexity of a building is always useful where possible. By using the results of a survey,

the vendor can take the steps which are required to prepare for the job, such as outreaching to regulatory bodies to request any installation permissions.

Nevertheless, he says: "It is very rare to come across cases where we have not been able to complete a job. However, rural sites come to mind here. With many often having cultural or religious significance, and no access to mains electricity, these sites can be very challenging. However, to avoid reaching the point of disappointing a customer mid-job, usually the pre-survey and our own assessments can identify these issues before we start working on the site."

Even though the buildings in question were built centuries ago, they are not alone in posing problems. White says that today, buildings are being designed to be environmentally friendly, energy efficient and also - especially those with lots of glass windows - to keep heat in and keep UV rays out.

"This does block radio frequencies from outside macro cells from getting into the building, negatively effecting indoor wireless coverage," he says. "As more and more older buildings are upgraded with low-E glass the requirements for in-buildings cellular solutions are set to increase."

White says this is where dedicated in-building wireless comes in. "Yet achieving the goal of reliable indoor mobile coverage is a significant challenge for operators, especially when businesses are based in large and complex buildings as we mentioned," he continues. "There is also an ongoing debate around whose responsibility it is to cater for the end-users; with mobile operators, building owners and facilities administrators all playing a role. We believe that establishing a dialogue and collaborative culture between these parties is essential – as businesses will look elsewhere if they can't get access to first class facilities, with wireless coverage, capacity and speed assured to enable productivity across their organisations."

It's also important to remember that adding cabling, access points and other modern technology to old buildings might not only be an eyesore, but there's a serious risk to the building itself. They've survived years of inclement weather, so it would be shame if they were to succumb to a masonry drill and other tools of the trade.

Brice says that having ample time is crucial when working with any type of older building. "When putting in place a networking infrastructure, you need the confidence that you're not going to damage the fabric of the building," he adds. "This means going through a number of steps to gain permission such as creating a solid plan and sending this to an authority to sign-off (all while leaving time for any flexibility in case design challenges arise along the way). Such steps were taken when we worked on old established colleges and universities - with designs ranging from medieval to Georgian - all across Europe."

Having said that, Brice says there is no specific type of older building that's more difficult to kit out.

"Every building brings its own challenges and difficulties, but we generally find that the older the building is, the more difficult it is to wire-up," he says. "One reason being is that most restrictions arise when building regulations are in place and with many older buildings often being listed or protected, regulations need to be navigated sensitively - which requires both an accurate building plan as well as time."

Brice warns that the biggest challenge can arise when looking at plans for older buildings as in "some cases they're not super clear" and in others, they may not exist.

"We have found this with the likes of Gothic buildings which has resulted in us working closely with our partners - and sometimes cable contractors and/or certified engineers - to conduct our own investigations," Brice continues. "These are often in the form of a pre-survey/audit. With these checks in place, we can analyse the physical aspects of a building and from there, identify the parameters we need to work within to mount access points (APs), for example. During one check in the past on a royal historical palace, we found shells used for soundproofing underneath the floorboards. We could not disturb these so worked closely with the customer to ensure we didn't break any rules".

Although buildings erected centuries ago were not designed for the connected world we operate in today, they can be adapted with a bit of ingenuity.

I do wonder, though, if the pandemic isn't brought under control, whether the next in-building comms feature will be about spare rooms and gardens sheds. ■

"The speed of the wireless network is influenced by the quality of the signal being received by the access point, so solid walls can pose a deployment challenge."

Alex Shuker, CTO, DrayTek

Councils give power to people

Local authorities across the country give internet connectivity boost to the locals

East Riding makes free Wi-Fi available

Connectivity is everything. In an age when being out and about doesn't mean you have to be out of touch, East Riding of Yorkshire Council is at the forefront of making free Wi-Fi accessible to all.

In the past year the council has made free Wi-Fi available in 39 of its venues across the county, meaning residents can now stay connected when visiting libraries, registry offices, entertainment attractions and leisure centres.

Need to send an email while watching your kids take part in a swimming lesson at an East Riding leisure centre? No problem. Just log on and register.

Want to post pictures on social media of a friend's wedding at the registry office? It's easy. Use the free Wi-Fi. Or how about if you want to live stream your big day to relatives in Australia? The ultrafast Lightstream broadband connection in Sewerby Hall's Orangery lets you to do that.

"Wi-Fi technology has revolutionised modern life, with many of our day-to-day tasks requiring a reliable internet connection, whether paying a bill or keeping in contact with family and friends," says councillor Jonathan Owen, deputy leader of the council. "The way residents are interacting with the council has also changed and ensuring that they can access services conveniently is important and the council is therefore pleased to have made this investment in its facilities. Working with KCOM to provide a managed solution has enabled the authority to roll out its free Wi-Fi to benefit local residents, encourage digital learning and tackle digital exclusion. The works represent an important investment by the authority in forward-thinking technology that allows residents to access services and transact with the council digitally.

Free Wi-Fi delivers a wide range of benefits. Having access to Wi-Fi allows visitors to market a venue by 'checking in' and posting comments or photographs on social media. It also streamlines the process of online booking and payment for services and allows customers to self-serve, providing reception staff with more time to give quality service to those who need it.

For learners at the East Riding's adult learning centres the new technology means they can work seamlessly between class and home on their own devices, accessing the virtual learning environment from home as well in the centre.

Among the benefits already seen by the council include being able to market and promote the wide range of bespoke ceremonies it offers and excellent ceremony room facilities available throughout the East Riding.

Since launching in 2016 the free Wi-Fi has proved popular, with 60,000 user sessions taking place across the 39 venues with 14,000 individual users.

New Wi-Fi delivers "digital inclusiveness" to citizens of Manchester

Science, technology and innovation have long been part of Manchester's DNA and promoting "digital inclusiveness" is central to this vision. In its drive to become a truly-connected city, Manchester has sought to harness the benefits of ultrafast broadband for the benefit of its citizens whilst offering free, high-quality Wi-Fi in many public places. As well as improving the overall quality of life, a key aim was to bring internet access within easy reach of new, previously excluded groups and communities, thereby enhancing democracy, opportunity and social cohesion.

Led by CIO, Bob Brown, Manchester City Council (MCC) has developed "Our ICT Strategy" which details ICT as a key enabler to transform the organisation, deliver new technologies to Manchester's residents and act as the vanguard to the digital revolution in Manchester.

To realise this ambitious vision, MCC needed to install fast, reliable and user-friendly Wi-Fi across a comprehensive array of public buildings. These ranged from libraries and leisure centres to historic buildings, heritage sites, sheltered housing, Sure Start centres, health and social care facilities, homeless shelters and many more – a total of almost 130 sites around the city.

At the time Daisy took on the project, Wi-Fi was only available in a few larger libraries. The existing infrastructure lacked the necessary scalability to support further development, while the user interface varied across locations, offering little scope to capture and understand user data or improve their experience. This meant that a comprehensive redesign was required.

Time proved to be another critical factor. In order to meet eligibility requirements for a vital tranche of funding, working Wi-Fi had to be delivered to all 130 sites within a short three-month period.

Daisy's state-of-the-art solution was based on a proven, resilient and scalable Cisco infrastructure housed in two separate data centres. Where possible, existing infrastructure was integrated into the design to provide fast, consistent and reliable Wi-Fi coverage across all sites.

The team designed a single proprietary portal, delivered via the Daisy Engage platform, to work across all locations, carrying the council's Busy Bee brand and greeting returning users with a "welcome back" page that remembers them by name and invites them to reconnect without the laborious process of entering usernames and passwords.

Reading's Invotra intranet designed, built and live within 21 days

Reading Borough Council first approached Invotra in September 2018 and soon confirmed Invotra's appointment as its preferred intranet provider. There were a number of challenges, including the fact that content was not easy to find or read, providing a bad user experience, staff struggled to find answers to help them serve customers, the appearance of the intranet was not modern and therefore did not attract users and the staff directory was not very informative, making it difficult for users to find and connect with each other.

One goal was to improve staff engagement to encourage collaborative working across departments thus improving services to the public. The other was to use an intuitive product to help improve digital skills and capabilities, encouraging employees to self-serve with access to timely, relevant information.

Invotra initially met and signed the contract with Reading in November. By the end of the month, Invotra had met with Reading's key stakeholders, including communications and IT teams.

Immediately, Invotra and the other existing government customers welcomed Reading into the Pan Government Portal, allowing it to collaborate and benefit from the ideas and best practices other customers shared. Following on from this, Invotra was able to create Reading's new intranet and provide them access whilst working with their IT supplier to integrate with their HR and Active Directory systems. This process would then populate their Invotra intranet with their people data that then builds out the Staff Directory and Organisation Chart features of the platform.

Also included within the onboarding package were detailed training and design workshops that included one to one contact between Reading and Invotra's UX and product team, allowing us to create an intranet that best portrayed Reading's value and culture.

Reading is now using Invotra and the platform is helping staff self-serve to find answers that better help them to serve the public and at a much faster rate.

It is benefiting from the social applications such as Groups, Message Wall, Polls, Ideas and Queries, that help to improve collaboration and engagement between staff.

Reading's intranet also allows to link out to other applications in use at the council, allowing them to create a single, unified platform for staff to access everything they need to excel in their daily roles.

Uckfield Town Council welcomes new high-performance solution

Uckfield Town Council plays an important role in the community by providing facilities for residents and visitors alike. The Civic Centre has offices, seven conference rooms and open public access - including a restaurant – which can see hundreds of visitors per day. Due to the number of visitors to the town council, having a secure, reliable wireless environment is key to its efficiency and the town council's existing Wi-Fi was not up to the job as it was slow, un-reliable and couldn't cope with the usage demand.

Mark Francis, estates and facilities manager at Uckfield Town Council says: "Our existing Wi-Fi was scattered which meant we couldn't scale the network. We actually had two networks, one for service which wasn't Wi-Fi and one for Wi-Fi, so we had to use several repeaters, meaning we had constant issues with coverage, interference and downtime. We were also concerned about network security as we hold large events for up to 280 people and our restaurant can hold 100, so we have a considerable number of visitors accessing the network at the same time".

In addition to providing a better Wi-Fi experience to visitors, Uckfield also wanted to encourage a more agile workforce by enabling staff to login to services from anywhere via a secure VPN. Francis knew that the town council's current network couldn't support its needs. He says: "I was recommended to use Redway Networks and after conducting an in-depth Ekahau wireless site survey Redway recommended a new wireless solution that would fit our needs."

Uckfield Town Council chose a new Extreme Aerohive Wi-Fi solution due to its reliability, ease of use and the fact it can be managed remotely through the Hive Manager. Redway Networks then built a virtual model of how the new network (which included HPE Aruba switches, 10 high-powered access points, a firewall and security software) performed to verify all the apps and devices worked efficiently before the new network was installed. Mark says: "During the install we had a great service from Redway's engineers. We had some complex troubleshooting to get around and they coped with it easily."

Uckfield Town Council now has a high-performance wireless solution with a VPN that provides unlimited connectivity 24/7, fast download speeds and the ability for staff to connect from anywhere, which is important to operations and efficiency. Customer service has been improved as visitors now have much faster, reliable Wi-Fi connections and the new guest acceptance portal keeps the network secure.

Cloud-driven networks the fuel that's powering the 'new normal'

Dahwood Ahmed, senior regional manager UK&I, Extreme Networks

With working regulations constantly in flux due to ongoing pandemic, organisations are thinking ahead to what the 'new normal' will look like in a Covid world. What many business leaders have realised during the pandemic is that the new practices implemented - such as remote working - are not just useful under lockdown measures but have universal benefits to be realised beyond it.

Organisations can't just go back to "how things were" before the crisis. Modern businesses will therefore offer employees a choice of where and when to work as part of a more sustainable, network-oriented landscape. This hybrid workforce will create new pressures on the technologies that organisations rely on, particularly when it comes to their network infrastructure. The new normal must be built upon a sustainable and hyper connected environment that can provide detailed insights into who, what, where and when connections to the network are being made, so what should the network of the future look like, and what should businesses consider?

Research from the ONS indicates that 49% of the UK adult population is currently working from home. And with many employers unable to fully reopen workplaces just yet, remote working is likely to persist into the future. Not only is it a safer option that greatly reduces the potential contact that employees experience during a working day, it is also proving to be popular among workers who enjoy greater flexibility. With this in mind, any organisation preparing itself for the new normal must consider how its network can facilitate safe and secure remote working in a post-lockdown world.

The first thing to consider is whether their current network enables employees to perform the tasks and operations they usually would in the office but in a home environment. If not, organisations should channel the power of cloud-driven networks to create robust and reliable connectivity that is consistent no matter where employees might be working.

Likewise, consideration should be given to the network structure. Given that remote access also potentially opens the door for cyber criminals to wreak havoc, network segmentation is key. This will still give employees the access they need while preventing cyber criminals from moving laterally throughout the network in case of a breach. There is also room to consider deploying more agile management tools so that as organisations become more distributed and administrators can become location agnostic.

However, not all employees can work from home and measures need to be taken to create a new normal in the office once we can all return to. This must begin with employee safety. Just as the UK government deploys contact tracing programs, so too should organisations - to an extent. Using connected occupancy sensors and real-time location analytics, employees and employers can minimise contact with others and interactions can be traced back if needed. These sensors also allow employees to easily see which rooms are the least busy throughout the day and thus the safest for their use.

At the same time, organisations should look to automate back office and business processes to minimise human interaction. Such measures are supported by a strong, cloud-powered network as these networks can be used to monitor and compile user activity. By using such insights around activity, businesses can create a picture of where employees are physically connecting to the network and how they move around within that environment by seeing which other devices were in use around the same time. Expanding beyond the scope of the workplace, this data can be fed into third-party applications that support contact tracing to further support containment efforts.

While such capabilities sound promising, many organisations currently don't have the network infrastructure in place to facilitate them. To meet the demands which come with the new normal, cloud solutions are a necessity. Fortunately, 82% of enterprises have ramped up their use of cloud-powered technologies in direct response to the pandemic. To support new features like real-time analytics and the increased number of IoT devices needed for occupancy management and remote working, the high uptime of cloud services will prove essential.

The scalability and simplified management of cloud-driven networks will also be critical going forward. As services become increasingly distributed and information needs to be accessed from more remote locations, a centralised management hub will be a boon. From this hub, the network can easily be scaled up or down to accommodate any current or anticipated requirements. While, with older wired and wireless systems flexibility and scalability are difficult to achieve or can only be achieved at an exorbitant cost - something today's businesses wish to avoid.

The pandemic has shown that businesses need to be ready to adapt to changing pressures at a moment's notice. Cloud-based network solutions that provide stability, resilience and flexibility are the next step in preparing organisations for the challenges of the future.

Connected devices and the future of cyber security in the retail sector

As retailers invest in IoT devices, security vulnerabilities increase. Lavi Lazarovitz at Cyber Ark Labs explores the foundation blocks of the future

The retail sector has experienced tremendous change in the last decade. The previously separate worlds of online and in-store commerce have become far more closely aligned, enabling us to move into an era of omnichannel shopping in which shoppers enjoy a seamless shopping experience, wherever, whenever and however they shop. Tech-enabled consumers are driving this important change — 81 percent of shoppers now research online and then continue to make their purchase in-store. Although the pandemic has skewed this data and led to a dramatic reduction in store footfall, the brick and mortar store experience is here to stay – albeit in a changed capacity.

The proliferation of IoT devices

The physical store now needs to act as an extension to its online counterpart. They're no longer focused specifically on customer buying, but more so around customer experience. Tomorrow's customers will be drawn in-store for a flawless customer journey and for a physical interaction with the brand identity of a retailer, rather than with the purpose of buying one specific item. However, achieving the provision of these seamless experiences requires a greater understanding of consumer behaviour.

So how do retailers ensure the same amount of sophisticated shopper data is captured in-store as online? And how do they analyse this data and respond quickly? The answer is technology at the edge. Retail success is being unlocked by a combination of innovative technologies, with Internet of Things (IoT) devices at the forefront of this change. According to research by MarketsandMarkets, the market for IoT devices in retail environments will be worth $35.5 billion by 2025.

Amazon Go stores are a perfect example of the complete transformation of the physical shopping experience. There are no human cashiers in these stores: weight sensors detect when items are taken from shelves, and they are added to a shopper's virtual cart, with products placed back on shelves automatically removed. Hundreds of cameras, which are able to distinguish between different shoppers by body type, follow them around the store, and when they leave, Amazon automatically charges them for the items they've taken using their saved payment details. This amalgamation of IoT devices provides an unparalleled, frictionless experience to the customer. Following their success in the US, Amazon has recently announced their intention to open up to 30 physical shops in the UK.

The accompanying threat

This proliferation in IoT devices, however, brings with it a distinctive set of cyber security vulnerabilities. Recent history tells us attackers typically target either point of sale systems – systems that process in-person, face-to-face payments from customers – or customers' credit card details when launching attacks on retailers. Successful attacks usually involve hackers either using compromised third-party credentials, credentials procured from phishing campaigns or vulnerable assets that have this data exposed to infiltrate internal IT systems.

IoT devices connected to a network create an attack surface that is likely to be a retailer's weakest link. They usually have limited processing power and memory, making it difficult to accommodate sophisticated security controls and making them easy prey. Many have admin passwords that have not been changed from factory settings or are fairly simple, making them easily hackable through a quick internet search. Once a hacker is able to hack a single IoT device, they are then able to traverse networks easily and make their way laterally throughout the retailer's IT infrastructure, often targeting privileged accounts – those with access to sensitive data and critical controls. Once compromised, malicious actors can use these accounts to cause irreparable damage to a retailer.

Due to their increasing proliferation, lack of security and organisations' lack of visibility of how exactly they are functioning, hackers often look to infect these devices with malware so they can be controlled and used to create a collection or network of 'bots' – usually known as a botnet. These botnets can then be used to launch Distributed Denial-of-Service (DDoS) attacks that overwhelm organisations' defences with more traffic than their network can accommodate or manage. These attacks either find a route into internal networks or establish an initial foothold that can eventually be used to target the crown jewels – point of sale systems and credit card data.

Tech-enabled consumers are driving this important change – 81 percent of shoppers now research online and then continue to make their purchase in-store

Securing the future of retail

The first step to securing connected devices is taking care of weak configurations. Misconfigurations mean these devices can often be accessed through default credentials, or through anonymous or insecure remote access. This is a relatively easy fix, as there are a number of Platform-as-a-Service and Software-as-a-Service tools out there that can proactively identify these misconfigurations and suggest how they can be rectified.

Zero trust is another tool that's useful for retailers trying to defend connected devices. Put simply, zero trust is a security model that does not trust any user or asset within a network until its security or legitimacy has been fully verified. In retail it should be seen as mandatory because it completely segments hackers from internal sensitive networks, and handling personally identifiable information (PII) and credit card data. Once these security measures have been implemented, retailers must also make sure they are constantly abreast with any software or patching updates. These updates might include repairing security holes that have been discovered and fixing or removing computer bugs. Hackers can take advantage of these weakness by writing code to target the vulnerability. The code is packaged into malware and then deployed onto the system. Simple updates can avoid the creation of these vulnerabilities.

The UK high street is set to face a tumultuous future, in the aftermath of the pandemic and the rapid shift in consumer behaviours towards online shopping. Investment in technology such as IoT devices can enable retailers to keep the tangible customer experience alive and create a retail landscape where physical stores retain their importance. But security needs to be kept front of mind when incorporating new technology to avoid the financial and reputational damage caused by a cyber-attack. Embedding security in the very foundational blocks of the future of retail will lead to long-term prosperity and stability, as our physical and virtual worlds continue to merge together.

Mitigating cyber-attacks with better DNS Security

Ronan David, vice president, strategy, EfficientIP

DNS attacks based on distributed, multi-vector and multi-stage assault modes have become highly sophisticated. Traditional security solutions such as firewalls, anti-DoS or IPS have not adapted to effectively ensure DNS availability and integrity. They have proved to be insufficient against cyber-attacks such as data exfiltration via DNS, DNS hijacking, amplification and reflection attacks and DNS flooding. Even worse, they present a high risk of blocking legitimate clients.

Considering the multiple threats posed by DNS attacks, it is important for companies to implement robust network security strategies. In order to ensure business continuity, DNS attacks require adaptive counter measures that go beyond just blocking. Traditional security solutions have proved to be insufficient against new attacks, mostly because they are not purpose-built for DNS functions so do not analyse the traffic at the DNS transaction level.

When it comes to ensuring network security, there are a number of procedures companies can adopt to mitigate the threat of DNS attacks. It is important that a modern DNS security system is agile enough to adopt its DNS protection mechanisms to mitigate the risk of blocking legitimate clients, whilst simultaneously safeguarding data and ensuring DNS service integrity and continuity to legitimate clients.

Companies must acknowledge that everything should be considered to be a potential threat to their network operations and more importantly to data confidentiality within their company. DNS Guardian provides a possible solution to this as it helps to protect data confidentiality. DNS Guardian separates the two DNS functions, cache and recursive, in order to dramatically strengthen and improve the security framework. Each function is protected separately, allowing an uninterrupted service to be provided, even when one function is targeted by an attack.

By analysing transactions at the heart of the DNS server--which include queries, responses, fragments, recursions--threat visibility is enhanced well beyond known attack patterns and overcomes the limitations of signature-based protection systems that only offer limited peripheral traffic visibility. It is important for companies to have visibility into the infected devices and to identify the user associated with the device trying to exfiltrate data. Additionally, it is important to guarantee data integrity and continuity of web services for businesses, even during an attack.

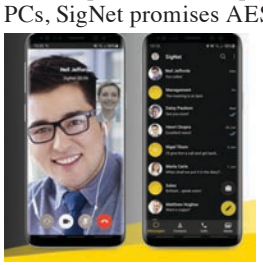
Additionally, it is beneficial to a company's data security to get instantaneous visibility on DNS services to improve remediation capacity with out-of-the-box statistics, delivering unequalled insights and reports on DNS traffic, without the need for additional appliances. DNS Guardian can offer a solution to this as it provides the most advanced DNS security solution on the market.

Moreover, the most effective way to address DNS-based data exfiltration is to build intelligent detection capabilities directly into the DNS infrastructure. Both sets of information gathered can then be sent to SIEM to provide enhanced reporting. As well as performing the critical functions of detecting and blocking data exfiltration attempts, lightning-fast remediation of the infected devices is necessary. This can be achieved by tighter integration between detection technologies and endpoint remediation solutions or NACs such as Cisco ISE to provide indicators of compromise when an endpoint is trying to exfiltrate data.

Analysing DNS traffic to develop internal threat intelligence is another key component of any modern data security strategy. DNS Guardian can help here as well: it detects zero-day malicious domains used by malware to communicate with external CnC servers (DNS tunneling) or exfiltrate data, and DGAs (domain generation algorithms). Identified malicious domains are dynamically shared between DNS Guardian appliances, delivering actionable predictive DNS security.

PRODUCTS

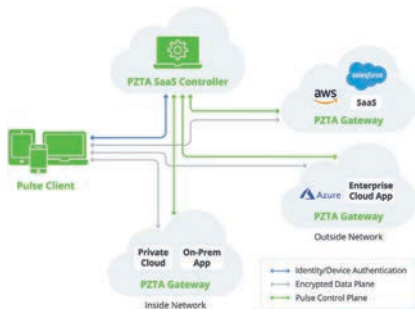
Developed for mobile phones and PCs, SigNet promises AES 256-bit encryption for voice, video, messaging, group chat, file attachments and Message Burn (self-destructing messages). **Armour Communications** says it has the ease of use of consumer apps and is available for iOS and Android as well as Windows 10, Linux and Mac OSX. The company says SigNet addresses some specific security requirements and as such will be sold alongside Armour Mobile. Features include: peer to peer encryption; files and attachments are kept within the app and therefore always remain encrypted, even when stored on the device; no recording or auditability; automatic alert to the sender of a message if a screenshot has been taken by the recipient; centralised control of only authorised users can connect to the service; and management of connectivity between users and groups. SigNet is available as Software as a Service (SaaS) and on-premises installation. Integration with PBXs and standard office desk phones is available. *armourcomms.com*



Taking data offline is the best way to keep it secure, says **Apricorn** as it introduces the latest in range of Aegis Padlock DT FIPS desktop drives. Pocket sized, it is said to be the first 18TB encrypted drive and includes the company's AegisWare firmware and feature set. All passwords and commands are entered on the device's onboard keypad. Apricorn says 100 per cent of the authentication and encryption processes take place within the device and never involve software or share passwords/encryption keys with its host computer. Additionally, it says, all have military grade 256-bit AES XTS encryption so firmware is locked down and cannot be updated or modified, defending against malware and ensuring data remains secure and accessible only by the user. The new model is the latest of eight, starting with 2TB. Apricorn says its devices help companies in regulated industries – such as finance, government, power and energy, legal and healthcare – to adhere to compliance regulations. *apricorn.com*

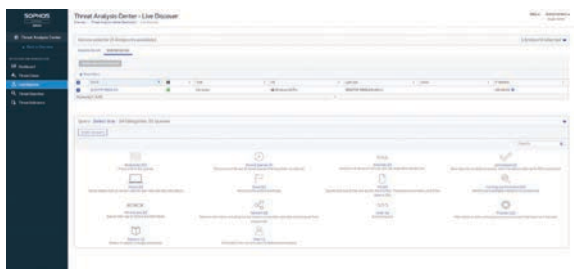
Three table-top firewall devices – all bright red – from Watchdog Technologies are said to offer enterprise grade security and business-critical internet speeds in a small form factor. Called Firebox T series, features include gateway antivirus, content and URL filtering, antispam, intrusion prevention, application control, cloud sandboxing and endpoint protections. T20, to extend protection to remote offices, can operate alone or managed from a corporate HQ. There is a Wi-Fi enabled model. T40, for small to midsized users, includes ransomware defence and AI-powered threat prevention. A Wi-Fi-enabled version offers 802.11ac wireless. T80 (pictured), for those with 50-plus staff or high traffic, features built-in Wi-Fi and an expansion module option for custom port configurations. All have SD-WAN capabilities and can be installed with the company's cloud-based RapidDeploy. T40 and T80 have Watchguard's Total Security Suite and Intelligent AV, to guard against present and future malware. T40 has one PoE port and T80 has two. Model T15 is for small sites. Users can deploy appliances from the cloud, update threat signatures, detect and eliminate malware and more with automation-enabled processes. *watchguard.com*

Rising numbers of mobile workers and increasing data threats were cited by **Pulse Secure** as it introduced its Pulse Zero Trust Access service. It comprises the Pulse ZTA Controller, hosted and managed by Pulse; the virtual Pulse ZTA Gateway that customers deploy on-premises or in the cloud; and the Pulse ZTA Client which runs on each user's Microsoft Windows, Apple macOS and iOS and Android device. Pulse says it offers users streamlined access while allowing organisations to govern every request by automatically verifying users' identity, device and security posture before granting direct, encrypted connection to applications in public/private clouds or data centres. Gateways are deployed in the customer's on-premise and cloud environment closest to the application or resource which, says the company, optimises users' experience, reduces latency and enables hybrid IT deployment at scale. Available for companies of any size, the service is priced at an annual subscription per user, with discounts for 500-plus and multi-year agreements. *pulsesecure.net*



Seven in 10 IT professionals report an increase in security threats as criminals target home workers during the pandemic, says **Check Point Software Technologies**, quoting its own research. And 95 per cent of respondents globally said it had brought security challenges. They have three demands: preventing even advanced, zero-day cyber-attacks; the ability to secure any type of network expansion or changes on demand; and unified solutions that speed operations and automate protection. It has a range of devices called Quantum Security Gateways, for branch offices up to corporate data centres, said to have twice the performance and half the energy use of rivals. They now include its SandBlast Zero Day Protection said to offer 60-plus security services for threat prevention, including a 100 per cent block score for malware prevention, exploit resistance and post-infection catch rate, recognised by NSS Labs. Also included: up to 1.5 Tera-bps of threat prevention performance; multiple expansion ports; SSDs and second power supply. *checkpoint.com*

Just 24 per cent of organisations hit by ransomware were able to detect the intrusion and stop it encrypting their files, says **Sophos**, citing its own survey. It says its updated Endpoint Detection and Response (EDR) includes features to help users detect threats and breaches that could otherwise take months to uncover. EDR includes Live Discover which, says Sophos, allows users to pinpoint past and present activity, retaining data for up to 90 days. SQL queries allow administrators to answer threat hunting and IT questions and can be selected from a library of pre-written options and be fully customised. It provides access to granular and detailed endpoint activity recordings, further enhanced with Sophos' deep learning technology. Live Response, says Sophos, allows users to remotely respond and access endpoints and servers using a command line interface for further investigation and remediation, easily reboot devices, install/uninstall software, terminate processes, run scripts, edit configuration files, run forensic tools, isolate machines and more. *sophos.com*



Please meet...

Paula Cogan, CCO, Colt

What was your big career break?

My big break was right at the beginning of my career. I hadn't planned a long-term career in telecommunications or technology, but a year after I graduated, I found a temporary job on a sales desk for BT, and I found that I really enjoyed it and was successful at it. This was at the cusp of the first mobile technology, and I was part of the first mobile sales team at BT. I was able to experience first-hand the boom in this technology and how it was changing the way societies and organisations worked. This was also my first foray into the world of innovative technology, at the time I didn't know anyone with a mobile phone and to be involved in the telco sector at this exciting time really changed the trajectory of my working life.

Who was your hero growing up?

My hero as a young girl and even as a teenager was Russian gymnast Olga Korbut. I used to compete in gymnastics, and she was a real inspiration for me. I was inspired by her level of fitness, grace, agility and also her competitive edge. She was a real role model.

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

The best piece of advice I have been given is 'don't be afraid of failure', and it really has stuck with me, because it was not advice that was simply given to me, instead I gained it through experience. I used to work for a large American telco, and I had a manager who would purposely test me. He would give me tasks that at the time seemed pointless and impossible, they were often really out there, and I couldn't see why I was being given them. After a while, he said to me: "You must have realised by now I wanted you to learn from these failures? I also wanted to see how resilient you are." This man became a great supporter and mentor of mine – he really taught me a lot through these stretch projects and this contributed to the level of confidence I have now.

What's the strangest question you've been asked at an interview?

Very early in my career, I was asked by an interviewer: "Why would you want to do this job? Doesn't your husband have a good job to support you?" Now, thankfully these questions are no longer commonplace, but I would imagine many women who are leaders today, may have encountered something like this before. It was questions like that that led me to found Colt's women's network - Network 25, to ensure gender equality was championed at Colt.

If you could live anywhere, where would it be?

Everyone who knows me knows that I have a passion for travelling. I travel extensively for both work and pleasure. Asia is one of my favourite places to visit, I love the vibrant colours, smells and diversity across the region. I also enjoy Italy because of its art, culture and of course the great food and wine! However, in all honesty, I am very happy living in the UK. There are three areas that I am really drawn to here, I was born in the North East, and I go back to the North Yorkshire coast frequently. I live in the Chiltern Hills in Buckinghamshire, and I also spend a lot of time in London, which is where our office is. So, while I am always happy to travel, there's something so nice about coming home.

What would you do with £1m?

It would be amazing to have £1m to give to charity right now. For me, I wish I could give half of it to charities that support homelessness, especially in advanced societies such as London. UK charity, Crisis, recently played a huge role in getting people into temporary accommodation during lockdown, and I think it's so important that charities like this can continue their work. I would like to give the other half to charities supporting women leaving domestic violence situations. Coronavirus has caused so much heartache globally, but lockdown meant for many that they were trapped in unsafe situations. It is already thought that domestic violence cases have risen some 20% during lockdown, with experts seeing this as a "shadow pandemic" alongside Coronavirus. These causes are close to my heart, and I support them personally, but this question got me thinking again about the importance of wider charities during the Coronavirus pandemic.

What law would you change?

As mentioned before, I love to travel. However, it saddens me that not everyone gets to experience travel like I do. Our Pride Network at Colt, which champions our LGBTQI community recently hosted an Ally Training and in that it was explained that in 70 countries it's still illegal to be gay. This is definitely something I would rectify if I got the chance.

The Beatles or the Rolling Stones?

I would have to say the Beatles. I love them both, but I grew up to my parents listening to The Beatles and also, they were the original boy band. I am a big lover of music, and I think The Beatles created music that covered such a range of genres from rock and roll, psychedelic rock and folk, their music changed as society did – making them truly iconic.