www.networkingplus.co.uk

OCTOBER 2019

networking

FIXED & WIRELESS NETWORKS FOR ENTERPRISE USERS

UK firms seal new investment
Lima and Data Centre UK backed in £12m deal
News, p2

'Emergency' upgrades for IT
Major makeover puts services back in action
Real World Networks, p9

Shining a light on the dark web
Robert Shepherd looks at the potential threats of the dark web
Feature, pp11-13

Confound the crooks
Foil the hackers with these products, plus top tips from an expert
Off-the-shelf, p14

UK government unveils £5bn funding for broadband plans

Chancellor of the exchequer Sajid Javid has announced a £5bn funding package to enable the introduction of gigabit-capable broadband in remote parts of the nation.

Ensuring that all parts of the UK are covered by next-generation broadband, the new funding initiative will also target the hardest-to-reach 20% of the country.

The government said the latest funding announcement doubles the previous commitment to support the rollout of internet technology to the hardest 10% places.

However, it added that the monies will not be used on fibre broadband, but for the launch of full-fibre, 5G and other gigabit-capable networks.

"This new multi-billion-pound investment to deliver gigabit-capable broadband for all the UK and investment in roads and buses will help people to get around and businesses to grow, ensuring no community is left behind," Javid said.

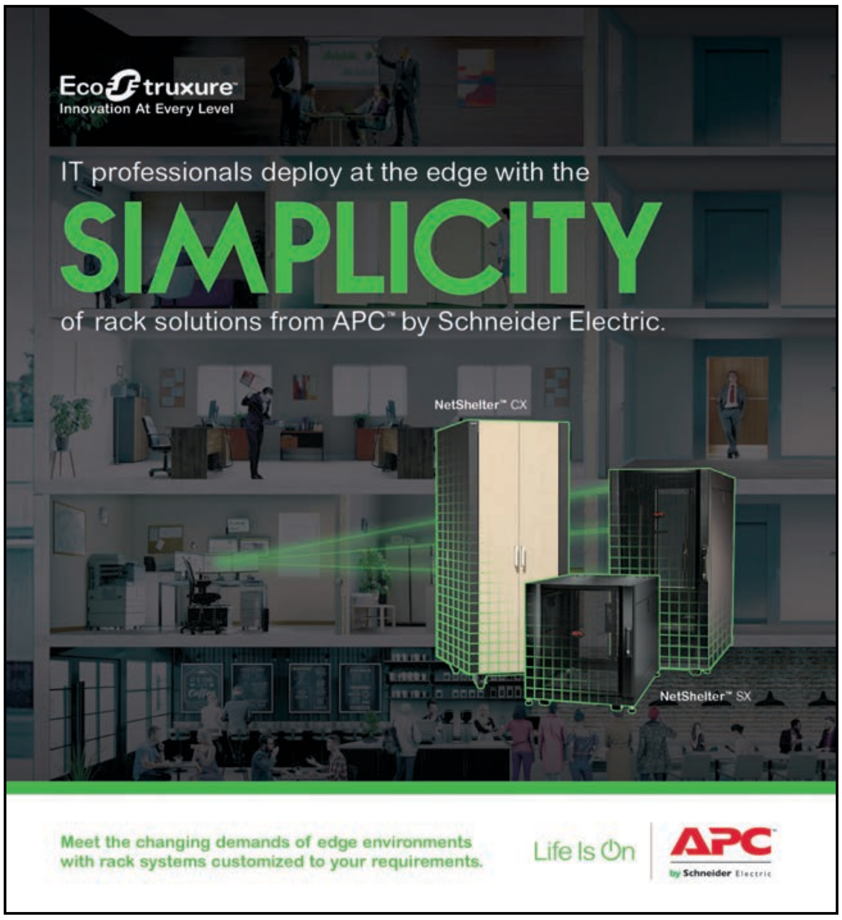
Furthermore, the gigabit broadband initiative is part of a suite of measures announced by the government to support the next generation, foster economic growth and prepare the country for when it jettisons the European Union.

Secretary of state for Digital, Culture, Media and Sport (DCMS) Nicky Morgan threw her weight behind the move when she tweeted: "We want everyone in the UK to benefit from world-class gigabit connectivity no matter where they live or work, so today Conservatives are announcing £5bn to ensure our rural communities benefit too."

However, it was not just fellow ministers who welcomed the news. Tim Breitmeyer, president of the Country Land and Business Association added: "Better connectivity is key to unleashing the economic potential of the countryside and we welcome that government is listening to the concerns of rural communities," he said. Breitmeyer added that ending the rural/urban digital divide will support rural businesses to create jobs, enable people to access services and allow agriculture to embrace the technological revolution, as well as persuade more tourists to visit.

Continued on page 2

Ensuring that all parts of the UK are covered by next-generation broadband, the new funding initiative will also target the hardest-to-reach 20% of the country


EcoStruxure
Innovation At Every Level
IT professionals deploy at the edge with the
SIMPLICITY
of rack solutions from APC™ by Schneider Electric.
NetShelter™ CX
NetShelter™ SX
Meet the changing demands of edge environments with rack systems customized to your requirements.
Life Is On
APC
by Schneider Electric

Floating data centre back on track

A floating data centre in Ireland is likely to be given the green light soon after an appeal that slowed it down was withdrawn.

Shannon Foynes Port Company applied in 2018 for permission for the building, estimated to cost in the region of €35m, on part of its lands at Ted Russell Dock in Limerick.

It will be developed by US data centre firm Nautilus, which has been backed by the Irish government and would create 24 new and permanent jobs, as well as employing 100 people during the construction phase.

Conditional permission was granted in March 2019, but development was subsequently delayed by an appeal to An Bord Pleanála by a group representing businesses on the docklands.

However, Limerick Port Users Group has since withdrawn its appeal, clearing the way for the development.

One of the main issues Limerick Port Users Group had with the development was that it was not consulted about the original application, which was one of its complaints when it made the appeal in May.

In its appeal – since withdrawn, the group also expressed concern that the development would reduce the port's space and hamper future growth.

Shannon Foynes Port Company said the project was being developed as part of a regeneration programme for the area as Limerick docks had landside assets that were "surplus to traditional port needs".

It said water would be drawn from the Shannon and pass through a cooling process before being returned to the river about 90 seconds later "unchanged other than being slightly warmer".

The company said the change in temperature would be less than 2° Celsius which was well below any regulatory threshold. ■

UK government unveils £5bn funding plans

Continued from page 1

"What's needed now is for the ambitions of this announcement to be matched by detailed and technical work with broadband providers and mobile operators to turn this into a reality," he continued. "But we are on the verge of overcoming one of the largest barriers to the rural economy becoming an engine for growth and productivity."

In the summer, prime minister Boris Johnson set a target of bringing full-fibre broadband to every premises in the country by 2025. Following that announcement, the UK telecom industry wrote an open letter to him, in which it said that the goal of 100% rollout of full-fibre by that time would only be achievable with 100% commitment from the government.

The letter went on to underline four key issues – fibre tax, wayleaves, new builds, and skills – which the associations want the government to address if it has to achieve the target of a full-fibre rollout.

In July 2019, the Department for Environment, Food & Rural Affairs (Defra) said it had ring-fenced £45m funding to help rural businesses and communities get vastly improved broadband access.

Prior to that, in May 2019, the government commenced the two-year £200m Rural Gigabit Broadband Connectivity (RGC) Programme, which was aimed at delivering gigabit-capable full-fibre broadband to the most rural and remote regions in the country. ■

M247's full fibre city network

Customers of global connectivity and cloud services provider, M247, can now access ultrafast fibre connectivity directly from its own network infrastructure following its full fibre city project in Manchester.

The move has improved connectivity options for over 27,000 businesses across the city, increasing its reach in these areas by 146%. Part of a wider expansion programme across M247's UK and international networks, the project is a seven-figure investment.

The new Manchester city fibre network offers customers a new range of business internet or ethernet services with speeds up to 10Gbps and faster connection times, as well as quicker fixes and competitive pricing

Furthermore, the new Manchester city fibre network offers customers a new range of business internet or ethernet services with speeds up to 10Gbps and faster connection times, as well as quicker fixes and competitive pricing.

Exchanges have been unbundled across three key business districts in Manchester and M247 also owns full fibre access networks in London and Leeds. It is planning to roll out further city networks in Liverpool and Birmingham within this financial year.

"As businesses are increasingly adopting cloud technology, many are turning their attention to the kind of connectivity they use to achieve business grade speeds," said Jenny Davies, chief executive officer at M247. "Customers want the ability to choose which connectivity solution best fits their business needs, whether that be radio (wireless), fibre (cable) or both. Wireless connectivity will still continue to form a key part of our offering, and our Manchester city fibre network is about offering customers that choice all through one provider." ■

Lima and Data Centre UK backed in £12m deal

Managed services, hybrid cloud and data centre solutions provider, Lima Networks and Data Centre UK have secured a £12m investment from active private equity house, Maven Capital Partners.

The deal includes an equity raise from Maven, a syndicate of institutional, family office and high net worth investors, alongside debt funding provided by CYBG.

Lima Group specialises in designing and implementing "intelligent" IT infrastructure solutions across a range of sectors and industries, including SMEs to enterprise level and public sector organisations.

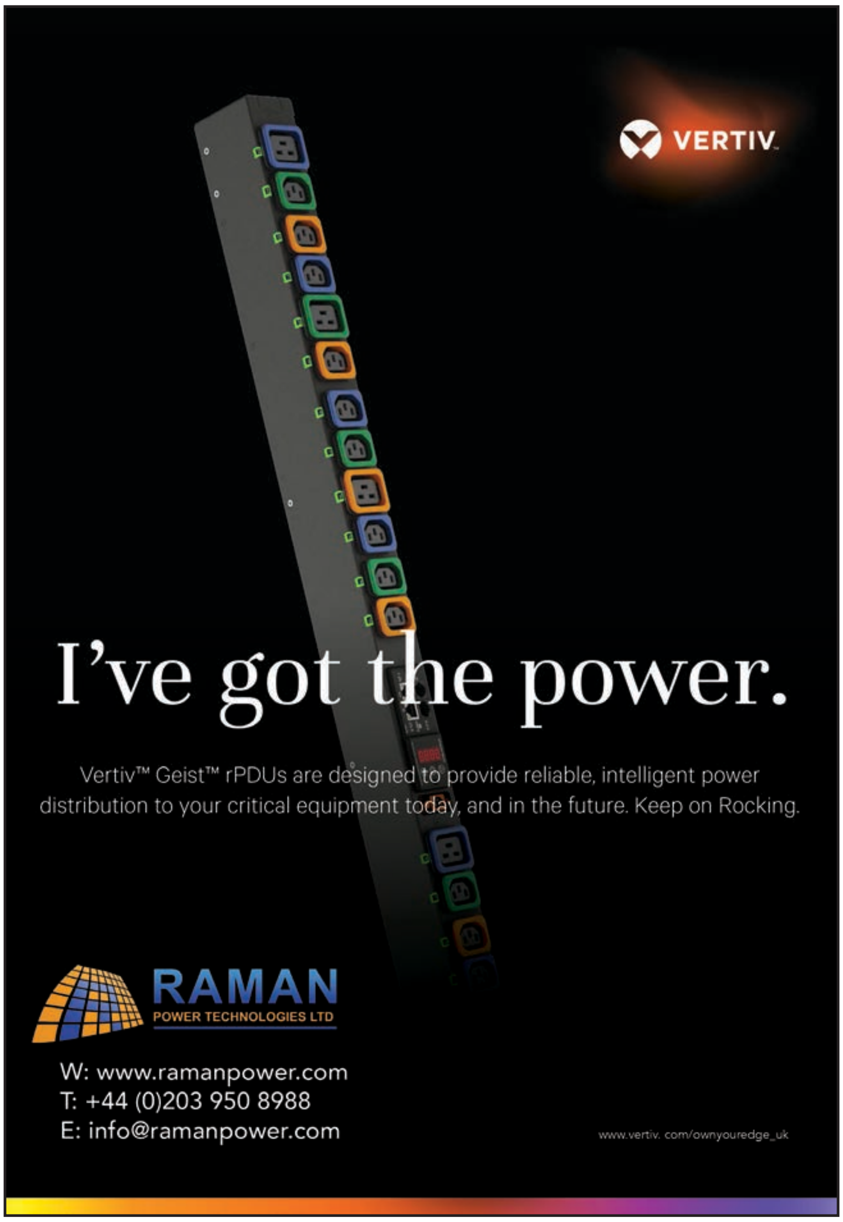
Maven's investment in Lima Group will allow the company to upscale its offering in cloud and managed services, as well as expand by undertaking selective acquisitions.

"As technology advances and customer requirements evolve, IT innovation is becoming more imperative to the success of an organisation and its future growth," said Ryan Bevington, investment director at Maven. "Lima Group is enabling its clients to gain a competitive advantage by designing and implementing IT solutions which match their organisational structure and business objectives. The market drivers for this type of specialist and highly technical service are overwhelmingly positive and Maven are excited to support the group's Senior Management Team on the next phase of their growth journey."

Lisa Thornton, chief executive officer and founder of Lima Group said Maven's culture, values and ambition for Lima "perfectly reflects" Lima's own vision for the future.

"We are extremely proud of our reputation which is thanks in no small part to a hard-working team, our unparalleled technical expertise and the refusal to compromise on quality customer service," she added. "Maven's investment solidifies our position as we now seek to broaden our portfolio and expand the business through a combination of organic growth and strategic acquisition, thereby underpinning our ambition to become the 'go to' cloud and managed service provider." ■

Maven's investment in Lima Group will allow the company to upscale its offering in cloud and managed services, as well as expand by undertaking selective acquisitions



EDITORIAL:

Editor: Robert Shepherd
roberts@kadiumpublishing.com

Designer: Sean McNamara
seanm@kadiumpublishing.com

Contributors: Gerry Moynihan, Paul Liptrot, Richard Blanford, Robert Neave, Paul Mercina, Chris Wellfair

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
www.networkingplus.co.uk

Annual subscription: £80 (UK); £95 (Europe), £100 (USA and the RoW) airmail. Cost per single copy is £8.25.

Printed in England by
The Magazine Printing Company
© 2019. All rights reserved·
ISSN No: 2052–7373

The contents of the magazine may not be reproduced in part or whole, or stored in electronic form, without the prior written consent of the publishers. The views expressed in this magazine are not necessarily those shared by the editor or the publishers.

KADIUM

Trio develop new liquid cooling solutions

Schneider Electric, Avnet and Iceotope have joined forces to jointly develop new liquid cooling solutions for data centres.

The collaboration will integrate Schneider's data centre infrastructure solutions, Avnet's technology integration services and Iceotope's chassis-level immersion cooling technologies.

Schneider's preliminary analysis of the difference between liquid cooling and air cooling found that the former could produce CapEX savings of 15%, while energy savings could amount to at least 10% – leading to a 20-year total cost of ownership savings of more than 11%.

"Compute intensive applications like AI and IoT are driving the need for better chip performance," said Schneider Electric's innovation and secure power chief technology officer and senior vice president Kevin Brown. "Our quantitative analysis and testing of liquid cooling approaches shows significant benefits to the market. This partnership is the next step in solution development, and we are excited to be working with Avnet and Iceotope."

All three companies illustrate graphical processing units (GPUs) as an example of a system that could benefit from liquid cooling power. GPUs can parallel-process a number of applications such as big data analytics and artificial intelligence.

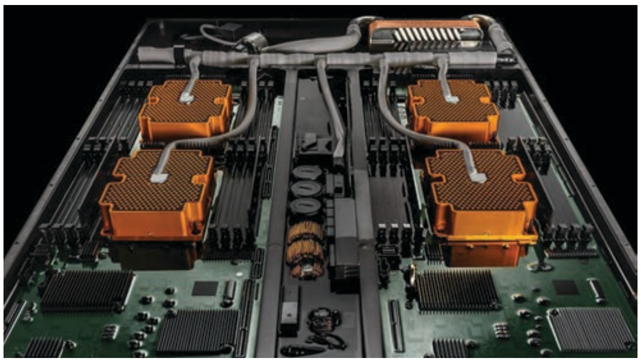
"The chips are increasingly power dense with thermal design power ratings reaching 400 watts or more. This makes traditional data centre air-cooled architectures impractical, or costly and less efficient than liquid-cooled approaches where the server is partially submerged in a dielectric fluid," the companies said.

Liquid cooling could offer solutions that are efficient, silent, resilient and compact.

"Iceotope is delighted to work with Schneider and Avnet on a solution that delivers on the promise of liquid cooling," said Iceotope chief executive officer David Craig. "Working with great partners that share the same passion for innovation, solution focused thinking and quality is a pleasure. Our ability to bring our IP to combined solutions that manage the pressing challenges of chip density, energy and water consumption, space and location challenges and the ever more complex issues relating to harsh environment and climate will be game changing in the industry."

Avnet integrated global president Scott MacDonald added that largely driven by the recent explosion of IoT, the processing power needed for workloads like AI in data centres requires advanced solutions to keep connected systems operating efficiently.

"The development of a liquid cooling technology solution offers customers the performance needed to deliver on these growing compute demands," he said. "This is a prime example of how we work with customers to provide the advanced solutions necessary to meet the needs of data-centric workloads in virtually every industry." ■



The collaboration will integrate Schneider's data centre infrastructure solutions, Avnet's technology integration services and Iceotope's chassis-level immersion cooling technologies

PHOTO: ICEOTOPE

Apple puts 'data centre plot' up for sale

Apple has put a 500 acre site in Ireland, which was being readied for an €850m data centre, up for sale.

The US tech giant first secured permission for the site near Athenry in County Galway in late 2016, but the plan was ultimately abandoned as a result of long-running objections.

In April this year, the Supreme Court of Ireland dismissed an appeal by local residents against the decision to grant permission. However, Apple had already abandoned the project by that point and concerns had been raised at national level about the implications of the case on future data centre projects in Ireland.

While local residents and politicians said they hoped Apple would reconsider investing in the area, the site is now on the market.

The *Sunday Times* said the site is a 500 acre plot advertised by agents as 'Data Hub West' – a ready-to-go data centre development site. However, there is no mention of the price tag or that the site is owned by Apple. ■

‘Enhanced connectivity could boost UK productivity’

UK businesses spanning every sector would benefit from £34.1bn in productivity gains if their workforces had better access to connectivity, according to research released by O2 Business.

O2’s Business without Boundaries: The role of connectivity in business growth report found that enhanced connectivity could deliver overall time savings of 3.14 hours per week for each employee, equating to an additional 18 working days a year and representing a significant advantage for workers and British business.

The second major study of its kind in five years, O2’s report further found that giving people the ability to work where, when and how they want can reduce time commuting to fixed places of work, enabling a more efficient use of working time.

However, since O2’s first *Smarter Working Britain* report in 2014, solid progress has been made with regards to remote working. The nation’s biggest businesses already benefit from a productivity boost of up to £10.5bn as more staff had access to flexible working – splitting their time between office locations and working from home.

The operator said if all employers embraced the potential benefits of offering a range of connectivity tools and technology – such as video conferencing and real-time collaboration apps – the UK economy could see an additional £14.7 billion in productivity gains for SMEs, and a further £19.4 billion for large companies.

“The definition of the workplace is changing at an ever-increasing pace,” said Jo Bertram, managing director, business at O2. “For many industries, gone are the days when work was a place you go. Now it is a thing you do – wherever, whenever and however you want. Businesses have already made great strides in enabling their people to make the most of the digital tools that can help them work smarter.”

However, Bertram warned that the latest figures showed that “it’s time for more of our leaders” to embrace the opportunity of better connectivity. “Not only will it help save time and money and make work more flexible for everyone, it’s also a solution to the UK’s productivity challenge,” added Bertram. “This is a critical obstacle to overcome if we want to stay a competitive global force in the years ahead.” ■

UK data centres meet climate change targets ahead of schedule

Data centre operators across the country have met their climate change obligations two years ahead of schedule, well exceeding the required 13.52% reduction in power usage.

Under the climate change agreement (CCA) scheme for data centres, they are required to reduce their power usage effectiveness (PUE) by 15% by the close of 2020.

Calculations by techUK, a trade association for the tech industry, showed the sector achieved a reduction of 16.72%.

“Provisional results from the Climate Change Agreement (CCA) for data centres suggest that the sector has successfully met its efficiency target, the third of four milestones in the life of the scheme,” said techUK’s associate director for data centres. “Collectively, UK operators have performed so well that they have fulfilled the final scheme target two years ahead of schedule. However, at individual facility level, the picture is more mixed, so the sector is not complacent and will be working harder than ever to build on these improvements in the final stage.”

Nevertheless, the figure is only an aggregation for results across 150 sites and a more detailed examination suggests there is much work to be done. Of 88 “target units” – defined as combinations several data centre sites – 40 passed the requirements while another 48 failed.

Although the headline is positive, critics have found fault with the PUE metric, claiming it is not a robust enough performance metric of energy efficiency. It is calculated as a ratio of the total amount of energy used by a facility, against the energy delivered to IT and computing equipment. The criticisms were also included in the report.

Calculations by techUK, a trade association for the tech industry, showed the sector achieved a reduction of 16.72%

“The CCA target of 15% improvement in PUE has been criticised by external observers unfamiliar with the commercial data centre business model,” techUK’s report said. “They claim that this is not nearly tough enough. Commercial operators providing colocation (or colocation-style services) control the infrastructure and not the IT, which remains a customer matter. PUE is a performance metric limited to infrastructure, so it is the best, or perhaps more accurately the least worst, metric to use for this type of provider.”

Brexit uncertainty has been cited as a key reason for this failure among sites that have not met their targets, due to a reduction in enterprise customers in the last few years. ■

US private equity firm buys Sophos for £3bn

Cybersecurity firm Sophos has been acquired by a US private equity firm for £3.1bn, making it the latest UK tech firm to be bought out by an overseas investor.

Thoma Bravo said its offer to buy Oxfordshire-based antivirus maker and take it private had been accepted.

It is also the first acquisition outside of the US for the private equity firm, which has, in recent years, pressed more heavily in to the cybersecurity sector, buying the likes of Riskonnect and antivirus giant McAfee.

Founders Jan Hruska and Peter Lammer - both Oxford science graduates - are set to pocket close to £500m between them from the sale, while chief executive officer Kris Hagerman will make £16.4m from selling his 0.57% stake in the company.

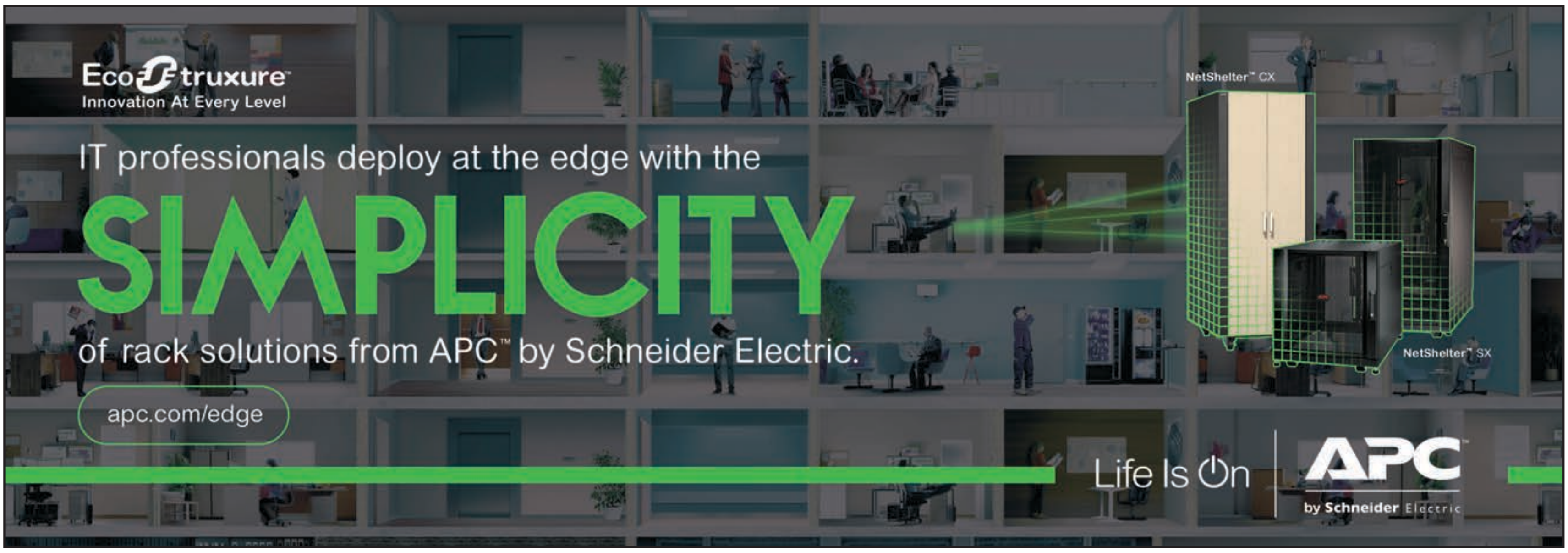
“Today marks an exciting milestone in the ongoing journey of Sophos,” co-founder Hagerman said in a statement. “Sophos is actively driving the transition in next-generation cybersecurity solutions, leveraging advanced capabilities in cloud, machine learning, APIs, automation, managed threat response and more.”

News of the sale sent Sophos shares on the FTSE 250 soaring by 37%.

The acquisition comes four years after Sophos – which counts the NHS and defence contractor Northrop Grumman among its clients - initially went public at a valuation of £1bn.

Since the EU referendum in 2016, UK tech assets have become attractive to international investors. In the same year as the Brexit vote, chip designer ARM was acquired by Japanese group SoftBank for £24.3bn. This was followed shortly after by the sale of Skyscanner to Chinese online travel site Ctrip for £1.4bn.

Other major acquisitions include music-recognition app Shazam, which was bought by Apple for around £300m in 2017, while Google quietly purchased Cambridge-based smartphone tech firm Redux in 2018. ■


EcoStruxure
Innovation At Every Level
IT professionals deploy at the edge with the
SIMPLICITY
of rack solutions from APC™ by Schneider Electric.
apc.com/edge
NetShelter™ CX
NetShelter™ SX
Life Is On
APC
by Schneider Electric

Zyxel provides multi-gig experience with new WiFi 6, 10G PON and managed WiFi products

Zyxel Communications expanded its WiFi 6 (11ax) portfolio with a brand-new managed WiFi platform, MPro Mesh and a 10G PON platform. The company said the products are designed to help service providers to unlock the full potential of their networks and deliver multi-gigabit connectivity to their customers.

Its expanded Wi-Fi 6 portfolio offers the choice of DSL, ethernet, active fibre, PON and extender models that can fit a variety of deployment scenarios.

Zyxel's MPro Mesh solution combines the abilities of its managed Wi-Fi solution with the industry standard, EasyMesh to deliver corner-to-corner, "high-performance" Wi-Fi with even greater mesh hardware compatibility.

"As more devices are falling into the hands of end-users, bandwidth demands are in turn increasing at an exponential rate, meaning service providers' networks must keep pace with their customers' demands," said Allen Lin, vice president at Zyxel broadband EMEA business unit. "Our newest range of solutions have specifically been designed with this in mind; from ultra-fast, whole-home WiFi coverage to delivering gigabit connectivity to the home or enabling seamless connectivity on the move, we are ensuring service providers can deliver a multi-gigabit experience to their customers – wherever they are."

The products made their debuts at the Broadband World Forum 2019 in Amsterdam mid-October. ■

UK cloud duo join forces to create new powerhouse

Two UK cloud service providers have joined forces to create a £30m annual turnover business after Birmingham's Acora acquired London-based Plan-Net for an undisclosed sum.

This newly-created group's revenues include more than 70% from "long-term recurring contracts", according to the west Midlands-based firm. Delivering services from four UK service operation centres, the group, which employs a total of 300 staff, will provide 24/7 coverage to a client base of more than 250.

The London business has been a specialist in supporting the IT needs of legal, financial and publishing organisations since 1990.

"Plan-Net has impressed us enormously in terms of its business model, the service levels it achieves with its loyal customer base and the way it aligns with our core offerings," said David Rabson, chief executive of Acora. "We see this as a merger with equal value for all stakeholders. It is transformational for the combined teams and the customers of Plan-Net and Acora alike."

Under the new management structure, Adrian Polley will join the Acora Board as managing director of the Plan-Net business, following 25 years of building Plan-Net with Jerry Cave, who will remain as an advisor to the board.

"Having worked alongside Acora previously, it was clear that the benefit for our customers and staff in bringing our offerings together provided an exciting opportunity for everyone," said Polley. "The combined proposition is incredibly strong, and we can see the merged group being dominant in the mid-market as we scale further and benefit from the growth opportunities."

Acora has been looking to expand its operations for some time and in February of this year, the company took a major step when it hired Paul Renucci as its new chief sales officer. He was brought in to share his growth strategies with the board and advise it accordingly.

At the time, Rabson said that given the company's plans and long-term ambition, "it was important for us to bring someone into the team that has been central to the growth of organisations, both through organic and inorganic strategies". ■

CCTV firm rolls out mobile workforce system

A construction site CCTV installation and monitoring businesses has rolled out a mobile workforce system as part of a cloud-based business system from Leeds-based BigChange.

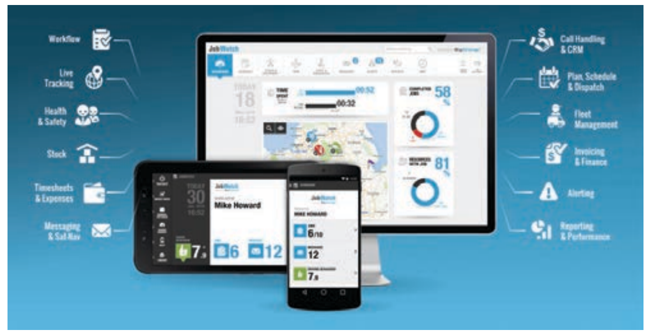
Equipped with rugged tablets running a five in one app called JobWatch, engineers at CCTV Monitoring are tracked and connected in real-time to the central system giving management 24/7 visibility of their field operations.

The firm has a team of CCTV and security specialists with engineers that can be deployed quickly nationwide to provide a complete CCTV service from site assessment to installation, monitoring and servicing.

Located in Emley, west Yorkshire, the company also operates a 24-hour "state of the art" monitoring station for "key" building sites across the UK. CCTV Monitoring services the likes of Kier, Balfour Beatty, Morgan-Sindall, Galliford Try, Willmott Dixon and Skanska.

BigChange has provided a complete end-to-end solution to CCTV Monitoring which handles the entire business process. From logging incoming service requests on CRM software, to work scheduling and job allocation, through to routing and tracking to live job reporting, invoicing and management reporting.

"Initially we simply used BigChange as a CRM but we knew straight away that it provided a tremendous opportunity to improve the way we worked," Stuart Capstick, managing director of CCTV Monitoring. "The potential became very clear when we installed some large screens in the office and we could all immediately see our entire operations in real time and see the exact status of each job."



Equipped with rugged tablets running a five in one app called JobWatch, engineers are tracked and connected to the central system giving management 24/7 visibility of their field operations PHOTO: BIGCHANGE.COM

Founded in 2005, CCTV Monitoring was formed to resolve the problems caused by opportunistic and professional theft from construction sites by using cost effective, technologically based CCTV alternatives to manned guards. ■

TeleData named point of presence for London Internet Exchange

TeleData UK, the data centre operator, has been named the fourth London Internet Exchange (LINX) Manchester (point of presence) PoP – extending LINX's regional internet exchange in the northwest.

Launched in 2012, LINX Manchester has attracted a mix of content and access networks on a local, national and international scale.

The exchange has over 140 connected member ports, peak traffic of over 100Gbps and greater than the coveted 99.999% for reliability.

"We are thrilled that LINX Manchester has selected us as their 4th Manchester PoP," said Matthew Edgley, commercial director for TeleData. "It marks a real quality stamp for us as a carrier-neutral data centre operator and is great news for our network-intensive customer base, who will benefit significantly from peering on the LINX Manchester exchange directly from our site. We plan to make it as cost-effective and simple as possible to become a member and join the exchange, by offering free of charge cross-connects and discounted rack space for connected members.

PHOTO: TELEDATA

TeleData UK provides colocation, cloud hosting, workplace recovery and data centre services

Jo Fereday, Product Manager at LINX added: "It's a great step in the right direction to be welcoming TeleData to the LINX Manchester peering network.

"They are long-standing members and partners of LINX and true supporters of our first regional exchange, so we are pleased to be able to make the location a LINX PoP."

TeleData UK provides colocation, cloud hosting, workplace recovery and data centre services. Last December, it announced that it would invest a six-figure sum into the development of its cloud platform, with an aim of making it one of the most resilient offerings available to businesses, as cloud services adoption continues to grow. ■

Dutch firm brings 'unique' outbound email security to UK

Zivver, a Netherlands-based data protection platform, is making its 'triple safe' outbound email and file transfer security solution available to the UK market for the first time.

The technology helps organisations to prevent data leaks, improve compliance and save costs from ineffective communication via fax, snail mail and courier. It does this by securing outgoing emails and file transfers throughout the whole communications process, before, during and after sending.

"In the Netherlands there was a new treatment protocol for HIV and the clinic that treated HIV patients wanted to inform them of it," Rick Goud, chief executive officer and co-founder of Zivver told *Networking+* "However, they (staff) put the names of the sufferers in the 'to' field and not the 'bcc' field. So, suddenly all the people in the email found out about other people who have HIV. That wasn't intentional, but it was still a data leak."

Having secured 2,500 organisations as customers in the last two years - including 25% of all Dutch hospitals and local governments – and raising $12m in funding in 2018, Goud said Zivver is ready to bring its technology to the UK.

"The UK is a very interesting market for Zivver - its innovative tech culture mirroring that of the Netherlands, with growing volumes of sensitive information being sent digitally," he added. "This similarity makes our triple safe technology a perfect fit, helping organisations here to more easily and affordably stop data leaks happening through human error and unauthorised access. Our integrations allow workers to use their normal email environment, such as Outlook and Gmail, and the strong encryption and two-factor authentication we apply – across all outbound email and file transfer content – minimises security risks still further."

Goud added that Zivver gives organisations – that hold the legal responsibility to prevent, identify and limit the impact of data leaks - "the controls and reporting tools needed to be in control of their digital communication via email and file transfer". ■

VIEW FROM THE TOP...

Comparing cloud contracts: what we've learned, *by Richard Blanford, chief executive, Fordway*

For most organisations, it's no longer a question of whether to use cloud but which applications to migrate and when. The good news is that, if your organisation has designed its applications correctly for cloud, the platform is almost immaterial because almost all the technology is pretty good. However, that doesn't make choosing the right service straightforward. There are significant differences in everything from design criteria and billing models to SLAs and data recovery terms – both between providers and between different services from the same provider. You need to understand exactly what you are signing up for to avoid future problems.

Finding the right solution requires a thorough understanding of the characteristics of the service you plan to migrate. Details that may not have mattered when you had your own servers can have a disproportionate effect on costs and quality of service. After helping many organisations migrate to cloud, we've identified key areas to review to help evaluate different options and avoid the most common pitfalls.

Availability and usage

First, decide whether your service requires persistent (reserved), non-persistent (on demand) or metered instances. You may decide you don't need 24 x 7 x 365 availability, but can your chosen contract guarantee availability when it matters? In the worst case, AWS' terms and conditions allow them to shut down on-demand instances without reference to the customer. If a service has to be available at specific times, you need to know whether the provider will ensure these within a non-persistent service and if this is cost-effective.

With metered services, ask the provider what guarantees they give that all capacity is available even if not used, and check what constitutes usage. Some applications generate keep-alive packets to ensure availability, and some metered services charge for these even when the application is not actually being 'used', so costs can quickly spiral.

Optimisation and granularity

Next, look at the characteristics of the service you want to migrate. Can you manage with general purpose instances or do you need computer, memory or storage optimised instances? Costs vary dramatically, both between providers and for different services from a single provider. For example, Microsoft Azure has five storage options, each with different capabilities, characteristics and dependencies.

You also need to know what the charging model includes. This is less of an issue with SaaS, which usually has a standard per user per month charge. If something is an extra, how is it charged and what is the likely impact on total cost? For example, an IaaS instance in AWS has five to eight metered costs that need to be tracked for a single Internet facing server. Azure and other public cloud services are comparable. Complexity increases for multiple server environments and if other elements are required to run the application, such as security, resilience, management, patching and back-up, which will be additional charges.

Security standards and guarantees

When considering security, start with the security classification and business impact of your data, and whether it mandates physical location awareness. Ask the cloud provider how they guarantee the security, access, audit and compliance controls you need. They may use self-certification, but you may want the assurance of independent verification and testing. Remember, with IaaS and PaaS services, the provider only secures the elements they are responsible for; they do not secure access and authentication to the application or service running, which remain your responsibility.

If a supplier adheres to recognised security standards, they should be able to prove that they have the relevant controls in place. If not, find out how they guarantee

Choosing the right service is never straightforward. There are significant differences in everything from design criteria and billing models to SLAs and data recovery terms – both between providers and between different services from the same provider PHOTO: BLUECOAT.COM

that their infrastructure is secure and patching is up to date, and their processes for handling any security incidents. It's up to you to audit them to ensure appropriate levels of information security are applied. Whoever hosts your data, your organisation retains responsibility for its security.

Resilience

It is important to find out what resilience is really being offered. You need to know the frequency and size of snapshots and the rate of change of data, as you will be charged for transferring data between domains. If the standard offering is not appropriate, you may be able to buy additional resilience.

Examine services guarantees closely and find out what compensation is offered if these are not met. Under most public cloud SLAs, if there is a major loss of service or even reduced performance, the cloud provider will refund a proportion of your monthly service fee. This may cover a very small proportion of the disruption you incur for a business critical service. Consider whether to have primary and recovery services hosted by the same supplier, and if you need an independent backup to restore from in extremis.

Service management, processes and contracts

You are unlikely to be able to persuade public cloud providers to revise their processes to suit your organisation without significant cost. Operational management is likely to be via a portal, so find out how the supplier handles escalation and service updates. What processes do they use for Problem Management or Major Incident Management, and what are the SLAs? You also need to consider contract flexibility, particularly whether there are exit or data transfer costs for switching suppliers.

Cultural fit

Finally, think about the cultural fit between your organisation and a potential provider. You are planning a multi-year agreement which will impact the services your organisation offers its end users, so it helps to ensure all parties are aligned before signing the contract.

ON THE NETWORK...

Why network asset management might be crucial for your business, *by Robert Neave, CTO and co-founder, Nlyte Software*

For many organisations the compute infrastructure can be complicated and inefficient. One of the main contributors to this complexity, and the leading factors toward inefficiency, is uncontrolled infrastructure spread. It's hard to comprehend that all these devices and software stacks are a singular collaborative unit as the types and management solutions for them fight for resources.

Imagine trying to manage all the devices within the Range International Information Group's data centre. Based in Langfang, this goliath facility is 6.3 million square feet – equivalent to 110 football fields. The larger the scale and proliferation to the edge the more problems that emerge.

If data centre managers don't have an understanding of what is happening in the network, applications will start to lag and acquire security problems, due to old versions of firmware and resulting non-compliance issues. If the network is not properly scrutinised, operating costs will soar from these multiplying inefficiencies. IT staff will always be held accountable for every piece of software and device running on the network – wherever it is located.

Explaining and exploring IT asset management

Data centre managers who don't attain a deep level of operational awareness encounter problems with their facilities as they don't have visibility or the metrics to see what's happening and why. However, managers sharp enough to install a technology asset management (TAM) system will avoid such hardware and software problems as it can collect detailed information in real-time. With the data collected, these managers have a single source of truth which covers the entire network which manages security, software licensing and compliance.

A global survey of TAM adoption and use delivered by Sapio Research, demonstrated how IT managers are struggling with not only identifying everything on the network, but also updates, audits and C-Suite expectations. It found that out of 1,500 technology asset decision makers in organisations employing over 1,000 people, almost all of them (96%) view hardware and software asset control as a top-five priority in their business. Nevertheless, nearly one third (31%) of those businesses were still trying to manually track their assets because of budget constraints – stopping these organisations having accurate visibility.

Of those surveyed, only 45 per cent said that their assets are validated daily, this dropped to 30 per cent regarding weekly validation of assets. The spectrum of commitment poses a direct question: What are IT staff actually tracking? The survey revealed that 62 per cent are doing this for desktops and laptops too.

C-Suite respondents believed that assets are being scanned hourly (27%) or daily (35%). However, at manager level there is less confidence as 8 per cent presume asset scanning of the network is taking place hourly, and 28 per cent think it's happening daily. When asked about their vendor software audit worries, 34 per cent of the C-Suite is concerned, in comparison to 19 per cent of Vice Presidents/Senior Vice Presidents, 20 per cent of Directors and 14 per cent of managers.

The IT security percentages were as expected as they ascended above the 50 per cent mark, on average 67 per cent have the latest security software and firmware patches. When the numbers descend below 50 per cent regarding audit trails for security patch management, 49 per cent of respondents said they have a solution that validates all devices, but 48 per cent said that they do not go out of their way to proactively manage devices. A standout revelation from the Global Technology Asset Management survey was that a massive 78 per cent of respondents claimed that up to 20 per cent of their assets remain undetected from network scans.

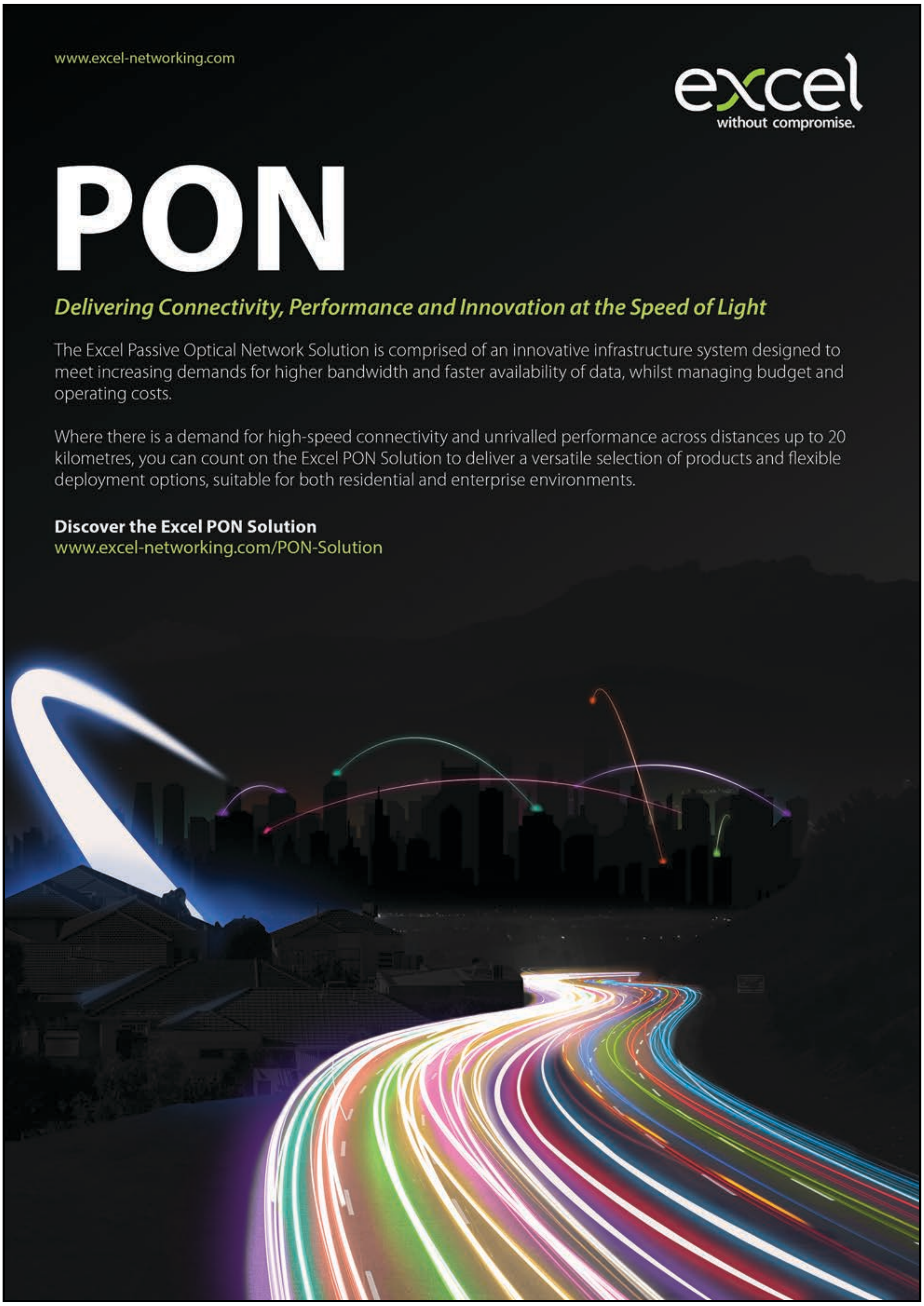
Of course the fact that 67 per cent of individuals claim to use the latest security software is good, it is crucial to also consider the fact that a third of assets remain in a state of risk. These assets are visible to IT and not inclusive of the total asset inventory. The risks from licensing, vulnerability and cyber hygiene are all still present.

Conclusion

It is evident that there is high understanding of TAM, but the adoption needs to be increased across the IT spectrum for larger organisations. The growth within organisations often runs parallel to a loss of control over technology assets. Taking back control no longer requires spreadsheets, keeping a watch on paperwork or counting off assets with a clipboard.

It is possible to exacerbate a false sense of network protection when the notion of proper security and compliance adherence varies from the C-Suite and different individuals across the organisation. This creates an urgency for obtaining true network visibility.

Achieving visibility and transparency can be found in modern solutions that allow the sharing of data across business systems such as ERP, IT infrastructure library (ITIL), data centre infrastructure management (DCIM), IT service management (ITSM), configuration management database (CMDB) and others. Utilising a TAM solution to automate the process by linking assets, locations and device usage with these systems for a single view at the whole edifice will reduce hundreds of hours of inventory, audit and compliance activity. This will give the IT staff more time to focus on delivering business value and innovation.



'Emergency' IT upgrades completed

Major makeovers get emergency services back on the road

HWFR's upgraded WAN infrastructure

The Hereford and Worcester Fire and Rescue (HWFR) Service consists of 27 full-time fire stations, 22 retained stations and 41 fire engines, strategically located across the two counties.

To put into context just how busy the service is, it receives nearly 10,000 emergency calls each year, requesting assistance to a wide variety of incidents. The service attends over 6,500 incidents each year, approximately 125 per week.

Being such a hive of activity, HWFR Service needs fast, reliable connectivity between fire stations and fire engines because it can be the difference between life and death.

Furthermore, the provision of this service comes with several challenges. Three in fact.

First, the HWFR Service must ensure that its firefighters can rely on a powerful network infrastructure that can effectively communicate vital information from one station, or fire engine, to another. Second, the Service must ensure it can rely on its network to mobilise its retained firefighters as and when they are required, in a timely and efficient manner.

Third, due to its 24/7 capability, the HWFR Service is also responsible for providing its staff with additional and alternative connectivity services. These services include back office activity, such as rota packages used by retained staff to clock in and out of shifts, basic connectivity back to SHQ and cable, satellite TV and internet access within the stations.

Without the required bandwidth to sustain both emergency services and additional services, the strain on the network has the potential to significantly affect connectivity across the wide area network (WAN).

After an extended seven-year contract with an incumbent national provider and with a growing focus on procurement values, the HWFR Service decided to tender for its ongoing communications requirements. Not only was it trying to benefit from new cost incentives resulting from a competitive market landscape, it was also looking to upgrade its WAN infrastructure.

MLL Telecom secured an initial three-year contract by the HWFR Service to deploy an upgraded WAN infrastructure to provide a faster, more resilient network, that is easy to manage and has the scope to be expanded if needed. The new WAN replaced the incumbent provider's MPLS network, a key step in providing the HWFR Service with a network that could guarantee fewer single points of failure.

The company was charged with enhancing ethernet fibre connectivity based on two overarching factors: price, as well as the provision and design of service. MLL Telecom was able to offer a fully managed solution replacing the incumbent provider's MPLS network, at a reduced cost and with additional bandwidth. It's solution also provided the HWFR Service with access to real-time network performance reporting and visibility of network utilisation to aid future capacity planning to support new services.

HWFR says the switch to MLL Telecom as a provider for the upgraded WAN has benefited the HWFR Service.

First, from a customer service point of view, MLL Telecom has been a refreshing change from the norm, offering a proactive and helpful service, and working with the HWFR Service to overcome any technical challenges that have arisen during the deployment.

Second, from a technical standpoint, the deployment of the new WAN across HWFR's 27 sites is already promising a significant increase in bandwidth, particularly to stations that are 24/7 and at a lower cost than the incumbent.

Vodafone helps out with fire engines

Emergency One was founded in 1989 in Ayrshire, Scotland and is now a key manufacturer of fire, rescue and emergency vehicles and rescue services across the nation.

Through its numerous partnerships with several fire and rescue services, Emergency One prides itself on listening and responding to the operational needs of firefighters. It works to create safer and more reliable firefighting equipment by supplying sensors, wireless connectivity and the internet of things (IoT), through which everyday appliances can connect to internet. Emergency One uses Vodafone IoT technology to power its telematics and tagging innovations, which it says have "revolutionised" the capabilities of fire services.

There were a number of challenges that needed to be taken ahead. The first was the need to track fire engines, monitor fuel and water efficiency as well as to ensure equipment is available and operational. Second, there was a need to enable firefighters to access Wi-Fi and stream fire footage or issue public safety warnings while out in the field. The other two challenges were to prevent vehicle downtime while repairs are made as well as make cost savings and optimise efficiency in the engineering and repair schedule.

Vodafone's IoT-enabled SIM cards were installed in fire engines to allow them to stay connected to the internet and Emergency One can now track its fleet at all times with RFID-tagging and telematics systems. Furthermore, with IoT SIMs, Emergency One can remotely assess the status of equipment, predict and repair faults, monitor water levels and more.

WiFi-connected fire engines make it easier for firefighters to communicate critical safety messages to the public. Remote problem-solving results in cost savings for fire and rescue services and less downtime for vehicles.

Global SIMs also mean Emergency One can expand into the international market assured that the vehicles will stay connected.

Updating the world's busiest international airport

The Airwave service uses TETRA (terrestrial trunked radio), an ETSI standard digital private mobile radio (PMR) systems which provides communications to keep emergency & public safety teams in touch using portable handheld & fixed vehicle radios.

It works in much the same way as a commercial mobile phone network and its digital voice and data service is trusted by the emergency service teams 24/7 as well as by other public safety agencies.

The nationwide roll-out of the digital Airwave network meant the old analogue radio communication system used by the emergency services would be replaced.

With Heathrow Airport's numerous buildings and infrastructure, it was soon identified that an airport-wide communication system would need careful planning to achieve the required operational criteria.

So, the customer entered close dialogue with Airwave as the new network was being created. This early involvement meant Airwave soon concluded they would need a company with specialist knowledge and experience of TETRA technology to deliver its customers' needs at Heathrow.

Airport coverage requirements were specified and it turned out to be almost everywhere. Affini was responsible for designing the system and so it had to satisfy the customer that all the airside, landside, public and private areas had the coverage required. In fact, coverage was so important that the customer wanted to independently test the system. This was completed during the final commissioning phase to ensure it met their requirements.

The network was designed to ensure that users have instant communication, even in remote areas and within the confined spaces of the building and tunnels.

Where radio coverage has often failed in the past. To make this a reality, Affini used its skills and expertise in design, to create and construct the wireless infrastructure to bring the network to life.

The network's comprehensive indoor and outdoor coverage is now operational in the following in all airport terminals, public car parks, pedestrian subways linking the terminals, airside road tunnels under the runway and the M4 spur road tunnel. There's also one rooftop macro cell inside the airport and seamless external coverage from neighbouring TETRA cells outside the airport boundaries.

Throughout the implementation they have been responsive and easy to work with," said Martin Benke, operations director at Airwave.“

Shining a light on the dark web

Cybersecurity is a ubiquitous and never-ending topic, but just what happens when the hackers get what they want? ROBERT SHEPHERD looks at the threat of the dark web

If you were given a pound for every time you saw a cybersecurity or hacking story, the chances are you'd have given up work now and be lounging by a pool in somewhere like Dubai, the city in which I currently sit writing this article. No, I'm not on holiday and neither have I retired – I've just spent a few days at the GITEX conference witnessing how almost every 5G and IoT presentation is punctuated with tales of, you guessed it, cybersecurity.

We know that hacking has long been the bête noire of the IT sector and it's not going to go away anytime soon, if ever. However, what's less talked about is where enterprises' data actually ends up and how it changes hands.

One such marketplace is the dark web, a network which allows users to explore the internet anonymously without a tracked IP address.

According to Marc Laliberte, senior security analyst at WatchGuard Technologies, the dark web or dark net itself isn't necessarily a threat to enterprises because it's relatively easy to identify and block access to it from corporate networks. However, there's a "but" coming.

"The real danger the dark web poses to companies is the information exchange that it facilitates," he says. "Cyber criminals can use dark web marketplaces and forums to anonymously sell and share stolen data like user credentials, PII and trade secrets."

James Maude, head of threat research at Netacea agrees and says the dark web offers a degree of anonymity and privacy that makes it a natural breeding ground for various forms of criminal activity. "From Hacking as a Service (HaaS) to databases of stolen credentials, there are a variety of threats that can affect enterprises," he adds.

The dark web sounds like such an ominous title, you'd be forgiven for thinking the entire thing is a nefarious set up. However, it may surprise you that it was built with good intentions.

"The dark web is often misrepresented as a cesspit of criminal activity, with forums selling everything from passports to drugs and even guns," adds Maude. "However, it was born from a dream of privacy and freedom of speech, in a time where governments increasingly saught to control and monitor internet use. In many cases, the dark web allows individuals to discuss ideas openly in countries with oppressive governments or whistle blow on corruption."

> "The real danger the dark web poses to companies is the information exchange that it facilitates."

Laliberte points to the fact there are "actually a few different dark web

Marc Laliberte
senior security analyst
WatchGuard Technologies

"In more regulated regions we also see the dark net used as a way to avoid censorship as users have access to the entire open web, which otherwise would be restricted through government firewalls."

Julien Patriaca
cybersecurity expert
Wallix

networks" like The Onion Router (Tor) and the Invisible Internet Project (I2P). Tor, the most popular flavour of dark web networks, was originally created with the help of the US government.

"The United States Naval Research Laboratory and the Defence Advanced Research Projects Agency (DARPA) both had a hand in developing the technology behind the dark web with the goal of protecting intelligence communications from agents embedded in foreign nations," Laliberte says. "As with most useful tools, it didn't take long for cyber criminals to hop on board too."

Julien Patriaca, cybersecurity expert at Wallix says that while Tor was originally developed as a means for the US government to privately explore the internet, it has evolved to become a not-for-profit "company" and is freely available to the public.

"The overall goal is to create a sense of freedom and animality for the user allowing them to browse with complete freedom and privacy," he says. "In more regulated regions we also see the dark net used as a way to avoid censorship as users have access to the entire open web, which otherwise would be restricted through government firewalls."

Regardless of where it came from, we are now in a very different place to when it was created because it tends to be used for ill-gotten gains.

However, Patriaca says it's easy to label the dark web as a threat due to anonymity it instils but it is not the network itself which is a threat. "Not everyone who uses the dark net is seeking to do so for criminal intentions, however, due to the elevated level of security and the ability to browse freely and anonymously it has become a hot bed for cybercrime," he adds. "A virtual black market has opened on the dark web making it easier for hackers to collaborate, share tactics and to buy and sell goods, data and intellectual property that would otherwise be illegal. While to some extent this promotes criminal activity, it is not the network but the hackers and cyber criminals who use it that enterprises need to safeguard against."

Cybercrime is on the rise and it is a serious threat to businesses of all sizes, so Patriaca says "as we continue to evolve in today's digital society", hackers will continue to look for new ways to penetrate the network with or without the communication available on the dark net. "Therefore, businesses need to ensure their security protocols are evolved and can adapt to meet these threats," he says.

Still, if the network itself poses no direct harm to enterprises, here's why they should still care about it.

"There are few worse feelings as a business executive than receiving a call (from the authorities) to inform you that they've found your organisation's data for sale on the dark web," says Laliberte. "An entire industry is now built around dark web scanning. That is, looking for stolen information on the dark web as another means to identify when you may have been the victim of a breach.

He adds that "any data that is valuable to your business" is valuable to an attacker and everything from trade secrets to customer records are potentially profitable targets for cyber criminals. "Even something as simple as your authentication database can be worth a lot to the right person though," he says. "Credential re-use is still rampant in all industries, which means a password dump can compound into even more breaches down the line."

So, what's the worst that can happen?

That very much depends on the business, argues Maude, however, one of the biggest risks he says is breached customer data and customers' personally identifiable information (PII), appearing for sale on a dark web forum.

"Many businesses invest heavily in security technologies to prevent backdoors in databases and systems being exploited to steal information, while neglecting the front door such as customer login forms," he continues. "These front doors are often vulnerable to credential stuffing. In this instance, attackers take combinations of usernames and passwords – that are readily accessible for purchase on the dark web – to directly hijack customer accounts."

For Patriaca, the worst outcome for a business is the loss of intellectual property to cyber criminals. "This can be a major catastrophe, not only impacting a business's day-to-day operations but if this information is passed on or sold to a competitor the long-term impact could be detrimental. Customers could lose trust in the business and if you have a unique proposition in the market this will no longer be the case, significantly impacting revenue and business opportunities."

For any industry or business to succeed, the old adage "supply and demand" has to be examined. We know the dark web is flourishing, but just how do you put in an order for what you want?

That's where HaaS comes in.

"Cyber-crime in general is becoming increasingly commoditised with off-the-shelf tools and networks available for purchase or hire, says Maude. "In the case of credential stuffing, tools that fully automate attacks against large enterprises start at around $20 and come complete with training and support packages. The barrier to becoming a cyber-criminal has never been lower and the use of the Dark Web makes it increasingly hard to track perpetrators. As a result, cyber-crime is a low risk and potentially high reward occupation."

Patriaca adds that not only is HaaS as "a real threat and although hacking is predominantly an illegal action the notion is growing in popularity. "The idea behind this is to hire a hacker, gain access to a botnet or purchase a toolkit in order to breach an organisation and while it is a potential threat to businesses, it is mostly larger organisations that are targeted as a result as it can be an expensive service," he says.

What's more, the hackers are after one thing: data. "Attackers are becoming increasingly sophisticated in monetising data and accounts," says Maude. "Hackers will target subscription services, compromising and reselling accounts. They will target loyalty points schemes to steal points and rewards. If you post content, such as videos or articles, hackers may steal this to repost and monetise with ad revenue. They will even scrape pricing information, goods availability and item descriptions to resell to other businesses."

In Patriaca's view, anything which details customer data is a high target – and data is vastly becoming one of the hottest commodities and organisations are willing to pay for it.

"Most often we see data which includes personal home addresses, phone numbers, birth names and dates as well as personal bank details and credit card numbers sold online," he says.

Laliberte says that while HaaS is a very real threat, he argues that the bigger threat is from marketplace items that enable low-skill hackers to carry out their own damaging attacks. "Things like Ransomware as a Service, where a skilled attacker creates and maintains the infrastructure for an evasive ransomware

One of the biggest risks is breached customer data and customers' personally identifiable information (PII), appearing for sale on a dark web forum

Although one can't ask for much more than having protocols in place, it appears that another risk for most businesses is the fact that they won't even know when attacks are coming

attack, enable anyone to launch an attack and potentially earn a hefty profit," he says.

Now, that the potential threats have been made clear, it's important to know what software/technologies are being used to combat it?

"It's actually fairly straight forward to block access to most of the dark web protocols like Tor and I2P," says Laliberte. 'Most UTMs and NGFWs include application control services that can fingerprint and block access to dark web networks from corporate machines. Keeping corporate data off the dark web is a whole different story though. Organisations need a layered approach including technical protections and user training to stand a chance. At a minimum, companies need multiple layers of malware detection that includes technologies capable of detecting evasive threats using behaviour analysis paired with detection and response services to identify threats that slip through the cracks."

Maude argues that while the dark web might seem like a worry to enterprises, it's important to remember that the risks it poses are not fundamentally different to those addressed by common security best practices.

"The one security protocol the dark web should drive enterprises to invest in, is protection against stolen credentials," he says. "This could come in the form of a dedicated bot management solution, designed to prevent automated credential stuffing bots from using your website or services to test lists of stolen credentials.

As well as dealing directly with the risk to an enterprise's reputation in the face of a credential stuffing attack, there are vendors who scan the Dark Web to identify any breaches or datasets that involve your brand. However, this is a highly reactive approach and is purely focused on post-breach damage limitation."

Patriaca says it's important to note that it is cyber criminals organisations need to protect themselves against and not the dark net itself.

"Many organisations focus on and invest in software to defend and protect against external threats, like malicious software or outside hackers," he says. "Perimeter software such as firewalls can help to safeguard against this. However, it's also important to protect against human error and insider threats through technology such as privileged access management. This will not only add an additional layer of protection, but it can also ensure that cyber criminals have limited access if they do penetrate the first line of defence."

Although one can't ask for much more than having protocols in place, it appears that another risk for most businesses is the fact that they won't even know when attacks are coming.

"In some not every organisation is aware when they have an intruder in the network," says Patriaca. "There are many occasions when businesses may even see their own personal data or customer data leaked online and only then do they realise there had been a data breach.

Typically, the problem comes down to budget constraints and added user burden."

Indeed, he says organisations must make the most out of what budget they are given, and employees want to work quickly without the need to type in multiple passwords. "Education and supporting employees can make a significant difference, it's important that anyone using the network takes an element of responsibility to safeguard data and password protection is a simple and effective way to do this," continues Patriaca. "Adding an additional layer of protection through privileged access management can also help to reduce some of this burden and improve security. If organisations encourage a strong security protocol internally and help to educate employees not only on the risks and what signs to look out for, but also how to create healthy passwords we will see a much more effective approach taken to cyber security."

Laliberte says attackers prey on complacency. "Enterprise IT staff should always assume they are under attack, because they almost always are," he adds. "The good news is, there are technologies available to detect even the most evasive attacks. Teaching your users to spot phishing attacks can also go a long way towards keeping your networks clean."

Maude offers the west African proverb 'speak softly and carry a big stick; you will go far'. He adds: "A good way to approach risks online is you must deliver a good experience to your customers whilst always being prepared to defend yourself. Organisations may worry about the risks associated with activity on dark web cyber-crime forums, but there is no real difference between this and the activity carried out on private forums, on the regular internet or even by lone threat actors."

In Maude's view an enterprise doesn't need to know when an attack is coming to be prepared. "It is important that enterprises get inside the mind of an attacker when developing new sites and services online and conduct threat modelling exercises to understand the risks and possible mitigations," he adds.

"The dark web is often misrepresented as a cesspit of criminal activity, with forums selling everything from passports to drugs and even guns."

James Maude
head of threat research
Netacea

There are precautions that can be taken, but if the dark web is used for things as serious and sinister as buying weapons, terrorism, drugs, kidnapping and prostitution, just what chance does an enterprise have of defending itself?

Maude says while its anonymous nature makes it hard to track users and shutdown illegal services, "it is merely an alternative method of communication, there is nothing particularly unique about the threats beyond potentially masking their origin".

Laliberte says networks are as secure as enterprises make them and an organisation's main goal should be to defend their networks and keep data off the dark web. "While there is no such thing as a perfect defence in cybersecurity, hope is not lost for keeping your company safe," he says. "The right mix of layered security with user training can give you a fighting chance against cyber criminals. If you take the time to deploy and maintain technical layered defences, you have a better shot at keeping cyber criminals out of your network."

Patriaca says, "simply put" even the most secure of networks are not impenetrable. "Unfortunately, as humans we are prone to mistakes and this can leave networks open to potential security breaches," he adds. "What is needed is a combination of both technology and education in order to minimise as much vulnerability as possible." ■

Confound the crooks

Foil the hackers with these products. And Paul Mercina, head of innovation at Park Place Technologies, offers his advice

Data security is a pressing issue. More than 1,900 known data breaches occurred worldwide in the first three months of 2019. The UK ranked third highest with 17 breaches in Q1, and our country's costs for such failures are up 41 per cent over the past two years. Add in the threat of fines under the General Data Protection Regulation and private and public sector organisations are rapidly adopting a heightened security posture.

The cybersecurity challenge has many IT organisations hoping for inoculation via the latest solutions. But before investing in cutting-edge security products, make sure the fundamentals are in place.

Although it may seem elementary, problems arise when basic measures are overlooked. The WannaCry ransomware attacks, for example, exploited a known vulnerability; a patch would have prevented harm.

Thus, many security best practices are the same as always. Patches must be pushed out enterprise-wise. Perimeter security remains essential, and newer firewalls and other solutions provide improved protection. Access controls need to be fastidiously maintained.

Data encryption imposes far fewer operational challenges than in the past, so you should seek to encrypt all data in transit and at rest. Proper key management is also necessary. Storing keys on the same server as the data is asking for trouble but many IT facilities still do so.

In the bring your own device era, it's necessary to segment Wi-Fi and aggressively wall off sensitive data with micro segmentation. Information rights management applications can also be a great addition to protect files that leave the corporate sandbox.

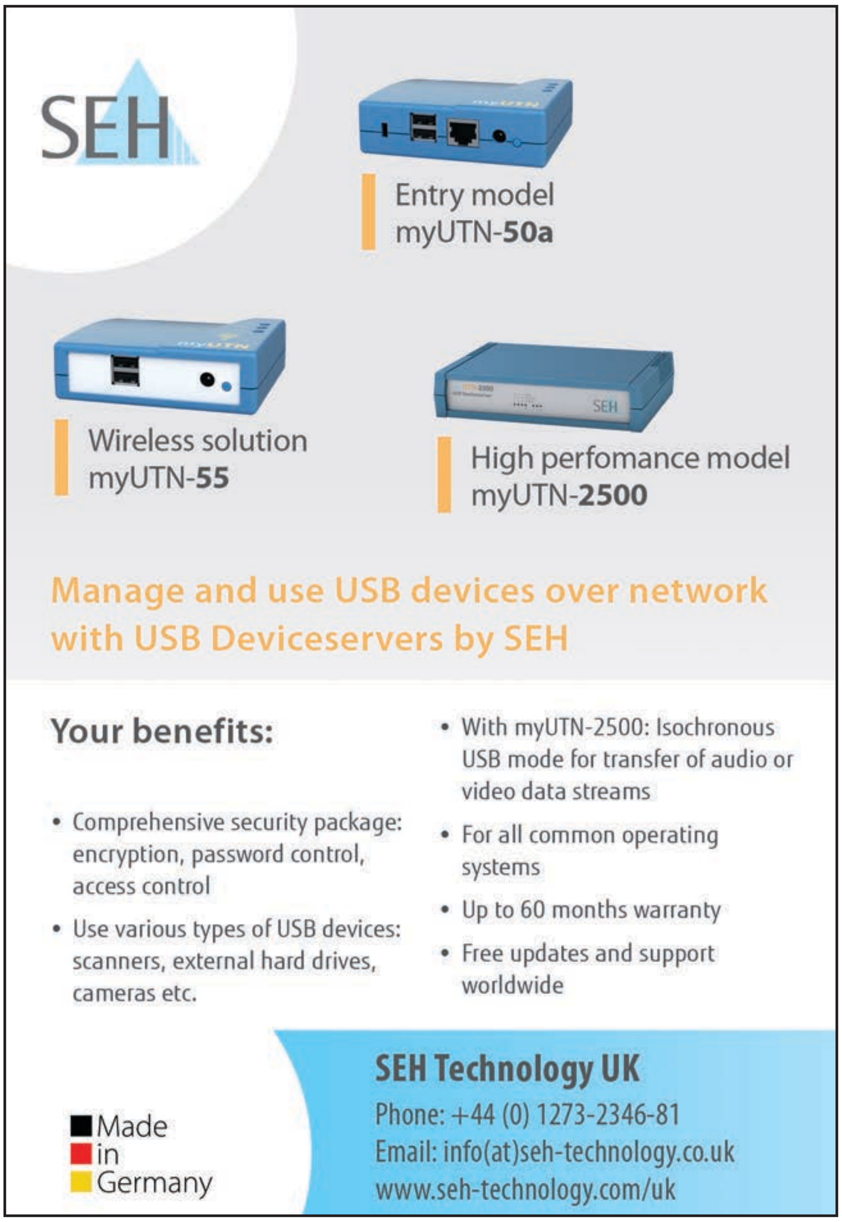
From an organisational standpoint, integrating security more seamlessly with application development, such as through DevSecOps, is advisable. Also consider bringing security into the network operations centre (NOC), thereby creating an integrated operations centre (IOC) for more coordinated and rapid-fire breach response.

Be sure to arm these experts with high-performance security information and event management (SIEM) systems and other post-breach response solutions.

Once the foundations are in place, your next step is to follow security advances and incorporate the right innovations.

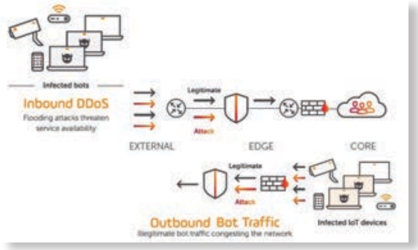
Deep learning systems are becoming increasingly capable of identifying potentially malicious activity and rooting out advanced persistent threats (APTs). Artificial intelligence will soon supply more robust security automation and, further down the road, homomorphic encryption will allow the use of encrypted data without decryption.

It's worth the time and investment to research options for upgrading data security. But as exciting as the cybersecurity field may be, basic principles still hold. Get your fundamental security processes and tools in order to outwit predictable threats and then branch out to defeat the most cunning attacks.



With DDoS attacks becoming more frequent and sophisticated, **Allot** says its DDoS Secure product is the first line of defence against both inbound and outbound attacks.

Allot says it surgically mitigates volumetric DDoS attacks and isolates infected hosts before either can hit users.



Customers can, says Allot, avoid rerouting traffic to scrubbing centres and save infrastructure costs; get always-on, bidirectional protection that responds in seconds not minutes; gain full automation with no need for supervision; cluster multiple sensors to thwart the biggest volumetric attacks; neutralise zero-day attacks; prioritise critical traffic during attacks; and deliver attack forensics.

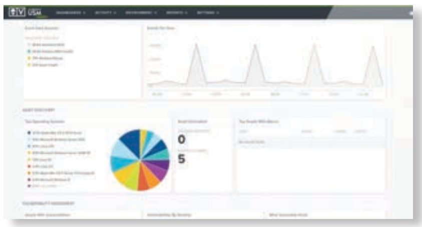
It says DDoS Secure inspects all traffic to form accurate traffic behaviour models and detect and halt even the smallest attacks, including those from IoT devices, outbound spam, worms or port scanning traffic generated by bot-infected users.

Setting up an effective threat detection and incident response programme is costly, particularly with the shortage of skilled security professionals, says **AT&T Cybersecurity**.

It has introduced a service called AT&T Managed Threat Detection and Response which it says brings together people, process and technology to help users quickly detect and respond to advanced threats before they hit the business.

Using AT&T Alien Labs' skills, it says a team of security analysts hunt for and disrupt threats around the clock and carry out in-depth incident investigations to produce recommendations.

AT&T says the service can be deployed faster and at less than the cost of hiring an additional security analyst and is priced according to the total number of events analysed.



Citing the growing use of open source software, **Contrast** Security says it brings security, legal and compliance risks which are not quickly identified and eliminated by scan-based tools.

It has introduced Contrast OSS which it says is the only product on the market which can continuously identify vulnerable open source components, determine how they are actually used by the application, and then prevent exploitation at runtime.

The company says Contrast OSS provides the ability to automatically create and maintain a business-wide inventory of open source components; provide real-time correlation of vulnerabilities, OSS license information and additional library metadata; continuously evaluate open source components for licence compliance and intellectual property risk; automatically enforce custom policies and provide real-time feedback; and continuously monitor applications and block attacks on vulnerable open source software.

Today's network and security operations teams face data volumes and velocity that exceed human scale, says **Ixia**.

It has introduced Vision X, a network packet broker, which it says provides scalable visibility for data centres today and in the future.

Ixia, owned by Keysight Technologies, says Vision X is designed with a modular approach so users can select different functions, capabilities and speeds as their needs evolve.

Features include: the ability to aggregate up to 6Tbps of total traffic, from the edge to the core; flexibility to expand and/or change monitoring using customisable, hot-swappable modules with multi-speed port choices; process up to 2Tbps of data at speeds from 10G to 100G and deliver it to the appropriate tool saving space and power with a three-rack unit design; zero-loss advanced packet processing with Ixia's dynamic filter compiler to manage security and privacy compliance; and a drag and drop GUI.

Hundreds of thousands of new viruses appear every day, says **Panda** Security. And the sophistication of techniques for penetrating defences and hiding malware means that corporate networks are more vulnerable than ever.

The company says its Panda Adaptive Defense 360 is the first product to combine endpoint protection (EPP) and endpoint detection and response (EDR). It also automates capabilities, reducing the burden on IT.

Panda says its EDR relies on three principles: continuous monitoring of applications on a company's computers and servers; automatic classification using machine learning on its cloud-based "big data" platform; and its technical experts who analyse applications that have not been classified automatically to be certain of the behaviour of everything that is run on the company's systems.

THE WORLD ACCORDING TO...

Solving the unsolvable, by *By Chris Wellfair, projects director, Secure IT Environments*

Whilst some parts of the political and petrochemicals establishment seem hell bent on trying to convince the world that climate change is not an issue, most would agree it is. Data centres of course make their contribution to this issue and it is down to the work of diligent designers, equipment manufacturers, and indeed software engineers that such great strides have been made to minimise that impact.

But the weather still has a big impact on our data centres. Temperature records were set in July last year and then again, this year for the hottest July on record, along with the hottest late August Bank holiday. The weather also had a role to play in the August 9th power cut that affected over a million people, and left travellers stranded. A small lightning strike, a normal occurrence on the grid and dealt with over a thousand times a year, led to a small loss of embedded generation. But then almost immediately two unrelated generators failed. This led to the frequency on the network dropping below 49Hz, which in turn caused other parts of the network to shut down. Distribution network operators reported that demand availability was restored by 6:30pm, even if travellers suffered for hours after.

Whilst weather is a common factor to these situations that could have easily impacted many data centres across the UK, the real point is that external factors are the greatest problem for data centre managers, and what can you do to solve these things that are out of your control?

The reality of course is that we can't, but what we can learn from the recent power cut, is that the national grid had tried and tested processes for dealing with power failure, that kicked in and worked exactly as they should. At the time of writing, we are still waiting for the final report on the incident and there may be things that can be learnt, but the point is that throughout the escalating problem, processes worked as they should.

It's all about risk mitigation, and in the data centre, the way we need to solve the problem of heat waves and power outages is through readiness, and we ensure this through proactive maintenance regimes and the regular testing of equipment such as UPS, ACUs and generators. I am sure we all breathed a sigh of relief when we knew our DCs stayed up through the power cut and heatwave, but if they didn't could you confidently say all of your failover and cooling equipment was regularly maintained, tested and cleaned? This summer, should tell us how important these things are to solving the uncontrollable DC problems.

Most of UK workforce lacks basic cyber training

Over three quarters of UK workers (77%) said that they have never received any form of cyber skills training from their employer, according to a new study from a provider of cloud-ready Zero Trust Privilege to secure modern enterprises.

Centrify surveyed 2,000 full-time professional services workers in the UK and also found that 69% of those polled said they lacked confidence in their own ability to keep their data safe and secure.

The report was published at the start of European Union's CyberSecMonth, designed to raise awareness of cybersecurity threats, promote cybersecurity among citizens and organisations. It is also there to provide resources to protect themselves online, through education and sharing of good practices.

Meanwhile, 27% of respondents admitted to using the same password across multiple accounts, whilst 14% said they keep passwords recorded in unsecured notebooks.

"Ignorance of the law is no defence," said Donal Blaney, cyber-law expert, Griffin Law said: "Company directors and business owners owe it to themselves, their staff, their shareholders, and their customers to know how to protect their businesses and their customers' data. They will only have themselves to blame if this blows up in their face one day."

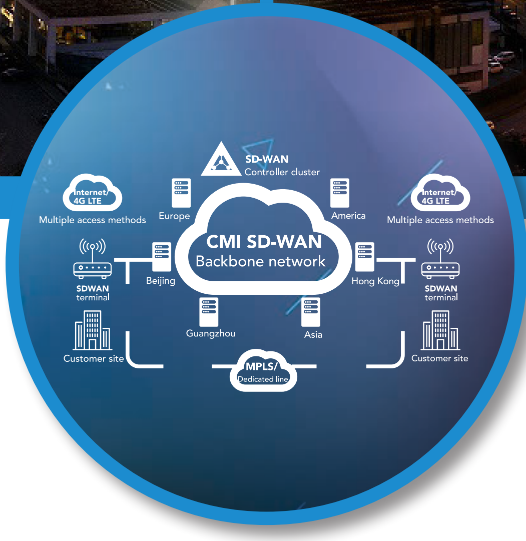
Andy Heather, vice president, Centrify added: "In an age where cyber-attacks have emerged as one of the most ruthless and successful forms of crime that can be committed against a business on a large scale, it is astounding to hear that so many UK companies neglect to instil even the most basic cybersecurity measures in their employees. Tackling this issue requires urgent investment in cyber skills training and adopting a zero-trust approach, to further reduce the risk of weak passwords leaving easy entry points and to ensure malicious parties cannot run riot in company systems with stolen log-in credentials."

Of those polled, 69% said they lacked confidence in their own ability to keep their data safe

CP Critical POWER
Supplies ■ Projects ■ Support
PLUS Fully qualified NIC/EIC electrical engineers and in-house F-GAS certified engineers available
ONE SUPPLIER...
Providing turnkey critical power solutions, including design, installation, maintenance & support
■ Electrical installation & consulting services
■ New thermal imaging capabilities
■ Power ■ Cooling ■ IT infrastructure
■ 3-Year warranty
■ World class impartial advice saving you time & money
■ Call now for a FREE site survey & health check
■ Nationwide sales & engineering team, on hand 24/7
■ DAIKIN Installer
Design & Build
Cooling
Batteries & Accessories
Generators
Onsite 24/7 Services
UPS
Data Centres
Voltage Optimisation
PDU
Racks & Enclosures
Critical POWER : When it matters most
www.criticalpowersupplies.co.uk | 0808 196 0370

中国移动 China Mobile | International

SDWAN



The China Mobile International SD-WAN solution provides central management tools, network visibility and the ability for customers to secure WAN networks at their fingertips.

SD-WAN traffic can travel through the CMI high quality global backbone network when hybrid with MPLS/IEPL products. By incorporating with Internet broadband or LTE as the last-mile between CMI POPs and enterprise branch offices, it will shorten WAN network setup time and reduce operational costs, without sacrificing network performance and security.

CMI SD-WAN will provide: Global WAN coverage | Fast WAN service delivery | Guaranteed international network bandwidth and latency | Competitive WAN service package | Value-added network and management services.

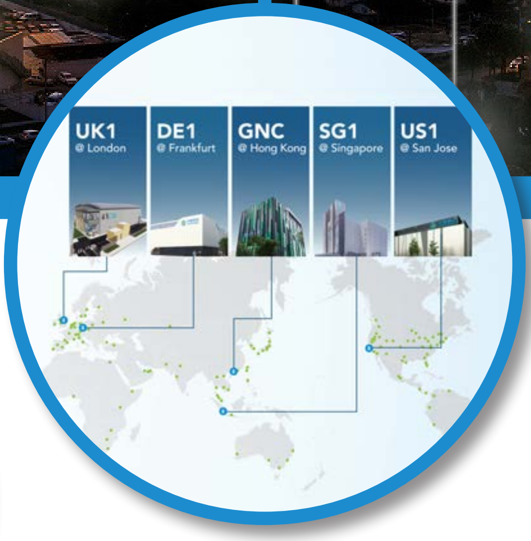
IoT End-to-End Solutions

Personal and Pet Monitoring
Agriculture
Smart Homes and Cities
Embedded
Travel
Telemedicine
and Healthcare
Internet of Things
Energy Use
Wireless Sensors
Banking and Finance
Building Management
Security

China Mobile's IoT service, OneNET 4.0, runs on a world class dedicated network infrastructure which is highly reliable, secure, fast and offers wide 4G coverage throughout China. We provide a variety of services such as M2M SIM Cards and multiple Data/ SMS/ Voice plans to meet your needs for different scenarios. We also provide platform integration solutions for carrier customers.

CMI IoT End-to-End Solutions will provide: M2M SIM Card | Sufficient number resources | Support 2G/4G | Various card sizes | Two types of encapsulation material.

Global IDC



The launch of China Mobile International's UK1 Data Centre at London in Q4 2019, adds to a network of 5 self-owned global Data Centres and over 750 data centre partners, across 150 cities, worldwide.

Based at Slough Trading Estate, UK1 Data Centre is a newly built dedicated data centre building with 1,680 racks, a total 15 MVA capacity, a floor area of 9,735sqm, meets Tier III standard and is also protected by a high standard, 9-layers security control system.

China Mobile International has over 941 million mobile subscribers, as of August 2019, with UK1 Data Centre serving as the hub for International Network Exchange and Internet Data Centre in one building in the UK. With three individual Cable Lead-in, it offers direct connection to other major data centres in London and the CMI Local Ring across Europe.

www.cmi.chinamobile.com | enterpriseuk@cmi.chinamobile.com | +44 207 933 9190