MAY 2022
networkingplus.co.uk

NETWORKING+

Security and hybrid working

How to handle security as staff work remotely

Ken Galvin, Quest
p6

Addressing gender inequality

How to make roles appeal more to women

Heather Hinton, RingCentral
p7

Questions and answers

Meet a fan of Manchester City and Majorca

Jon Fielding, Apricorn
p16

Zayo and Equinix complete 400G London-Paris data centre trial

Global fibre-based communications provider Zayo Group Holdings and data centre business Equinix successfully completed a 400G trial, connecting data centres in London (Slough) and Paris on the former's subsea fibre network.

Undertaken in Q1 2022, the 400G networking technology trial marks the latest joint innovation between the companies, as they seek to meet growing demand to move continually-increasing volumes of data ever faster.

As part of the trial, Zayo deployed a 500G optical channel on its 800G-enabled DWDM network.

It used the additional bandwidth to deploy an extra 100G wave for enhanced monitoring capabilities, creating increased visibility to ensure the consistent viability of the network. The connection managed to withstand full-load testing without any traffic loss.

Both companies said the new 400G technology produced many benefits by reducing hardware from four separate 100G optical cards to just one 400G card. This resulted in a simple application with fewer handoffs between the customer and Zayo, reducing the potential points of failure. Equinix streamlined operations by having fewer circuits to manage and operate its network while reducing costs. These achievements mark key differentiators for customers who build their networks around high bandwidth capacity, the companies added.

"At Zayo, not only are we focused on our customers' connectivity needs today, we are preparing for their speed, latency, and capacity needs of tomorrow while simultaneously driving efficiencies and simplifying the overall network design," said Yannick Leboyer, Zayo's chief operating officer, Europe. "Equinix is sitting at the epicentre of several trends that are reshaping the industry – from digital transformation and big data to IoT and AI. Together, we're future-proofing the ecosystem to help companies grow and innovate."

As part of the trial, Equinix, which is also a colocation provider for enterprise network and cloud computing streamlined operations by having fewer circuits to manage and operate its network while reducing costs.

The company said the trial's achievements mark key differentiators for customers who build their networks around high bandwidth capacity.

"Our success in this trial is about more than faster speeds; it's about the outcomes it will enable for our customers, such as achieving the low-latency requirements of critical devices transforming everything from transportation to healthcare," said Muhammad Durrani, senior director of global network architecture for Equinix. "As the first global data centre platform to trial 400G, we see tremendous potential in how it will help power our next generation of services."

As part of the trial, Zayo said it also reduced power consumption per gigabit by 40% compared to prior generation hardware. In addition to reducing energy costs for customers, the achievement aligns with commitments by both Zayo and Equinix to sustainable business practices and efforts to reduce environmental impacts. Zayo has also achieved efficiencies in hardware and equipment usage, the company said.

In addition to reducing energy costs for customers, the companies added that this achievement aligns with commitments by both Zayo and Equinix to sustainable business practices and efforts to reduce environmental impacts.

Zayo's communications infrastructure solutions include dark fibre, private data networks, wavelengths, ethernet, as well as dedicated internet access and data centre connectivity solutions.

Founded in Silicon Valley in 1998, Equinix has more than 220 data centres in over 60 markets on five continents. ■

Cabinet Office admits to losing nearly 800 devices

The Cabinet Office, the UK governmental body responsible for supporting the prime minister and cabinet, has reported almost 800 electronic devices lost or stolen in the past three years, according to official figures.

Data retrieved via the Freedom of Information Act and analysed by niche litigation firm Griffin Law, observed the number of electronic devices reported lost or stolen each year for the past three financial years, FY 19-20 to FY 21-22.

In total, the Cabinet Office reported 791 laptops, mobiles, Mifi wireless routers, and other devices either lost or stolen, 61% of which 479 were mobile phones.

Laptops accounted for 28%, 219, of the devices whilst Mifi's made up 38 devices and a further 55 'other' devices were reported missing.

The news comes after Liberal Democrat Sarah Olney exposed a number of government departments for misplacing devices, labelling it as "deeply worrying."

Cybersecurity expert Achi Lewis, Area VP EMEA, Absolute Software, said:

"It is a tricky task for large organisations, including the Cabinet Office, to manage a vast workforce of staff and devices, especially through unprecedented circumstances like the pandemic. These organisations represent an example for many businesses and as such need to ensure they have the proper cybersecurity solutions and protocols in place to both prevent and manage the loss of devices."

The financial year 2019-20 saw the most devices lost or stolen with 435 devices, as organisations transitioned from their offices to remote working as a result of the pandemic. ■

Custodian selects Aqua for new Dartford site

Custodian Data Centres, the colocation provider for MSPs, cloud, enterprise and digital entertainment organisations, has enlisted Aqua to design, supply and install an innovative temperature control system and the new 10MW site located in Dartford, Kent.

The former's Maidstone facility is nearing capacity, so it commissioned its new 'DA2' facility in Dartford, Kent, to "meet the continued growth demands of its customers". Less than 15 miles outside of central London, Custodian's goal was to provide an advanced facility for end-users to relocate and host their mission-critical applications. The new site is carrier-neutral, operating at a PUE rating of below 1.3 and powered by resilient, 100% dual diverse renewable energy feeds.

Aqua delivers an energy-efficient, bespoke, closed-loop air cooling system with integrated free cooling. The design for Custodian's DA2 includes 12 custom-designed cooling coils and a free cooling chilled water system, comprising of 3 x 500kW Aqua EcoPro+ optimised free cooling chiller units, to accommodate for the initial phase of the site opening. The EcoPro+ units operate on R454B green refrigerant. Utilising integrated free cooling chillers, drastically reduces the amount of time mechanical cooling is required, saving significantly on energy usage, carbon impact and wear & tear of components parts, in particular the compressor.

"With the new DA2 Dartford site boasting a 10MW capacity, we needed a reliable cooling system that could handle the increased demands from the bigger site," said Callum Woodhouse, M&E manager at Custodian Data Centres. "As our customer base continues to grow and expand over time, this Aqua solution allows us to adapt to the additional demands, in a seamless and efficient way".

The system is also future-proofed, with the option for expansion into higher density cooling further down the line, as Custodian continues to grow and expand. ■

Tata further strengthens IZ Internet WAN for global enterprises

Digital ecosystem enabler Tata Communications has bolstered variants of its IZO Internet WAN for enterprises in the UK and Ireland, addressing a business environment that is increasingly entrusting priority business traffic to internet connections.

IZO Internet WAN first launched in 2014 and Tata claims it to be the world's first predictable and dependable internet. The introduction of IZO Internet WAN suited for enterprises is designed to provide high-quality internet services and access to more than 150 geographies, allowing enterprises to have what is described as simple and agile management over their global and regional networks.

It is also claimed to enable what Tata said will be "seamless" data transfer from branch offices to datacentres, from branch offices to clouds, and across multiple clouds for enterprises.

Tata added that the service is suited to enterprises introducing cloud services to their existing IT and networking architecture as well as for businesses keen to cost-effectively extend their global reach to new markets. Key target industries for which Tata sees the service as particularly suited include manufacturing, IT, ITeS, retail and BFSI.

"We closely listened to our global enterprise customers, and for them, guaranteed uptime is business-critical," said Song Toh, vice-president of global network services at Tata Communications. "Hence, our objective has always been to deliver highly available quality internet.

Tata quoted Gartner research, which shows that growing cloud deployments of business-critical applications will drive 30% of global enterprises to use enhanced internet services by 2023, up from less than 1% in 2020.

The new variants have also released for enterprises across North America and Asia-Pacific markets. ■

Daisy helps Greggs roll shops into the future

Daisy Corporate Services, the provider of secure IT, communications and cloud services, has partnered with British bakery chain Greggs to deliver a future-proof, security-centred SD-WAN solution.

The Meraki-powered service "offers businesses improved agility via a network that evolves in line with specific current and future needs as well as offering a zero-risk approach to security". Greggs will use the service to ensure faster in-shop connectivity that can drive increased use of in-shop devices. It will also ensure that shops who partner with the likes of JustEat, "have the consistent, high-quality bandwidth required to fulfil growing demand".

In addition to the SD-WAN design, Daisy is providing LAN Switching, Wi-Fi and 4G/5G connectivity through Meraki.

"The new Daisy SD-WAN will deliver a security focused network with enhanced application control and performance," said Chris London, data sales specialist for Daisy Corporate Services.

Tony Taylor, IT and business change director at Greggs, added: "Daisy has been working with Greggs since 2008, delivering a variety of connectivity and managed services. Daisy's SD-WAN will allow for faster, more usable connectivity to more than 2,100 shops, with better reliability, and resiliency." ■

EDITORIAL:
Editor: Robert Shepherd
roberts@kadiumpublishing.com
Designer: Ian Curtis
Sub-editor: Gerry Moynihan
Contributors: Anthony Brown, Ken Galvin, Heather Hinton, Sandeep Jandu, Russ Kennedy, Paul Ward, Alan Hayward, Courtenay Mills and Jon Fielding

ADVERTISING & PRODUCTION:
Sales: Kathy Moynihan
kathym@kadiumpublishing.com
Production: Karen Bailey
karenb@kadiumpublishing.com
Publishing director:
Kathy Moynihan
kathym@kadiumpublishing.com

Networking+ is published monthly by:
Kadium Ltd, Image Court, IC113, 328/334 Molesey Road, Hersham, Surrey, KT12 3LT
Tel: +44 (0) 1932 886 537

ISSN: 2052–7373

Uni researchers develop technique for improving broadband service

Researchers at Bangor University have found a cost-effective way to improve the performance of networks which supply mobile services and broadband to businesses.

As well as improved performance, the new technique developed at the Welsh university's Digital Signal Processing (DSP) Centre, is also said to be "kinder on the planet". This is because the technique's lack of complexity means less energy is needed to transmit a given amount of data, which results in less of an environmental cost.

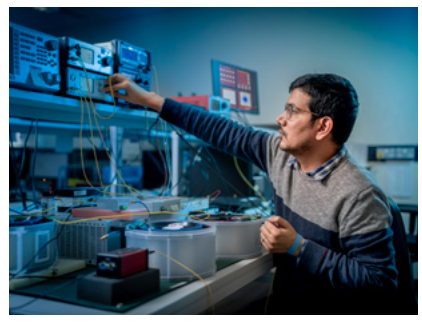
In the process, the researchers have set a new world record for using DSP to transform complicated, non-linear, low-speed optical transmission systems into simple, linear, high-speed ones, Bangor University said.

Results from the latest research carried out at the DSP Centre demonstrate that a 10-fold increase in bandwidth of commercially installed access networks is technically feasible over an extended distance of 100 kilometres by manipulating the way the data is processed in the receiver using a technique based on digital signal processing.

"Using advanced digital signal processing, we are manipulating the way in which signals are processed in the receiver to compensate for the effects that usually limit bandwidth and transmission distance," said professor Jianming Tang, director of the DSP Centre, Bangor University. "This approach could be used to upgrade existing networks without requiring considerable changes to be made to these networks. The approach also allows cheap and low-power consumption solutions to be deployed in new networks, capable of satisfying unprecedented technical requirements associated with 5G and beyond."

Tang added that the DSP Centre is now looking at how this approach could be further integrated with its "other cutting-edge techniques to provide additional network security by detecting unauthorised changes to the network, and unauthorised access to the data, which is of paramount importance these days".

The DSP Centre at Bangor University has secured £3.9m in project funding from European Regional Development Fund through the Welsh Government. In addition to this funding, the centre has also recently secured £3m from the North Wales Growth Deal as one of the projects within the Digital Programme. ■



Motorola's BWV to cover all major roads

National Highways will equip traffic officers across 4,300 miles of roads with VB400 body-worn video cameras (BWV) from Motorola Solutions.

The cameras will be used by officers conducting patrols across England's strategic road network (SRN), which comprises 4,300 miles of motorway and major roads in the country.

National Highways said traffic officers help to keep traffic flowing smoothly during more than four million journeys that take place across England's motorways and major roads each day.

"Our traffic officers patrol England's motorways and major roads 24 hours a day, seven days a week and are at the front line to keep people safe and help the network run smoothly," Mel Clarke, customer service director of National Highways, said: "The body-worn cameras protect citizens and our traffic officers and are now part of the officer's uniform. This investment forms part of our commitment to maintaining the safety of England's roads and providing greater operational visibility for our staff and the general public."

Motorola says the rugged VB400 is designed to withstand rigorous use in all situations and captures high-quality video and audio in all weather and light conditions. The deployment also included Motorola Solutions' VideoManager evidence management software to upload and manage the recorded video securely in the cloud.

"The VB400 body-worn cameras are developed locally in the UK and will support the safety of millions of passengers who drive across England's major roads during the day and night," added Fergus Mayne, Motorola's UK & Ireland manager. "By deploying the cameras to all traffic officers, National Highways has committed to the highest levels of safety for everyone who travels and works on the roads."

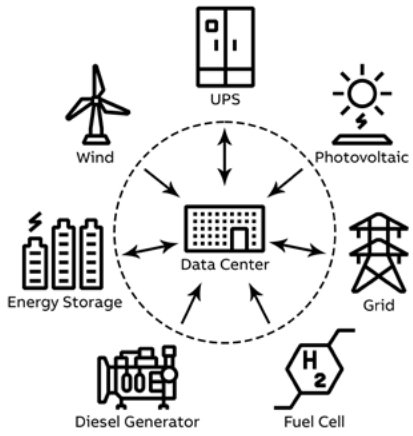
This latest National Highways deployment is one of several recent applications of Motorola's BWV by UK public safety organisations including NHS England, Lancashire Constabulary and Police Scotland. ■

'Most UK businesses experience up to five security incidents a year'

The majority of UK businesses experience up to five security incidents each year, according to new research. This data is taken from Infoblox's new *State of Security* Report which shines the spotlight on the latest security risks plaguing organisations around the world. It discovered that whilst organisations are accelerating digital transformation projects to support the hybrid landscape, attackers are seizing on vulnerabilities in these environments, creating bigger headaches than ever for security teams. The report also found that half (50%) of UK companies more concerned about data leakage than anything else. The good news is 73% could detect and respond to a security incident within 24 hours. ■

ABB's microgrid solution keeps sustainable power flowing

ABB is pioneering new microgrid solutions to pave the way for data centres to have self-generation options and to enable grid services whilst ensuring the mission critical availability of power is fulfilled. The solutions are covering microgrids to be able to operate both on-grid and off-grid with different options depending on the energy mix of the data centre as well as the possibility to actively interact with the grid. "Data centres can support and adapt to this shifting energy landscape with new technologies which allow them to be both consumers and prosumers," said Danel Turk, data center solution portfolio manager for ABB. ■



CommScope introduces XGS-PON suite

CommScope has released a new cloud-to-edge suite of next-generation XGS-PON solutions, designed to facilitate the global growth in FTTP deployments. The company said it can achieve this through three main advantages: a flexible architecture; open, interoperable components; and dynamic, cloud-based operation. Furthermore, the cloud-to-edge solution allows service providers in both greenfield FTTH and fibre-deeper scenarios to bridge multiple network topologies and take advantage of SDN efficiencies to prepare their networks for the future, regardless of requirements. The Cloud-to-Edge Next-Gen PON suite consists of four components: new CommScope FLX PON OLT and ONU portfolio, ServAssure domain management and ServAssure NXT performance management software, fibre connectivity solutions, and engineering and project management services. ■

'IT cost control is top business challenge'

More than half of IT decision-makers name cost optimisation as the biggest challenge they face today, a new study has found. Research from global IT services company Crayon reveals that controlling and managing the costs of an increasingly complex and expensive IT estate is keeping global IT decision-makers awake at night. Globally, only 54% currently believe they have an exact understanding of their IT costs. In the UK, a third of technology leaders flagged they lack knowledge on how to optimise their cloud spending, with another third stating they do not have the time to search for the best deals. The new data was obtained through a study conducted by Sapio Research, polling 2,050 IT decision-makers at large organisations (200+ employees) worldwide. ■

Bridewell becomes 'first carbon negative cyber firm'

UK cyber security services company Bridewell has become carbon negative, making it the first UK cyber security organisation to achieve carbon net zero in accordance with recognised standards. The milestone, which was achieved in less than a year, was down to a combination of initiatives, including a switch to renewable energy, offsetting and climate projects. Importantly, the company said. "We wanted to go beyond the minimum requirements in the GHG protocol," said Martin Riley, director of managed security services, Bridewell. ■

Netskope expands data protection capabilities

Netskope, the security service edge (SSE) and zero trust vendor, has introduced a key expansion of data protection capabilities to endpoint devices and private apps. The patented endpoint data loss prevention (DLP) solution will enable Netskope Intelligent SSE customers to protect data everywhere it moves across the hybrid enterprise. With the continued expansion of the Netskope Intelligent SSE platform, customers will be able to protect data across SaaS, IaaS, private applications, web, e-mail, and endpoint devices from a single converged data protection solution. The service also allows for leveraging machine learning, user and entity behaviour analytics (UEBA) and insider threat mitigation capabilities to improve security efficacy, efficiency and agility. ■

Microsoft adds free VPN to Edge browser

Microsoft is adding a free built-in virtual private network (VPN) service to its Edge browser to boost security and privacy, the company said. Called "Edge Secure Network," the software giant is currently testing the Cloudflare-powered VPN service and says it will roll it out to the public as a part of a security upgrade. When turned on, Edge Secure Network should encrypt users' web traffic so internet service providers cannot collect browsing information, such as health-related searches. The new feature will also let users hide their location by making it possible for them to browse the web using a virtual IP address. ■

Scott Logic wins HM Land Registry contract

UK-based software consultancy Scott Logic has been awarded a two-year, £9m contract with HM Land Registry to help it achieve an ambitious transformation programme. The department is responsible for more than £7tn of land and property ownership across more than 26 million titles and ensures that land and property rights are guaranteed and protected. HM Land Registry is aiming to transform by using innovative technology, investing in expert people and streamlining processes to make all interactions easy, effective, and more user-friendly. The contract entrusts Scott Logic with the provision of a range of software delivery roles to complement and extend the capabilities of the Authority, covering architecture, front and back-end development, testing and DevOps functions. ■

Word on the web...

Long live the desktop

Raeford Liebenberg, manager at Silvermoon, a Galix company

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

Preparing for the convergence between edge, IoT and networking tech

By Alan Hayward, sales and marketing manager, SEH Technology

What can the market expect from the convergence between edge, IoT and networking tech? As the industry continues to slowly recover from the Covid-19 pandemic, Forrester Research outlines the predictions that tech leaders can anticipate regarding the shifts in edge computing, IoT and networking technologies. Altogether, it's difficult to imagine that any business wouldn't be affected by these predictions, they need to look to revolutionise connectivity in a sustainable and streamlined manner.

Looking specifically at the networking technology sector, the focus will be rising to the challenge of 5G, increase in smart infrastructure investments and the mission to reduce carbon emissions.

The evolution of 5G

IoT devices are on a staggering growth trajectory, revolutionising homes and places of work. Its potential, however, has been staggered due to a network data bottleneck - but 5G is set to be the most promising solution. Up to 100 times faster than its predecessor 4G, the new era of cellular internet will create never-seen-before opportunities, advancing everyday life. As IoT devices and their applications grow more complex, they continue to send an increasing amount of data to the Cloud. To date, the industry utilised edge computing, pushing data processing and AI capabilities from central Cloud servers to other parts of the network. This approach is now reaching its limit, meaning its now time for 5G to take the lead.

In simple terms, 5G networks widen the pathway that carries data to the Cloud, which ensures the increased volume of data can be transferred at a faster speed. This results in low latency of 5G networks and can also solve the connectivity issue in rural areas. In fact, Forrester predicts that 85% of satellite internet users will be in rural locations. Looking ahead, full-scale 5G network adoption for IoT devices will require businesses to make significant infrastructure investments, which may not be feasible for all. It's important to remember that as with edge computing, 5G is essential for the next generation of IoT connectivity. Despite delays in the introduction of 5G, it is set to help the industry build a harmonious network of devices, homes and businesses in the future.

Investing in smart infrastructures

Forrester also predicts a boom in smart infrastructure for 2022, with investment expected to increase by 40%, driven by investment from China, Europe and the USA. Whilst much of that spending will go towards alleviating pandemic recovery, the investment will also be directed to internet connectivity. Early technology adopters of IoT, edge computing and 5G are already beginning to demonstrate that these technologies can empower smarter infrastructures. This highlights the opportunities that businesses can gain from leveraging data insights to modify operations and drive new projects.

As we move into the next phase of COVID-19 recovery, more and more companies and governments are investing in building a smart infrastructure as a way to make their institutions more adaptive, resilient and creative. They can also use this to launch new projects that span across emerging use cases that leverage an array of technologies. Not only will this technology lead to a transformation in the way stakeholders operate, but it will also help them deliver the relevant services or products that customers are coming to expect in today's fast-paced marketplace.

Combining edge and IoT to cut emissions

Moving forward, the demand for sustainability-related services powered by edge computing and IoT will grow in relation to energy efficiency and resource management. This is especially important in the case of environmental monitoring, resource management and supply chain processes. With edge computing, the data from sensors and devices is processed at the edge, where a company's data is being generated. As the data never has to leave the network to provide insights, it helps to reduce latency and puts far less strain on network bandwidth, which ultimately lowers CO2 emissions.

In fact, a recent report from Vodafone and WPI Economics discovered that emerging technologies such as IoT, 5G and edge computing will help the UK reduce the country's CO2 emissions by 17.4 million tonnes per year. Whilst these technologies will deliver the efficiency improvements that reduce businesses' carbon footprints, they will not impact society's ability to live, work and travel without significant disruption.

A future of technology convergence

If the past two years have taught us anything, it's that businesses can't prepare for anything. There are some trends that are converging and can help guide them in regard to future plans. Whilst these technologies will help reduce a company's carbon footprint and cut emissions, it also creates opportunities to invest in smart infrastructures and encourage IT leaders to consider investing in 5G to tackle the emerging challenges related to IoT. ■

How to control the IT chaos of a hybrid workforce

By Ken Galvin, senior product manager, Quest

Organisations across the world have embraced remote working, offering more agility and flexibility than ever before. There was a time where tablets, smart phones, and new IoT devices were not a common business tool. However, just as organisations started to get to grips with how to handle these applications and devices, we faced a new turn of events with employees looking to work not only from any device, but across any location and at any time. Our digital lives make us more productive and offer us the potential to work in a much more free and agile way. The good news is that this opens up a whole host of benefits and worker productivity for the organisations that can make this work, but we can't neglect the hard-working IT teams in the background. These new trends can present a whole host of challenges in terms of security, compliance and data access. So, with the new hybrid workforce set to stay, how can organisations enjoy the benefits and minimise the risks?

In the past 18 months, while employees have enjoyed a more flexible working style brought on largely by the pandemic, IT admins have suddenly found themselves overwhelmed. They have had to adjust almost overnight and manage a remote workforce, who are using a variety of different company owned and personal devices, downloading and installing software from various sources and are relying on IT teams to help overcome challenges that are keeping them from being productive.

As part of this, IT admins have had to also consider how secure the home is for remote employees, how to patch devices remotely, look at password security, VPNs and battle against ever more destructive cyber-attacks.

The reality is that every device connecting to an organisation's network is a potential attack vector. We see every day that malicious actors are taking advantage of the lack of control many organisations have over this sudden flood of unknown devices.

As the number of remote devices increases in both volume and diversity, it's no surprise that teams find it harder and more time consuming to manage, secure and keep track. Without some type of automation in play, organisations simply cannot keep up. But automation simply for the sake of it will not cut it. A lack of consistent and unified endpoint management leaves businesses in a precarious situation.

If businesses don't know what devices they have, then IT teams cannot manage them. And if you cannot manage them, you cannot secure them. For any organisation that is embracing either remote working in some form or mobile devices, one of the first and most critical steps is to gain visibility. Businesses need to address this issue by tracking remote devices and ensuring they can manage them when it comes to security updates and data access. However, it is important to note that gaining visibility means doing a thorough inventory. Endpoints also include printers, cameras, and an ever-growing amount of IoT devices. It essentially means tracking any device that has the potential to connect to your corporate network or will be used to access company data. Not only will this give a business more control, but IT teams can be aware of what devices are accessing their network, administrative rights can be set and if a device goes missing or is corrupted the organisation can act swiftly to ensure company information is kept safe and secure.

Once organisations have started to get to grip on the different devices connecting to the network, IT departments must prioritise addressing the security risk, regaining control and improving management and compliance.

Although employees might be accessing information away from the traditional corporate office or on remote and personal devices, this doesn't mean that we should give way to usual business protocol and privileges. It is just as important that IT admins set admin rights and restrict a user's ability to access sensitive information or change operating system configurations. Too much user control potentially introduces vulnerabilities that allows malware to gain a foothold. In addition, if devices get lost or if data does become corrupt, by limiting the access this in turn is going to limit any potential data loss and help businesses to stay compliant with data protection laws.

Alongside access restrictions, it is also important that businesses look at when devices were last patched and updated. There are tools out there that make device patching super simple, and organisations are aware of the security risks, however this continues to be a pain point for many businesses.

As we saw earlier this year, it is something the UK Government was even scrutinised for when malware was found on laptops they had given out to support vulnerable children who were being home schooled during lockdown. This was due to an unpatched vulnerability, and it could have been prevented if the machines had been adequately updated. It is far too often that we hear of hackers preying on individuals and companies that are already struggling through a challenging time, but hackers are opportunistic, and they will continue to look for any attack vector to infiltrate.

All too often organisations do not formalize their patch management. The recent Emotet outbreak acts as a perfect example of this. Of course, every IT admin knows the importance of patching, but it can take longer when it comes to remote devices and some businesses struggle to push patches to the right devices at the right time. Businesses need to have a specific plan for patching remote devices and a solution that can roll out patches, compliance and access rights in an automated fashion regardless of device location. With the number of endpoints showing no signs of slowing down and IDC predicting there to be 55.7 billion connected devices in use by 2025, we need to be careful of the potential consequences and ensure that businesses have an effective endpoint management plan in place. Organisations can't rely solely on the security they had in place inside the corporate office. We need to evolve our approach and leverage automated endpoint management plans when it comes to the remote workforce and remote devices, to ensure that businesses have visibility, robust regulatory compliance and security no matter which device employees are using and wherever they may be. ■

Why cybersecurity needs to address gender disparity

By Heather Hinton, chief information security officer, RingCentral

We have passed the two year anniversary of Covid-related lockdowns in the UK and businesses have continued operating through a hybrid working environment. Many companies are going back to a full in-the-office mode, while Apple for example announced that employees will return to the office three days a week from April. Cybersecurity issues remain a key focus for all businesses, with increased emphasis for those businesses that will operate partially remotely. Before the pandemic, most workers were on a corporate network, with limited access from a home or public network; during the pandemic, almost all users were on a home network. Now, businesses will have to deal with an almost even split of network access: home, public and corporate. However, when we look at the cybersecurity industry as a whole, the ongoing talent shortage continues to threaten efficient protection for businesses. In fact, according to recent research, cybersecurity reported its highest skills shortage on record in 2021, not to mention that there was a reported shortfall of 10,000 people a year in the UK's cybersecurity talent pool alone.

One way to address this shortfall is by correcting the evident gender disparity issues that continue to beset the industry. Recent findings showed that only 25% of jobs in cybersecurity were held by women. While there has been some progress made in addressing the disparity, such as initiatives like GCHQ's CyberFirst Girls Competition that aim to address the issue, fully correcting gender disparity in cybersecurity needs to be a priority for the industry this year.

There's a common perception that cybersecurity roles involve sitting in a darkened room as a lone ranger, working to stop the "bad guys". This may not appeal to those who are looking for a career that is more people-oriented and involves creativity, problem solving and being part of a team. Ultimately, in many cases, the gender disparity issues boil down to the industry as a whole not doing a good enough job at explaining how attractive and broad it is for potential employees, especially both early and mid-tenure individuals.

The industry must remedy this. We need to talk about cybersecurity in terms beyond the default "ransomware" and "attacker" elements. Cybersecurity roles involve a range of interesting responsibilities, including; technology architecture and product development, monitoring people's behaviour/usability, risk management and business impact as well as situation management. Cybersecurity day-to-day behaviour includes brainstorming, problem solving, collaborating, and being part of a team. Successful cybersecurity teams will therefore need to have a broad and diverse set of team members, made up of individuals who bring diverse ideas and experiences. To attract the new talent needed to be successful, we need to address the lack of women taking on roles: we need to change the public's siloed perception of a security professional.

A lack of representation can also have a knock-on impact on the products that eventually come to market. If there is no diversity in the product life cycle then organisations can fall into the trap of building products that don't meet what the market needs. Similarly, without diversity of voices in the sector, the industry could be building responses and solutions that are not up to standard in protecting all businesses and consumers. It's evident that technology will continue to encroach into our daily lives, and the industry must ensure that it is designing, and resolving, security problems that reflect how the general population thinks, works and lives. As highlighted by the World Economic Forum, a lack of diversity blinds us to the ways that cybersecurity attacks can impact businesses, as well as robbing the industry of engagement and talent from key demographics of the world's population.

If the industry lacks in different perspectives, it will become more difficult to look ahead for future threats. We must make a conscious effort to appeal more broadly to women. This is especially pertinent now, as according to the Allianz Risk Barometer, cybersecurity is becoming one of the greatest challenges of the modern digital era, with cyberattacks in the top 10 biggest risks for businesses globally. Additionally, as UK workers and businesses continue to embrace a hybrid form of working, the possibility of inefficient cybersecurity solutions is a worrying one, as 72% of businesses reported to be fighting to keep up with increased security threats that hybrid working models create.

To truly overcome the issue of gender disparity in cybersecurity and attract the diverse range of talent we need, we must commit to evolving how we are perceived. Cybersecurity professionals need to be visible, be career models, mentors and coaches, so that we can inspire others to join us. Ultimately, cybersecurity needs to promote the variety of roles and responsibilities that are available to anyone considering a career in the industry. ■

Dealing with disaster

Nobody knows when a disaster will strike, but we can be prepared. However, with so many types ranging from hacking to 'acts of God', does one solution fit all? Robert Shepherd finds out

The word 'disaster' is rather broad in modern parlance. A bad job interview, the wrong result in a football match and losing your home due to an 'act of God' are all – although completely relative and on very different levels in terms of their seriousness – seen as a disaster' to many.

It's the same thing when it comes to the IT, data and communications world. Systems can be taken out and data lost as result of anything from human error to a hurricane. The obvious answer to this is disaster recovery (DR) plan. However, with so many types of disaster ready to take aim, it's important to know what can be done about such unforeseen circumstances.

Let's get started and ask the experts how they define a recovery plan and what should be included in the package.

Greg Jones, business development director EMEA at Datto says that to address increasingly complex ransomware threats, some companies are now thinking beyond established security tools and are now building true cyber resilience. "This powerful strategy combines the practices of cybersecurity, business

"This powerful strategy combines the practices of cybersecurity, business continuity, and incident response which requires capabilities in five functional areas: identify, protect, detect, respond, and recover"

Greg Jones, business development director EMEA, Datto

"Studies show that a majority of DR plans fail when needed"

Sandeep Jandu, senior recovery specialist, Assured Data Protection

continuity, and incident response which requires capabilities in five functional areas: identify, protect, detect, respond, and recover," he adds. "These capabilities cannot be purchased, they need to be built by combining people, processes, and technology. With the right cyber resilience capabilities in place, companies can protect themselves from unknown threats, minimise the impact of attacks, and reduce downtime."

Jones also says that "recovery needs to start before an attack takes place". To that end, he says it's critical for companies to evaluate their IT and security budgets to ensure that they're able to implement advanced security and data management capabilities. "This will allow them to effectively back up and secure networks, while enabling business continuity capabilities. Having a business continuity and disaster recovery solution in place is the most effective solution for preventing the loss of data following an attack, as it provides the ability to quickly retrieve data and avoid costly downtime."

More on costs and budgets later, but Russ Kennedy, chief product officer, Nasuni says the DR package should reflect the current environment and prioritise the systems and data that need to be restored first to return to normal operations. "The plan should also be tested regularly and updated as environment and business priorities change," he adds. "For file data, organizations are turning to the cloud to provide flexibility for their disaster recovery plans and to minimize the cost and still meet the RPOs and RTOs associated, required by their business. Being able to save versions of file data in the cloud with sufficient granularity and recovery speed is why these organisations are modernising their DR plans."

A DR plan can consist of many things and recovery of IT systems is only one part of that, according to Sandeep Jandu, senior recovery specialist, Assured Data Protection. "The key parts of any plan should include contact details for staff and external organisations, what protocols and procedures need to be done in the scenario, expected order of events and expected timeframe of which things should be done, if staff relocation is in order, how will this happen and where do they need to go," he adds. "A complete DR plan looks at all aspects of a DR scenario not only within IT but as an organisation as a whole. One of Assured Data Protection's strengths is that we can cater for multiple different scenarios."

I don't profess to be an expert on disasters of any type – if I was, my career path to date would look very different to how it does now – but surely the recovery process is different depending on the type of attack (IT failure, natural disaster, terrorist attack, sophisticated hack)?

Jones puts me at ease immediately. "Absolutely," he says. "The disaster events differ in their durations, area and scope. Disasters can and do affect disaster recovery infrastructure as well as the production. That is why it is important to have a multi-tier strategy in place."

He also shares an example as to where a single server can be recovered on local disaster recovery infrastructure, i.e., purpose-built disaster recovery appliance, Datto SIRIS. "Yet, the hurricane may wipe out the entire data centre, including local disaster recovery systems," he continues. "For major area disasters the business must have a remote, cloud-based disaster recovery solution, located at least 100 miles from the production. In case of malicious actions like a terrorist attack or a hack, the recovery process would also include security-related actions to eliminate potential sabotage of the backup and disaster recovery infrastructure, i.e., injection of backdoors and time-triggered malware."

Kennedy adds that organisations need to plan to address natural or malicious disasters with a key focus on restoring the organisations IT systems to full production as quickly as possible. He says that in the case of disasters impacting their file data, whether natural or malicious these organisations need to quickly identify the cause of the disaster, mitigate the impact of the disaster and restore the environment to full productivity with minimal impact on their users.

"Recovery point objectives (RPOs) and recovery time objectives (RTOs) are the crucial key requirements and metrics when developing disaster recovery (DR) plans and strategy," Kennedy continues. "The difference that cloud file storage makes is that CISOs and IT teams can take a surgical and less labour-intensive approach to meeting these requirements: if there is an attack or disaster incident, they can simply dial back their data volume to a point immediately before files were lost or corrupted and achieve an up-to-the-minute recovery point. Second, IT teams can focus on restoring

only the files that have been affected vs. combing through the entire volume. In most cases, end users will never know an attack happened."

When it comes to dealing with disaster, Kennedy explains how Nasuni has supported several companies with global operations to recover their business-critical data. He says serious cases included an organisation that faced a ransomware attack on its core data centre infrastructure but was able to recover within one weekend using file restoration. "In another incident, a company executive told us that when mitigating a ransomware attack on its systems, their biggest concern was locking down infected workstations and preventing users getting re-infected," Kennedy continues. "The executive noted that file restoration from Nasuni snapshots worked perfectly, bringing all the organization's data back online and intact. Customers have reported to us that due to power situations they have lost locations in their enterprise, but users are still able to access their data." He says this was due to Nasuni's unique architecture where the "gold master" copy of the data lives in the cloud object storage solution and each location has edge devices that provide access to the data and cache a copy of the active data locally.

There are also some steps businesses can take to minimise their chances of being hacked or losing data. "The 3-2-1 rule is an easy rule of thumb for a resilient backup strategy," adds Jones. "You need at least three copies of a backup, two of which are in different locations, and one of which must have protection against destruction (immutable). This immutable copy of the backup means you will always have the ability to restore backups after an attack, despite the attacker's best attempts to destroy them."

While it's heartening to learn that a plethora of vendors are ready and waiting to help your enterprise should disaster strike, these services aren't gratis. So, in very stark terms, what if you don't have, for want of a better expression, the protection money?

Kennedy claims Nasuni is the only primary cloud file storage solution with the in-built ability to recover file shares from a ransomware attack or random disaster within minutes at no extra cost. "We believe that organisations shouldn't have to choose between protecting their company's file data and their IT budget," he adds. "Using cloud file storage, file data in use at all locations can easily be restored at a fraction of the time compared to traditional backup systems."

Jones says there are an amazing number of great technologies and services to help build security and cyber resiliency. For example, he says MSPs and SMEs can purchase an endless number of products or services, including hardware, software, or outsourced services. "Much of the technology that was once only available for enterprise organisations are now accessible and affordable for SMEs," Jones continues. "However, rushing to buy such technology and services is not always the best approach when building cyber resiliency. As an MSP or SME, it is important to first discover and identify gaps within your cyber resiliency plan and/or framework. Start with people then move onto processes before looking into technology and services." However, Jones says there's an element of caveat emptor.

Jandu's analysis is pretty blunt: "Seeing that data is the lifeblood of most organisations, and the loss of your data or access to your data would affect the running of your business, we suggest that you beg, borrow and steal from other budgets in order to ensure you have a good backup and DR strategy in place," he says. "There are cost effective solutions out there that you can employ, but the adage of you get what you pay for comes into play - especially when it comes to dealing with a data loss scenario that involves a ransomware attack. The key thing is ensure that your backup data is immutable, and whatever DR plan you put in place that you test it on a regular basis. Studies show that a majority of DR plans fail when needed."

Whatever the budget you have ringfenced for DR Jones would like to impart "a word of caution" to any enterprise or network manager charged with protecting data.

"Don't rush into buying new technology just because it's in the security category, as this can sometimes hinder building true cyber resiliency," he concludes "Only after gaps have been found and identified should the right technology be purchased."

Overall, a good disaster recovery plan reflects the current environment and prioritises the systems and data that need to be restored first to return to normal operations. The plan should also be tested regularly and updated as environment and business priorities change, according to Kennedy.

"For file data, organizations are turning to the cloud to provide flexibility for their disaster recovery plans and to minimize the cost and still meet the RPOs and RTOs associated, required by their business," he adds. "Being able to save versions of file data in the cloud with sufficient granularity and recovery speed is why these organizations are modernizing their DR plans."

Unfortunately, as Jones says, sometimes disaster must strike first before you start to invest. ■

"In most cases, end users will never know an attack happened"

Russ Kennedy, chief product officer, Nasuni

Teaching with new technology

World renowned Eton College moves from a wired network to wireless infrastructure, while Devonport High School for Boys looked to more comprehensive network coverage

Eton gets high performance campus Wi-Fi upgrade

As a boys' boarding school, Eton College is home to 1,300 students who join at age 13 and continue until age 18. With teaching staff also living on campus, school operations never stop. Eton has four hundred buildings and all major technology systems, school-provided desktop computers, laptops, and audio-visual equipment are connected via the core network that also powers Eton's wireless infrastructure.

In the past three years, boys have increasingly arrived at Eton with multiple devices— usually a minimum of laptop, tablet, and smartphone—and they expect a robust wireless network. Delivering high-quality Wi-Fi across many different environments on campus is challenging. Students and teaching staff need reliable connections in both classrooms and boarding houses.

With a cloud-based Virtual Learning Environment, use of video and wireless in classrooms, online access to college systems and an IP phone system, Eton College required a high-performance wireless infrastructure.

The wireless network originally started with 100 access points, but every boy has his own room so the number of rooms, walls and doors makes it difficult to deliver uniformly good coverage and high capacity.

Eton also has rigorous privacy, security, and online safety policies. Its robust physical security network includes networked video surveillance cameras, and it recently enhanced already-strong online safety measures in line with recent government requirements to protect children from harm online—including cyber bullying, pornography, and the risk of radicalisation.

As Intec Education expanded the wireless network from 100 to 700 access points, growing volumes of high-speed wireless traffic taxed the existing wired infrastructure so the company implemented Ruckus ICX® Switches to relieve bottlenecks and ensure high-speed connectivity for wireless traffic across campus. Deploying Ruckus Cloudpath software for online security and policy management enhanced online security and iboss Cybersecurity ensured uniform protection across network and cloud deployments.

Eton College now has a strong, reliable Wi-Fi network, meaning that boys can quickly connect to Office 365 and work. Faculty and staff can work without being slowed by their network, supporting Eton's mission to provide a broad-based education that enables all boys to discover their strengths and make the most of their talents within Eton and beyond. ■

Adapting through adversity

Schools have faced enormous challenges in the past 24 months in delivering learning. As educators look to make up for lost time in the classroom, these pressures have changed but their seriousness has not abated. We are now very much in a position where digitally enabled hybrid learning is less a nice to have and more a cornerstone of curriculum delivery. Nowhere is this more evident than Devonport High School for Boys. Having embarked on a mission to rapidly roll out the digital delivery of teaching in the last seven years, the school needed a wireless infrastructure that could enable their ambitions for a serverless school that delivered cloud-based, personalised learning that supported students into further education or apprenticeships.

In a school where nine in I0 students have their learning delivered via their own dedicated Google Chromebook, being able to get online was a priority. However, with the previous wireless architecture delivering connectivity to less than two-thirds of the school, the network was not providing the comprehensive coverage the teachers required.

In making a change, Devonport School did not just want to meet their network needs today, they wanted to get ahead of

"The new network has improved the seamless delivery of teaching, underpinned the running of the school, and the ease of management means that staff can troubleshoot basic problems themselves without expert knowledge. Thanks to Cambium Networks and Magicka the school can confidently guarantee that students can take their exams online, and it will open up new learning opportunities that will enrich our student's learning for years to come"

Nick Berryman, assistant headteacher, Devonport School for Boys

future requirements. Technology such as interactive white boards were already being used widely across the school, mobile applications for administration were becoming commonplace, and Devonport's leadership team were alive to the potential for AI-enabled teaching delivery in the future. Moreover, with the Department for Education pushing more and more exams online, it had become critical to the success of students that the school had a robust network, capable of supporting multiple users in the same room(s), all at the same time.

The school also opens its facilities to organisations in the local community, allowing them to host events. In such instance, these organisations and groups often need internet access to run their event. This meant that the network not only had to be robust, but also easy to manage to allow for the seamless granting and removing of access.

Moreover, the pandemic brought with it the unique challenges of remote and hybrid learning. Not only did teaching need to be delivered digitally, but the operations of the school, parent's evenings, and governor's meetings all had to move online.

Finally, amongst all of this, the UK's education sector faces strict budgetary requirements. This means that the potential of every pound spent to enrich the student experience and deliver better learning has to be maximised to the fullest. As such, a solution that delivered robust high performance and value for money was needed.

The school uses what was the Stoke Military Hospital in Plymouth, which given its previous purpose has incredibly thick walls which do not make for an ideal Wi-Fi environment. It also means the classrooms are spread across four main buildings, plus additional outbuildings. As a result, making sure that each classroom had the connectivity it needed was not straightforward. To ensure the best possible ROI, Magicka opted for a primary fibre ring around the school site and gave each block up and down back up for added resilience. Due to the thickness of the walls, the site survey showed that every classroom would need its own access point. In total, 131 access points were installed across the school. Cambium Networks XV3-8 access points were chosen to deliver Wi-Fi 6 connectivity in high bandwidth areas, with XV2-2T0 Wi-Fi 6 access points being used outdoors. Across the rest of the school, XR-320, XD2-230, XD2-240, and XD4- 240 access points were used. The school also installed 37 switches, choosing from the EX2010-P, EX2016M-P, EX2028-P, AND EX2052-P models to provide a resilient backbone for the network.

It was crucial that the network was easy to manage and that problems could be resolved quickly. The network is managed using Cambium Networks' XMS-Cloud Management platform, which means that any issues can be highlighted and dealt with quickly whilst guest assess can be easily granted and removed from anywhere by the Magicka team. In fact, the network management is so simple that members of the Devonport School staff also have access and often troubleshoot network issues themselves. This is made even easier by the zero-touch configuration of Cambium equipment, allowing faulty access points to be swapped out without expert technical knowledge.

Thanks to having a robust network infrastructure, the school was able to have full confidence in its decision to become completely cloud-based, realising its ambition to become a serverless school. The upshot of this over the past two years has been immeasurable, as this flexibility allowed the school to quickly pivot between remote and hybrid learning in a way, they would not have been able to do before. In the long term, this flexibility will ensure that children don't fall behind if they are off ill for extended periods of time or if the school has to close due to snow or bad weather. Connected learning is also opening up opportunities for schools and trusts to join together to optimise their individual specialisms. This means that schools will be able to offer high-quality teaching across a broader range of the curriculum, providing a major benefit to students.

As well as learning, the management of the school is also now able to be done remotely. Instead of holding socially distanced in-person meetings, everything from governor's meetings to the school's financial operations were organised remotely.

With robust connectivity, the experience during lessons is seamless with no breaks that might cause disruption. Class registers can be taken on laptop or mobile devices and the student's work is easily shared to internet connected whiteboards to inspire further discussion and learning. In future, the network will also be ready to support applications such as virtual reality, for subjects such as Design & Technology or the sciences, where 3D modelling will help students gain an even greater understanding of the subject. ■

The benefits of visibility for IoT and OT security

By Anthony Brown, director, Gigamon

In this article, Anthony Brown of Gigamon looks at what challenges arise when operational technology converges with the IoT. He suggests that without a deep layer of observability into all data in motion, security along with performance will suffer significantly

Internet of Things (IoT) and Operational Technology (OT) devices are becoming invaluable in modern times, as they allow organisations to improve their product and service quality, reduce operational costs and increase workforce productivity. A new forecast from IDC estimates that there will be 41.6 billion connected IoT devices, or "things," generating 79.4 zettabytes (ZB) of data by 2025, while for enterprises in the manufacturing and logistics environment, OT-based automation has been invaluable for a number of years already. As OT, IT and IoT systems continue to converge, more proactive maintenance and critical infrastructure monitoring has been made possible and businesses are becoming increasingly agile.

However, many OT environments were designed with no intention of being connected to a wider IT environment and therefore threat analysis was never a top priority. What's more, these networks cannot cope with the data deluge produced through threat monitoring processes and patching is often difficult. As inherently more vulnerable, OT and IoT networks have therefore become an attractive target for hackers and this risk is only growing as adoption increases. Without effective monitoring and management driven by visibility, malware, ransomware and data breaches are becoming a significant problem across these networks and its essential organisations understand how to better protect their devices moving forward.

Gaining a clear, singular view

It is impossible to manage and protect what you cannot see, and visibility across IoT and OT networks is integral. Enterprises must ensure they have a clear view into the number of authorised (and unauthorised) devices across their IoT network, where these devices are located, whether they have the latest patches and how often they are utilised. It is also important to gain sight of which servers each device communicates with and whether any part of the chain may be vulnerable to malicious actors. In order to gain this level of visibility across systems with varying security capabilities, it is important that security issues are addressed within the network and not at each end-point.

To completely eliminate blind-spots, a single pane of glass view into all environments from cloud to on-premises is the best option. This means there will be no piecing together of individual tools as NetOps teams hope not to miss anything, and all devices, data and dangerous actors can be in sight at all times from one integrated platform. This holistic view into environments should also include the ability to capture traffic that is flowing from IoT devices into the cloud, as well as east-west traffic across IT networks.

Eradicating these blind-spots is critical in an age in which ransomware poses one of the largest threats to businesses. While IoT might not offer the access to the wider IT system at the moment, the threatscape is fast-moving and businesses must make sure they are ready for criminals to switch their tactics. This is particularly pertinent given that adversaries have changed the way they deploy ransomware dramatically over recent years; rather than a 'spray and pray' approach with little skill involved, cybercriminals will carefully target vulnerable organisations and lay dormant on their network for months on end. In fact, the latest stats demonstrate that network dwell time for these criminals averages at 285 days. Therefore, to best protect OT and IoT devices from the evolving threat of ransomware, it is clear that end-point detection alone is not sufficient. Instead, a deep level of observability into all traffic is integral.

Optimising data

Delivering increased visibility not only supports IoT and OT security, it also enables organisations to better scale and boost service performance. Observability into these networks will allow operations teams to recognise whether the right data is being directed to the correct tools, or make changes if this is not the case. Integrating de-duplication processes can reduce the amount of unnecessary traffic running past security monitors in order to prevent packet loss and avoid expensive maintenance or upgrade costs. A significant amount of investment can be saved for organisations over-spending on tool upgrades, when instead traffic reduction techniques can better optimise their IoT network and devices. Given the financially challenging environment that has continued to dominate business decisions over the last 12 months, solutions that reduce costs and simultaneously bolster cybersecurity are likely to be well-received by the board and will be essential to industries leveraging IoT and OT devices daily.

OT systems are increasingly under threat due to the deployment of IoT devices, yet these converged environments spell the future of agility and productivity in enterprise. The foundation for solving security challenges has to be network visibility; a clear view into the traffic created by IoT and OT devices not only means that threats can be continuously monitored, but performance can also be optimised. The risks for organisations leveraging IoT networks should not be underestimated – yet with the right processes and tools in place, they can be a simple hurdle to overcome. ■

"This is particularly pertinent given that adversaries have changed the way they deploy ransomware dramatically over recent years; rather than a 'spray and pray' approach with little skill involved, cybercriminals will carefully target vulnerable organisations and lay formant on their network dwell time for these criminals averages at 285 days"

A mission critical comms revolution

By Paul Ward, director of international commercial and marketing, ETELM

Private 4G/5G communications offers an exciting opportunity for mission critical users – the move towards high-speed broadband services will enable new, advanced applications and offer significant operational improvements for users. However, there will still be a demand for traditional PMR technologies…. so can the industry gain more than just the improvement in data services?

ETELM has long been providing mission critical infrastructure, specialising in TETRA, more recently our own LTE RAN and an advanced Hybrid TETRA & LTE system called 4G Linked. Having developed our new range of mission critical LTE base stations it became clear that the powerful 3GPP Core networking standards could (and should) be used for all communication technologies across the sector.

Traditional narrowband PMR technologies will be required well into the future…affordability, spectrum availability, cell coverage and re-use of existing subscriber equipment are issues that need to be considered. We believe that a hybrid approach to technologies is the ideal solution to allow users the best choice; and a fully integrated, single network solution will always be more cost effective and a better solution than gateways to separate networks.

The TETRA standard was developed over 20-years-ago and a major benefit was the interoperability between subscribers from different manufacturers. However, interoperability at infrastructure level was never fully implemented by vendors. This proprietary issue created difficulties for users; it was particularly restrictive for governments deploying large national TETRA networks and they were locked into single sourcing which limited options and stifled competition.

In the UK, ESN wants to move from a long-term managed service contract [Airwave], paying per subscriber for what is essentially proprietary system. Migrating to a new technology at a national scale is always going to be complex, but for ESN it has been extremely challenging as it moves from a proprietary network and an exclusive operator. Although moving to broadband services was the correct decision, initial timescales were over optimistic and based more on commercial pressures (due to fixed monthly fees) rather than realistic availability of technology. Although the new MCX standards for LTE have developed at pace, they were never going to meet the initial ESN deployment plans to start replacing Airwave in 2019, making delays inevitable. However, the MCX standards have matured rapidly and the benefits will no doubt soon be realised.

Supplying infrastructure for security and public safety means collectively working towards a future where customers are not left locked-in to a supplier or service – and we have a responsibility to ensure migration paths are more seamless and less complex than they are currently.

Different technologies can inter-operate on the same core network, reducing costs and increasing options for users, while simplifying the architecture by avoiding gateways and separate interfaces. ETELM's 4GLinked TETRA base station can co-exist with eNodeB's on the LTE core network….so how can we take this opportunity to revolutionise how vendors of different technologies co-operate in the future?

The technical solution is possible and lessons can be learnt from the network standards established by 3GPP for the mobile consumer market – the 4G and 5G Core network is internationally standardised and all base stations from different vendors inter-operate on the same network. Operators can select suppliers based on a competitive market and the ability to switch suppliers quickly should the need arise. This competitive approach has been a major factor in the rapid rate of deployment and technology advances in the consumer communications market.

All infrastructure manufacturers can adopt the same approach and develop their technology into the 3GPP standards for core networking – creating a single eco-system for all communications technologies and allowing users to select and mix technologies based on cost, service and user requirements. ETELM's TETRA eNodeB's demonstrate this approach as they can connect directly to any LTE Core network in the same way as any LTE eNodeB, by utilising the LTE-S1 connectivity standard. This allows our TETRA system to be deployed over the same, single network core solution alongside 4G and future 5G base stations. The solution has been successfully tested at 3GPP Plug tests and already deployed in numerous scenarios for emergency services.

3GPP's 4G and 5G networking standards are open, so any vendor can develop the same solution into their base stations. It means we can all benefit from the advances in core networking and allow inter-system and inter-technology solutions over a single core. The technology is available but commercial barriers remain – this is where users can influence vendors and ensure that they never find themselves locked-in to proprietary networks. ■

UCaaS has emerged as the answer to the post-pandemic hybrid working challenge

Courtenay Mills, head of voice and data for EfficiencyIT

In a world of post-pandemic upheaval, two work-based mega trends are becoming increasingly clear – cloud is king and hybrid working is here to stay. The latest research from the Chartered Institute of Personnel and Development reveals that a growing number of employers are reporting significant productivity gains as they embrace cloud-powered work-from-anywhere models. But moving your comms to the cloud, or switching to Unified Communications as a Service (UCaaS) can be a daunting prospect, with a myriad of vendors selling a multitude of solutions with varying levels of service.

The following checklist will help you navigate the complicated UCaaS landscape and find a solution that will not only serve your business well for a decade or more, but transform your customer and employee experience levels. All while reducing costs, optimising budgets and seamlessly integrating key business-critical systems and software applications in the process.

1. Empower your employees to work from anywhere

Having lived and worked through two years of lockdowns, social distancing and the move to home working, UCaaS platforms not only have to be disaster proof they need to support the move to hybrid working. This means switching key communications channels to the cloud so that dispersed teams not only have a full set of communications and collaboration tools at their fingertips, they are fully engaged and they are empowered to be as productive as possible. In this environment purchasing the right UCaaS platform will not only boost productivity, it will also help companies improve their recruitment and retention figures and ultimately win the race for talent.

2. Provide a single pane of glass

Today's workforce wants to hold multiparticipant video calls, share documents in-call, send emails and communicate via instant messaging – to name but a few channels. The most effective platforms do this through one unified dashboard (also known as a 'single pane of glass'), reducing complexity, accelerating workflows and boosting user experience. Another important consideration is whether the vendor owns the full tech stack or whether they manage a series of third-party solutions. If this is the case, and they're managing third parties there is the very real possibility that one of their providers could withdraw its application at some point and your business service levels could be negatively impacted.

3. Achieve seamless integration with key business platforms

Flawless communications are a key requirement for best-in-class UCaaS platforms, but your wish list should not end there. Market-leading solutions now also integrate business-critical apps, such as accountancy software, CRM and ERP out of the box, with automatic field population being the watch words. This fast and seamless integration speeds up employee workflows and accelerates productivity. It also means there's no longer the need to hire costly middleware developers to integrate complex systems.

4. Secure the right service and support levels for your business

Big businesses hardly ever sleep, and with technologies connecting employees and clients across the globe, any system downtime can fast become problematic for your business. As such it's essential to choose a UCaaS vendor with 24/7/365 support as standard. It's also wise to take a similarly risk-averse attitude to data centre availability. If your vendor does not have a data platform collocated globally it's doubtful there will be sufficient redundancy if one data centre goes offline.

5. Insist on vendor-backed SLAs

Many market-leading UCaaS vendors will also offer a "five nines" service level agreement. In other words, they promise that their service will remain fully operational for 99.999% of the time. Such agreements have very little value, however, unless they are financially backed by the vendor, meaning they will compensate you if they fail to meet the five nines standard. This is a must for any business selecting a UCaaS solution.

6. Ensure your vendor has regulation and compliance covered

Regulation and compliance are business-critical, and too complex to discuss in detail here. Needless to say different industry sectors in different geographies have their own specific challenges. The ideal solution is to find a UCaaS platform that takes responsibility for ensuring the activity on its platform is compliant. For example, this may involve ensuring on-platform customer data handling complies with GDPR or payment information held on the system is PCI-DSS compliant.

7. Resist the urge to be primarily price-driven and do your due diligence

Get UCaaS procurement wrong and it may cost your company dearly for the life of your licencing agreement. Get it right, however, and it can prove to be truly transformational on a business-wide level. As with all IT procurement exercises, due diligence is essential. Armed with our seven-point checklist, however, it is possible to thoroughly interrogate the market and find the perfect UCaaS solution for your business – one that will flex and scale with your needs and potentially deliver 15 to 20 of years of service. For further information, visit https://efficiencyit.com ■

PRODUCTS

BT Cloud Work is a cloud-optimised, mobile-first cloud communications platform for voice, video meetings, messaging, fax, presence and team collaboration. The telecom giant says with this solution, "you can future-proof your communications while maintaining tech stack freedom and optimising total cost of ownership on your traditional phone systems". What's more, the company says BT Cloud Work allows you to unify all your communications services on a single platform. This allows the enterprise to access "the same powerful features from any device". Also included is the ability to seamlessly integrate BT Cloud Work with all your critical business applications and cloud services. BT also says worry not about audio quality – "your calls will be the top priority for your network's bandwidth. And BT Cloud Work's online portal lets you monitor network performance 24/7 with service reports". *bt.com*

Vodafone Business UC with RingCentral is described as "a flexible unified communications solution, enabling more efficiency and control for businesses". All communication streams are merged into a single, manageable platform, combining phone video messaging and file sharing from anywhere, and so much more to support business and employee needs. With 99.9% uptime and in-built security, the solution promises an enterprise-grade service.

As well as flexibility on features and subscriptions, the solution integrates with current infrastructure, integrating with existing collaboration, CRM, contact centre and cloud applications simply and securely. The technology supports business preferences, working to deliver a seamless working environment that encourages continuity and collaboration. Every feature and service on Vodafone Business UC can adapt to how the business and customers work best, helping to boost productivity and support. The platform offers customers the ability to scale depending on their needs while also addressing a variety of specific industry needs. Some of the features include; real time analytics to see how the team is collaborating, a corporate directory that is automatically updated and accessible to all users, a built-in call log to make it easy to search calls by duration and call type and role-based access permissions so new roles can be assigned at just a click. What's more, employees can seamlessly switch between mobile and desktop devices, and get a consistent experience on any device, no matter where they are.

The business will be given access to a network readiness assessment, a dedicated project manager and a comprehensive site analysis to ensure that the launch goes smoothly and they make proper use of their needed feature plan. *vodafone.co.uk/business*

The Jabra Evolve2 65 Wireless UC Stereo Headset with Link 380c, Jabra says, provides "better calls and seamless collaboration".

"We've made the incredible call performance of our world-leading Evolve series even better, with an advanced digital chipset that's three times more powerful and three strategically placed professional microphones," the company further claims.

What's more, Jabra reckons the powerful leak-tolerant 40mm speakers and its most advanced digital chipset ever, deliver "outstanding audio that always keeps you in the loop".

The headset comes with isolating foam oval ear cushions and what Jabra describes as "pioneering new angled earcup design work to effectively block out your surroundings, giving you passive noise-cancellation". What's more, the firm reckons the advanced battery efficiency technology and aforementioned new digital chipset "have helped us to squeeze a full 37 hours of juice from this powerful wireless headset". There's also an optional charging stand – just in case. *jabra.co.uk*

8x8 Work is a cloud-based app that brings together voice communications, video meetings, and team messaging on your desktop PC or smartphone.

Use 8x8 Work to bring integrated communication and collaboration experiences securely to every employee, with the convenience to do more from anywhere on any device, building relationships and inspiring customer trust.

Create a networked organization without silos and gain data insights across multi-modal communications to make routine decisions seamless.

With 8x8 Work, manage and scale your business communications from a single administration interface that simplifies user provisioning and management.

Give your users the best voice and video quality so they can connect and communicate with co-workers, customers and suppliers with full confidence.

Built on an open cloud communications technology platform, 8x8 Work integrates with today's leading business applications, providing a consistent unified experience that today's modern workplace culture demands. *8x8.com*

Please meet...

Jon Fielding, managing director, EMEA, Apricorn

What was your big career break?

Moving into electronic payments and Public Key Infrastructure off the back of the Identrus(t) scheme when at IBM in the mid-90s. I ended up working on a huge global deal for a large bank where we needed to bring in a number of complementary technologies, most from pre-IPO start-ups as it was fairly cutting edge at the time. This opened the opportunity to consider a radically different work environment and, after 10 years at IBM, I felt the time was right to take the plunge and work one of these "new wave" businesses. This led to a number of first man on the ground in country/region roles; all of which have been great fun and packed with wonderful memories and experiences, leading up to where I am today.

Who was your hero when you were growing up?

As a Manchester City fan, I idolised the late, great Colin Bell. I'd just started going to football and Colin was in a different class. Unfortunately, he was badly injured a couple of seasons later and was out for quite some time. I can still remember the crowd noise on his return, but he never fully recovered to the player he once was. I suffered some barren times in those early years and beyond. However, I now feel privileged to watch an exceptional team, both footballers and managerial staff, and can see some of Colin's attributes in different players – Rodri/Bernardo's work rate and De Bruyne's vision for example. We still sing his name

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

Trust in you. That's not to say don't trust anyone else, but you need to back yourself first. I find myself passing this onto my kids now. Reminding them to have faith in themselves, bear in mind positive past experiences, trust in their gut and, 9 times out of 10 (or hopefully more), they will make the right decision for the right result.

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

"Have you ever skinned a buck?". I was 17 years old and travelling through Canada and America. I ended up in Atlanta staying with family friends and we went to an Atlanta Braves baseball game. Half-way through, a man in the seat in front of me, and with whom I hadn't had any previous conversation, turned round and asked, "Have you ever skinned a buck?" before turning back to his friend to continue their discussion without waiting for a response. I sat scratching my head for some time after. The answer, then and now, is of course "No!"

What would you do with £1m?

I would put it towards helping my kids buy their first homes. I have 4, so the £1m is easily spent. With the current state of the housing market, I'm not sure how else they will ever be in a position to own their own home before middle age at the earliest.

If you could live anywhere, where would you choose?

My wife would say Majorca, I'd say Portugal – so Majorca it is! To be honest, that would work for me too. We enjoy visiting both, as well as the Greek islands. We have simple tastes – sun, beach, relaxed way of living and good food.

The Beatles or the Rolling Stones?

Both are great and have influenced a lot of the music I like but, if pushed, I would have to go for the Rolling Stones

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

Mobile catering – I've always fancied the idea of setting up a food truck that serves up high-quality food that is slightly different from the norm, then travelling round, building a loyal following and having fun - like in the film "Chef".

What's the one thing you must do before it's too late?

I often promise myself that, one day, I will learn to play the drums and join a band. I don't have a musical bone in my body in terms of pitch, melody etc. so reckon drumming is my best bet. I'd hope to be the sort of drummer that is able to contribute equally to the overall song rather than just keeping time – think Dave Grohl, Reni, Matt Helders. ■