

**IN DEPTH:**  
GDPR post  
Brexit: what  
should firms  
expect?  
P8-10

## When continuity plans go wrong

What to do when the worst happens

Craig Atkins,  
1-Fix, p7



## Looking at OEM alternatives

Identifying the best fit scenarios for you

Mihaela Dinu,  
Curvature, p13



## Questions & answers...

Networking+ meets Rajant's VP of artificial intelligence

Jon Lederman,  
Rajant, p15



# Government's education cybersecurity warning



The UK government's national security body has warned the country's education system about possible cyberattacks, as students across the country return to school following the nationwide lockdown that curtailed the last academic year.

Fears have arisen that institutions could face attack due to a lack of proper protection and the National Cyber Security Centre (NCSC) said that schools and universities need to take steps immediately to make sure they stay protected. This includes moves such as upgrading cybersecurity protection, ensuring data is stored securely, and making sure systems are backed up away from the premises.

The alert urged schools and universities to take immediate steps such as ensuring data is backed up and also stored on copies offline.

"This criminal targeting of the education sector, particularly at such a challenging time, is utterly reprehensible," said Paul Chichester, director of operations at the NCSC. "While these have been isolated incidents, I would strongly urge all academic institutions to take heed of our alert and put in place the steps we

suggest, to help ensure young people are able to return to education undisrupted. "We are absolutely committed to ensuring UK academia is as safe as possible from cyber threats, and will not hesitate to act when that threat evolves."

Furthermore, the NCSC said it has been investigating an increased number of ransomware attacks affecting education establishments in the UK, including schools, colleges and universities over the past few months.

Fredrick Forslund, VP enterprise and cloud erasure solutions at international data security firm Blancco, said the NCSC's decision to issue a cybersecurity alert to the academic sector comes as no surprise. "The global pandemic has resulted in an unprecedented shift to online working, mirrored by an increase in cyberattacks," he told Networking+. "As schools and academic institutes return, vulnerable IT systems will be put to the test by a new wave of cyber threats, from contemporary ransomware attacks to phishing attempts. Education providers handle a lot of sensitive information about their staff, students, and the institutions themselves. As part of that responsibility, strict data retention policies are crucial. Failing

that responsibility can mean breaching privacy laws, resulting in steep consequences – fines, plus a loss of reputation if there is a data breach."

Educational institutions across the world were hit by a wide-ranging cyberattack attack known as Blackbaud (see *Networking+* July edition) with schools and universities hit with ransomware assaults.

The NCSC advisory lists a number of ways it has seen criminals target schools in recent months, including phishing emails, unpatched or insecure hardware and software, and remote desktop protocol attacks. Furthermore, the rise in online schooling over lockdown may have contributed to a rise in the latter, with students and teachers alike using personal devices to log in to workplace networks or connect to lessons.

"The NCSC recommends that organisations implement a 'defence in depth' strategy to defend against malware and ransomware attacks," the NCSC said. "Your organisation should also have an incident response plan, which includes a scenario for a ransomware attack, and this should be exercised."

*continued on page 2*

ninja  
RMM

Find out what you need to  
make technicians 50-70%  
more efficient.

READ MORE





## Education sector given post-lockdown security warning

*Continued from page 1*

Forslund added that the way education providers handle data is changing in tandem with the new “blended learning” landscape. “For those responsible for keeping data storage clean and secure, it’s important to recognise exactly where your data is distributed and stored,” he said.

“Today we are dealing with sensitive data on-premises, at home and in the cloud, which all require varied data management approaches. The NCSC’s alert has urged academic institutions to take certain immediate steps, one of which is ensuring all data is backed up and stored locally.”

The recent Blackbaud hack saw universities and schools exposed after an attack on the cloud computing provider, which affected more than 125 organisations. Those affected included the University of Edinburgh and Aston University in Birmingham. ■



**Blancco's Fredrick Forslund believes the way education providers handle data is changing in tandem with the new “blended learning” landscape**

## ‘Nearly 80% of enterprises want CSPs to drive 5G adoption’ - survey

UK enterprises stand to reap significant benefits from the adoption of the latest 5G communications technology, but there is still much work for service providers to do, according to a survey by Hansen Technologies.

In partnership with Coleman Parkes Research, Hansen surveyed 100 tier-one enterprises across eight sectors worldwide, finding that respondents believed increased adoption of communications technology could add \$200m per year to the revenues of the largest companies.

The first edition of the B2B Telecom & Tech Index found that 80% of surveyed respondents believe communications technologies are important or very important to generating new revenues, while 76% said they can improve business agility.

However, a mere 34% said they were “very satisfied” with their current CSP, with almost half showing no overt levels of satisfaction – presenting a challenge as relationships move from strategic to more of a tactical nature. This also represents an opportunity for CSPs to become innovative enablers of their customers’ business.

Elsewhere, 81% of respondents said 5G is strategically important or extremely important to their businesses and 77% expressed a strong desire to collaborate strategically with their CSPs around 5G.

Meanwhile, 79% said they are looking for CSPs to take the lead role in driving 5G technology into their businesses, demonstrating that a major opportunity looms on the ho-



**The first edition of the B2B Telecom & Tech Index found that 80% of surveyed respondents believe communications technologies are important or very important to generating new revenues**

rizon for service providers in the digital age.

“The first edition of our B2B Telecom & Tech Index highlights that enterprises are looking to tap 5G technology to create new revenue streams and improve operations,” Glenn Gibson, chief marketing officer, Hansen Technologies. “We have strong evidence that as end users, enter-

prises are keen to embrace new communications technology – and they want their CSPs to help them get it right. As we inch ever closer to a 5G-centric reality, the message is clear: if they can effectively align to capitalise on new opportunities, CSPs and enterprises are in a great position to monetise a digital future.” ■

## Connexin raises £80 to take smart cities to the next level

Smart city group Connexin has secured an £80m investment from a global fund to build “smarter, more efficient services”

The money marks an “initial commitment” from Whitehelm Capital, one of the world’s largest independent infrastructure managers.

Hull-based Connexin company said that the investment would support its expansion, with the aim of becoming the leader in smart infrastructure and the IoT sector.

“Whitehelm is delighted to partner with Connexin to support the development of digital infrastructure in the UK,” said Tom Maher, head of business development at Whitehelm Capital. “At a time when connectivity has become more important than ever, we have identified

a significant need to invest in regional networks and support local communities.

Connexin’s long and successful track record in providing connectivity services to these local communities, businesses and municipalities make it a perfect partner.”

Connexin co-founder Furqan Alamgir added that “this investment isn’t just about Connexin” in that it affects every community. “Everyone deserves clean air, tidier streets, safer roads,” he added. “By allowing all communities to have access to our digitally connected infrastructure, it enables connected devices to “speak” to one another which paves the way for amazing things.

The company uses an IoT foundation for its Smart City Operating System, with CityOS centralising information. ■



**Connexin said that the investment would support its expansion, with the aim of becoming the leader in smart infrastructure and the IoT sector**

## Oracle inks Ministry of Defence cloud infrastructure deal

Defence Digital, the digital arm of the UK Ministry of Defence (MOD), has selected Oracle’s cloud infrastructure to add to the MODCLOUD multi-hybrid suite of secure services.

The vendor said its flexible hybrid cloud infrastructure allows the choice and scale of technologies to handle data in a largely compliant environment.

Oracle Cloud Infrastructure (OCI) is an infrastructure as a service (IaaS) that provides on-premises high-performance computing power to manage cloud native and enterprise company’s IT workloads.

It is said to offer real-time elasticity for enterprise applications by combining the company’s autonomous services, integrated security, and serverless computing.

“The real opportunity of digital transformation—which includes artificial intelligence, machine learning, IoT, blockchain, and human interfaces—is to embrace data on a scale we’ve never seen before,” said MOD Defence Digital application services and dev ops head Brigadier Sara Sharkey. “Selecting Oracle Cloud Infrastructure within our MODCLOUD Multi-Hybrid suite of services offers new technologies that are

reshaping how we approach IT and using this information, allowing us to focus on innovation and outcomes for both business and importantly, people.”

Digital Defence will make the cloud infrastructure, integrated suite of business applications, and platform services available to the larger defence community. This will be made available under a pan-defence Oracle enterprise agreement, and through Oracle’s integrated collection of services under a ‘single-sign on.’

Oracle said that as a result the Ministry of Defence can access digital assistants, mobile hub, data visualisation, low code development tools, and emerging technologies.

“The Ministry of Defence will capitalise on the choice and economic benefits Oracle Cloud Infrastructure can provide, all of which will help meet challenges that lie ahead,” added Oracle UK senior vice president and country leader Richard Petley. “It joins a whole host of public sector organisations, such as the Home Office, Western Sussex Family Assist, Lambeth Borough Council, Croydon County Council, The Office for National Statistics and Scottish Water, which are already using Oracle Cloud.” ■

### EDITORIAL:

**Editor:** Robert Shepherd  
roberts@kadiumpublishing.com

**Designer:** Sean McNamara  
seanm@kadiumpublishing.com

**Contributors:** Gerry Moynihan,  
Craig Atkins, Mihaela Dinu, Jon  
Lederman, Olivier Subramanian

### 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

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 publisher. The views expressed in this magazine are not necessarily those shared by the editor or the publisher.  
ISSN: 2052-7373

# Microsoft retrieves data centre from Orkney

Microsoft has retrieved an underwater data centre just off Scotland's Orkney archipelago after two years of providing cloud services from the bottom of the ocean.

The 40-foot cylinder was descended into Scottish waters in spring 2018, powered by tidal turbines and wave energy converters.

Marine specialists took just a day to retrieve the data centre, which was coated in algae, barnacles and sea anemones from the seafloor after being deployed 117 feet deep – without affecting its operations.

Throughout its test period, 'Project Natick', as it is known to Microsoft, had a lower failure rate than a conventional data centres and reduced energy consumption.

Furthermore, the on-board servers – the physical electronic equipment that process data storage – were protected

from the surrounding water, supporting customers of its Azure cloud services.

Microsoft Azure is now looking to serve customers who need to deploy and operate data centres anywhere in the world.

The data centre was originally deployed at the European Marine Energy Centre, a test site for tidal turbines and wave energy converters and stationed in waters off Orkney.

US firm Microsoft has been testing the feasibility of keeping data centres underwater in the long term, which helps to keep low and consistent temperatures.

Project Natick has proved the concept of underwater data centres is "logistically, environmentally and economically practical", it said.

When the Project Natick cylinder was

hailed off the seabed around half a mile offshore, just eight out of the 855 servers on board had failed. Overall, the underwater data centre had one-eighth of the failure rate of a similar data centre on land.

All of Orkney's electricity comes from wind and solar power, but there were no problems in keeping the underwater data centre supplied with power.

"We have been able to run really well on what most land-based data centres consider an unreliable grid," says Spencer Fowers, one of the technical team on Project Natick. "We are hopeful that we can look at our findings and say maybe we don't need to have quite as much infrastructure focused on power and reliability. We were pretty

impressed with how clean it was, actually. It did not have a lot of hardened marine growth on it – it was mostly sea scum."

The container was brilliant white when deployed two years ago, but upon retrieval it had a thin coat of algae and barnacles. After being power-washed, the data centre was transported to Orkney for tests to be carried out on it and samples sent for analysis at Microsoft headquarters in Redmond, Washington, US. Microsoft researchers believe a sealed container on the ocean floor could provide ways to improve the overall reliability of data processing.

Once analysis is completed, the steel pressure vessel, heat exchangers, servers and all other components will be recycled. ■

## Smarter Technologies selected for G-Cloud 12

Internet of Things (IoT) solutions business Smarter Technologies has been selected as a supplier to help public organisations access cloud computing services.

The firm has been approved as a supplier on the G-Cloud 12 framework Digital Marketplace, which is managed by the governmental department, Crown Commercial Services (CCS).

The framework is an innovative procurement initiative for public sector bodies that use cloud computing, including central government, local government and important sectors such as health and education and emergency services.

So far, over £5bn has been spent via the first 10 versions of G-Cloud, which provides a simple route to market for SMEs to engage with public sector departments.

Furthermore, it is the second time that Smarter Technologies has been selected to be a part of the initiative, having previously been selected as a G-Cloud 11 supplier with the support of sister company Visionist.

"We are happy to cement our position for another year for public sector organisations to take advantage of our industry-leading cloud-based services," said Smarter Technologies chief technology officer David Miller. "We look forward to helping public organisations around the country realise greater efficiencies and cost-savings through our innovative and tailored technology solutions."

Smarter's solutions include network security, appropriate smart building and compliance recommendations, asset tracking and monitoring, recommendations for utilities brokerage and other business services. Its client base includes many recognised institutions including the MOD and NHS. ■



So far, over £5bn has been spent via the first 10 versions of G-Cloud

**HellermannTyton**



Arriving December 2020

I wish we could say more...





## Making the case for an RMM

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

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

### Improve end-user productivity

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

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

### Make technicians more efficient

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

### Improve security

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

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

**ninja**  
RMM

Interested in getting your hands on the #1 rated RMM? Visit [www.ninjammm.com](http://www.ninjammm.com) for a free trial.

## Cardo Crew launches mesh comms tech

Wireless intercom specialist Cardo Crew has launched a new mesh communication solution that could “transform personal protective equipment (PPE)”, as well as improve communications and safety in the construction sector. The Cardo Crew PRO-1 is a lightweight mesh communication module that fits inside PPE such as helmets and ear

guards. It is designed for PPE manufacturers to introduce team communication to busy, noisy, or hazardous environments, helping to prevent work-related incidents and improve on-site safety. According to the health and safety executive's 2019 UK statistics, the rate of non-fatal injuries to construction workers has risen for the first time in five years.

## ‘Data centres face climate challenge’

Data centres in Europe face major challenges as climate change affects the continent's weather, according to a survey of data centre consultants from the UK, Ireland, France, Germany, the Netherlands, Sweden and Norway. The report, commissioned by temporary power, cooling and heating provider Aggreko, found that countries are not confident in the grid's ability to power their facilities and believe they may be ill-equipped to deal with temperature rises linked to climate change. Third-party research group, Censuswide, compiled the report from 700 questionnaires filled in by respondents who “provide specific consultancy to data centre operators, with regards to design, energy and engineering”.

## Expanding threat landscape a concern

A new survey of cybersecurity experts by Gartner found that analysts are most concerned about the rapidly evolving threat landscape, which has changed rapidly since the onset of the Covid-19 pandemic. Gartner conducted the Security and IAM Solution Adoption Trend Survey online in March and April, taking responses from 405 experts in western Europe, North America and the Asia/Pacific region. Hundreds of those surveyed said the coronavirus pandemic had changed the way attackers were attempting to infiltrate systems and had led to a new, diverse array of cyberattacks that will continue to evolve over the next three to five years.

## Nearly half of IT bosses yet to upgrade security

Nearly half (47%) of UK IT bosses have not updated their security strategies to account for their move to cloud environments, putting their businesses at higher risk of cyber-attack, according to a new study by Trend Micro commissioned for CLOUDSEC Online. The survey showed that many IT leaders are keen for a single platform to provide cloud and on-premises security, with lack of integration between the two types of tooling cited by 43% of respondents as the biggest barrier to the adoption of cloud security. Additionally, 33% stated that this integration issue was their biggest day-to-day operational headache.



## TP-Link delivers Omada cloud networking business solution

TP-Link has launched three new cloud-enabled products in its Omada range. Equipped with fast dual-band Wi-Fi speeds totalling 1750 Mbps\*, MU-MIMO, Load Balance and professional antennas, the EAP265 HD access point connects more devices simultaneously

and improves capacity in high-density environments. The EAP265 HD supports both standard 802.3af and Passive PoE (PoE adapter included) for flexible installations, while the JetStream TL-SG2210MP and TL-SG2428P Gigabit Smart PoE Switches provide high-speed

connections for various networks, device and site requirements. TP-Link's TL-SG2210MP switch has a 150 W PoE power budget with 8x 802.3af-compliant PoE+ ports and 2x gigabit SFP Slots and abundant security strategies enabled by built-in LAN area investment protection.

## NTT's Global Data Centers begins construction of Hemel Hempstead 4

Global Data Centers, a division of NTT, has recently begun construction of its new Hemel Hempstead 4 data centre, located just north of London. It will join NTT's company's other current UK expansion project, London 1 in Dagenham and its five completed data centres in Hemel Hempstead and Slough. On completion, the facility will have 9,600 sq m (100,000 sq ft) of available data centre space and support 24MW of IT load. The first phase is expected to open in Q4 2021. NTT is investing a total of around £500m on these expansion projects in the UK market, giving it a London hub of data centres with a total capacity of 100MW. All of NTT's London facilities are interconnected with one another. This means each facility can offload storage to other facilities improving its resiliency and disaster recovery capabilities. “We



continue to expand to meet the demand from our clients for high-quality data centre space and to protect the growing volume of their sensitive data,” said Florian Winkler, CEO EMEA of Global Data Centers.

## Northumbria University hacked

Northumbria University was hit by a cyber-attack, which led to exams being cancelled and the clearing hotline being disrupted. It said there had been “operational disruptions across networks and IT systems” on Friday, August 28. The university said “immediate action” had been taken to mitigate the impact and it was working with external specialists who have launched an investigation. The Information Commissioner's Office and police have been informed. “The investigation is still at an early stage and we are currently assessing the scope of the incident,” the university said in a statement. Students were told that the campus would be closed for the rest of the week. However, people can still access limited services, including email, office applications and video conferencing tools.

## New Intelsat service for enterprise users

Intelsat has introduced a new service, which helps enterprises' end users to access their cloud applications anywhere, anytime. Initially available to Intelsat FlexEnterprise customers, Cloud Connect currently supports Microsoft Azure ExpressRoute connectivity via the FlexEnterprise managed service, providing network service operators and the businesses they serve, with a new level of flexibility in adopting a growth-oriented cloud strategy. Last year, Intelsat became an Azure ExpressRoute partner, enabling enterprises to private access Microsoft cloud services from anywhere, which it claimed was “a more secure and consistent experience than the public internet offers”.

## Word on the web...

**Welcome to Switzerland: visit our website to read this month's post by Adrian Brookes, solutions strategy and pre-sales director, Infovista...**

**To read this and other opinions from industry luminaries, visit [www.networkingplus.co.uk](http://www.networkingplus.co.uk)**





Just like today's industrial leaders, Rajant's network is

# Smart. Autonomous. Always moving.

Rajant Kinetic Mesh® is the only wireless network to power the non-stop performance of next-gen applications—from real-time monitoring to robotics and AI.



Works peer-to-peer to maintain **hundreds of connections simultaneously** for 'never break' mobility



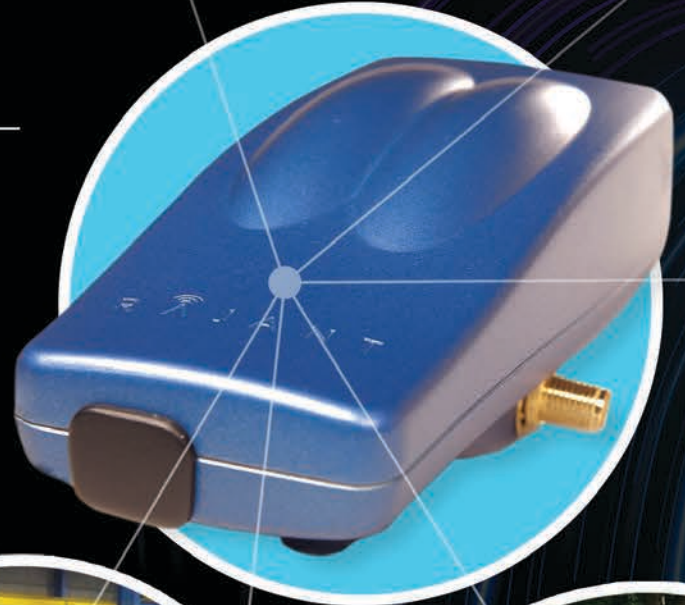
Intelligently self-optimizes to **change in real-time**, ensuring mission-critical reliability



The *only* network to enable **machine-to-machine communications** required for autonomy



Provides **Industrial Wi-Fi** for **extended Wi-Fi connections** in challenging environments



**IF IT'S MOVING,  
IT'S RAJANT.**

Industrial Wireless Networks **Unleashed.**

**RAJANT**

Request a free demo at [rajant.com/networkingplus](http://rajant.com/networkingplus)



# Moving from blocker to enabler

The IT landscape and world of security are changing. Olivier Subramanian, account principal at Contino, explains

Change often brings about a sense of fear and anxiety, and therefore a reluctance to shift to a new way of working. This sense of 'being outside your comfort zone' prevents individuals and organisations from executing real change and embracing the public cloud.

We often see disappointing and frustrating outcomes, when old world thinking and behaviours are applied to the new world. The CISO and security function becomes a blocker, instead of enabler.

Many public sector organisations have been embracing public cloud and understanding the difference between the old and new world is a key ingredient when enabling change.

The traditional approach to IT security was to ensure the edge was secure and that the doors and windows were closed, thus securing the perimeter. I call this the Egg model.

The changing threat landscape of public cloud is forcing the adoption of a strength and depth approach to security with controls on each component of the architecture. I call this layered approach the Onion model.

The adoption of modern DevOps delivery techniques is helping to shift security to the left. This involves building security controls into the platform and application, performing automated security testing as part of the Continuous Integration process, and the introduction of continuous compliance assessment at build and run.

Given the scope and pace of change, it is unrealistic for an individual to remain completely up to date on all things cloud.

The modern CISO must become an enabler to ensure that the business achieves agility and value of running its services in the public cloud.

The starting point is to trust the cloud and the CSPs. As a CISO you need to validate the respective security and governance controls yourself.

Each CSP lists the standards and compliance they have achieved through audit reports and attestations:

- Azure: Service Trust Portal
- AWS: AWS Artifact
- Google: Cloud Compliance & Regulations Resources

It is important to satisfy yourself that these independent audits and certifications provide sufficient information to meet your security and compliance requirements. Under-

standing how these standards align to the UK Government security classifications is a key aspect of the Public Sector CISO. The key standards to familiarise yourself with are CIS, CSA and NIST. In my experience Public Cloud solutions have been built to successfully satisfy

OFFICIAL and OFFICIAL-SENSITIVE classification. SECRET and TOP SECRET are outside the capability for standard Public

Cloud to satisfy due to the global nature of the services and support capabilities.

When you move to the Public Cloud it is important to review the threat landscape and identify the threat actors. The primary actors to consider are:

- Bad company system admin - company admin that has access inside your cloud environment and takes negative action
  - Bad company tenant - this is where there is a malicious activity happening within your cloud tenancy that impacts others
  - Bad CSP system admin - a cloud service Provider admin that has access to the cloud fabric and takes negative action on customer services
  - Bad CSP Employee - a cloud service provider employee that takes negative action
  - Naughty neighbour (in the cloud) - Another tenant in the cloud taking action on other tenants
  - Eavesdropper - listening in to ingress/egress traffic collecting customer data
  - Malicious external party - a party not associated with the customer or the CSP that seeks to access the cloud
  - Supply chain attack - A party that takes action on the CSP upstream supply chain.
- The next stage is identifying the key threats to your public cloud environment across the supply chain. Some example could be:
- Unauthorised code - has someone introduced weak or malicious code
  - Data breach - customer data is copied
  - Customer admins have "god" status and full control - this increases the blast radius of human error or malicious actions.
  - CSP admins have "god" status.
  - The DevOps tool chain is not controlled - fully automated pipelines allow bad or malicious code to be deployed automatically.

Having built your knowledge, work with your senior engineers and CSP architects to identify all the mitigations that are needed to manage the threats identified.

This is where the public sector CISO can make a massive difference to the organisation, by driving security to the heart of the organisation culture. I recommend three steps to drive this culture change:

**Educate:** as a starting point I recommend that the IT security teams should build their knowledge in the key cloud concepts:

**Embed:** adopt the cross functional team concept by embedding empowered security personnel into engineering teams. They have delegated authority and knowledge to make relevant security decisions that are within the bounds of the project.

**Evangelise:** the final task on the journey is to educate the wider community from the c-suite to operations and be seen to champion IT Security and how it can empower the business.

As IT has embraced the latest innovations of public cloud and DevOps ways of working, the role of the public sector CISO is becoming more important.

The journey to becoming a modern CISO is rooted in trust. Trust the cloud and CSPs and enable the IT Security teams and community to drive change.

Olivier Subramanian, account principal, Contino

# New, high speed Gigabit routers, ideal for small business and remote working

Introducing the DrayTek Vigor 2927 series



Business class networking solutions manufacturer DrayTek is delighted to announce the introduction of the Vigor 2927 series. This new line of DrayTek routers offers dual Gigabit WAN throughput, enhanced broadband failover, wireless and firewall VPN features - perfect for small business, home offices and remote workers.

The DrayTek Vigor 2927 series will help users make the most of fast, fibre-to-the-premise (FTTP) broadband connections and includes many features for security, segmenting users, load balancing, content filtering, Quality of Service and remote management.

"Building on the success of the Vigor 2926 and 2925 series, DrayTek UK/IRE is excited to offer new routers for small offices and demanding home offices," stated Julian Hubble, DrayTek Sales Director. "The Vigor 2927 delivers the reliability and flexibility you expect in a DrayTek product, all with a total NAT throughput of 1.8 Gbps or 950Mbps per-WAN."

For small businesses - connecting multiple sites or remote workers - the Vigor 2927 series supports up to 50 concurrently active VPN tunnels, with fast and secure IPsec VPN tunnels.

Home office users can address the challenges of sharing bandwidth with multiple household members with the DrayTek App QoS. This application based Quality of Service simplifies setup significantly by allowing users to select which latency-sensitive applications they wish to prioritise, such as Zoom and Skype. Voice traffic (VoIP) is automatically prioritised through the router without additional configuration.

With multiple LAN subnets and VLANs, the Vigor 2927 can manage up to 8 separate networks. Each network can have its own Content Filtering, Firewall, Quality of Service and Route Policy.

For users who need fast and efficient wireless networking to computers and devices, the Vigor 2927 'ac' models has AC1300 Dual-Band wireless and can also be used as a Mesh Root within a DrayTek Mesh wireless system.

DrayTek offers superior broadband failover options. The Vigor 2927 'L' models, with two SIM slots, is ideal when connectivity is mission critical. In the event of an ISP service interruption, the router can switch to a mobile broadband connection using one of the two SIMs.

The Vigor 2927 series is compatible with DrayTek's cloud-based centralised management platform, VigorACS, which provides a cost-effective full management system for your entire network across multiple

"Building on the success of the Vigor 2926 and 2925 series, DrayTek UK/IRE is excited to offer new routers for small offices and demanding home offices"

sites. The Vigor 2927 can also manage DrayTek VigorAP access points and VigorSwitch switches connected locally to the router.

Vigor 2927 Series Key Features:

- Gigabit Dual-WAN Ethernet WAN Router with Load Balancing & Failover
- Up to 950Mbps Throughput per WAN interface, 1800Mbps in total
- Up to 300Mbps IPsec VPN Throughput
- 50 LAN-to-LAN & Remote Teleworker VPN Tunnels
- 25 DrayTek SSL VPN Tunnels
- 5+1 Gigabit RJ-45 LAN Ports
- 4G/LTE with dual-SIMs for second backup telco ('L' models)
- AC1300 - 11ac 'Wave 2' Dual Band Wireless ('ac' models)
- 8 LAN Subnets with VLANs (Port-based / 802.1q)
- SPI Firewall and Content Filtering
- Compatible with VigorACS centralised management platform

DrayTek UK has marked a fast and steady growth to become a leading manufacturer of business class broadband and networking solutions. Today, we offer a complete range of business networking gear, including wireless, switching, routing, security, along with services such as central management system. DrayTek's business philosophy is focusing on promoting high-performance, cost-efficient and reliable networking solutions that will help businesses exploiting the full potential of the Internet.

For more information, please contact:

UK/IRE Sales Contact:  
info@draytek.co.uk

Main Tel: 0345 5570007  
Website: www.draytek.co.uk

**DrayTek**



# When business continuity plans go wrong

Craig Atkins, managing director, 1-Fix

Covid-19 has been a great test of company's business continuity plans. The firms that had solid plans jumped into action to implement them, with varying degrees of success, and those that didn't have them – or hadn't reviewed them since drafting them years ago – quickly scrambled around to get themselves operational.

The heartening thing with this whole situation has been that, on the whole, most companies have been able to adapt and get themselves back up and operational in a very short time period, indicating that their continuity plans were well designed and executed.

However, it is not all sweetness and light. As the MD of an IT managed services provider I've seen some great examples of both good and bad business continuity plans, and I've got a couple of examples of recent real life failures of those plans to share with you so that hopefully you don't make the same mistakes that these companies did. The first example I have is from a company in the service industry sector.

They had what appeared to be an excellent business continuity and disaster recovery plan, and they ran regular tests and scenarios against the plan – something that many other firms don't do, or at least not as regularly as they should. They felt like they were well prepared for most disaster scenarios, as they already had 75% of their workforce working remotely (although crucially not the admin & back office teams).

Their plan had a full process for what should happen if the office is inaccessible, which was then implemented once lockdown had been announced.

The plan stated that initially they would provision some key business critical staff with spare IT equipment that was kept on-site, and then over a period of a few days they would source and supply the remaining staff with computers and remote communication tools once they had determined how long the office would remain inaccessible.

Unfortunately, the plan they had designed, although ideal in the scenario of office inaccessibility through natural disaster, terrorism, or other threats isolated to their own business, had not considered what should happen in the event of all businesses being forced to do the same thing.

When they came to source the equipment that they required for the staff to work remotely it was almost impossible to get all the items they needed, due to high demand.

Luckily, they managed to source enough equipment – and loosen their "bring your own device" policies to allow home users' machines to be utilised for work – so they adapted short term.

Longer term, their revised plan is now to switch many of their older desktop machines out for laptops which can be easily taken off-site in the future.

They are also planning to keep a smaller cache of equipment available at a second site location in case a disaster rendered all the main office machines unserviceable. In a very similar manner to the first example, this particular company – an accountancy firm with 30 staff – had considered the scenario of their office being unavailable, but they had not foreseen it being for longer than a few weeks.

Their plan had determined that a longer office closure would have resulted in a temporary re-location to a service office environment, and the sourcing of a new site if the closure was permanent.

They had been considering upgrading their telecoms for some time but were still 'sweating the asset' of a traditional PBX phone system

that was physically located in their office.

Their disaster plan for their communications was to forward the calls from their inbound number to an emergency mobile phone, take messages and ask their staff to use their own communication devices to make calls back to the customers.

Unfortunately, once this plan was put into action it was very quickly apparent that it was flawed. Firstly, the plan relied on one member of staff to take all the calls inbound to a company that previously had 30 staff available to answer the phone.

Secondly, due to self-isolation the person who had the phone was unable to pass it over to another staff member to help share the duty.

They attempted to work around the issue by trying to forward out calls to multiple staff mobiles, but it soon became apparent that their fixed line phone system was a millstone around their neck when it came to flexible working.

There was also the compliance issue of a lack of call reporting and metrics from staff using their own devices to make calls, and the reputational issues caused by bad lines, poor signal, and the inability to present the corporate number on outbound calls.

Thankfully the major VoIP network providers were still able to onboard new clients while in the midst of the pandemic, so this company were able to get their

staff set-up with softphones on their computers or mobiles and pushed through a very quick migration of their phone numbers onto the cloud.

Having put our continuity plans to the test during Covid-19, the most important thing for all businesses is that we now take the time to analyse what we did well, what we could have done better, and what didn't work at all. Finally, don't be afraid to play devils advocate when analysing the plan – ask lots of "what ifs", after all, I'm sure not many of us expected the "what if" of a global pandemic but we're all going to finish with a better, tested continuity plan at the end of it all!



## Total Control in Computing

### Specialist suppliers of Datacentre equipment

### call for a quote today!

See our latest 'working from home solutions'

HASSLE FREE PROCUREMENT OF: IT / POWER / INFRASTRUCTURE EQUIPMENT



**Raritan** **ADDER** **ATEN** **mcab** **PatchSee** **AUSTIN** **IEC** **LOCK** **addon** **PDUeX** **iPower**  
**MINKELS** **FUJITSU** **APC** **ProLabs** **ROSE ELECTRONICS** **Smart-AVI** **SPOOK** **Sunbird**

[sales@kvmchoice.com](mailto:sales@kvmchoice.com) | [sales@pduchoice.com](mailto:sales@pduchoice.com)  
[www.kvmchoice.com](http://www.kvmchoice.com) | 0345 899 5010





# GDPR post Brexit: what should firms expect?

**The UK has finally severed ties from the EU and will now plough a lone furrow. But what does that mean for data and GDPR? Robert Shepherd asks the questions**

**D**ata privacy has been a focal point among government leaders and business executives for a number of years.

In the wake of major scandals involving the likes of social media giant Facebook and telecom group Talk Talk, officials have joined forces to enact measures like GDPR in an effort to curb the mishandling of data — and give peace of mind to the public at large about their personal information and how it is shared.

However, the world is now in a very different place to when the General Data Protection Regulation (GDPR) law was made in 2016 — the year the British public voted to leave the European Union (EU) — and implemented in 2018.

Whether you voted for it or not in referendum, we have got “Brexit done” and severed ties with 27 EU member states in a bid to plough a lone furrow and “make our own laws”. Then there’s

the small matter of the world at large running a Sunday service as it tries to deal with the Covid-19 pandemic.

Prior to the pandemic, one couldn’t move for news coverage of Brexit, GDPR and what “deal” prime minister Boris Johnson was going to announce on the steps of 10 Downing Street or in the House of Commons. Businesses and customers alike were still facing widespread data privacy issues and discovering the limitations and flaws of policies like GDPR. These include thousands of recent data breaches because of continued gaps in protection, and millions of dollars in fines for businesses that didn’t protect their customers or continued to misuse their privileged information. There are also complaints that government agencies are underperforming in their own measures, such as resources allocated to data protection watchdogs.

A significant component of the Covid

recovery plan involves location tracking of patients and “contact tracing,” or logging details about the people who have come in contact with infected individuals. Now, there are plans afoot to see pregnant women who drink alcohol have all their consumption recorded on their baby’s medical records — even if they only had a single glass of wine. In other words, a near-future flurry of personal data leading to new privacy risks is a massive understatement.

On the plus side, the Data Protection Act (DPA) 2018 is the UK’s implementation of the General Data Protection Regulation (GDPR) was passed to support the UK’s withdrawal from the EU. But what does that mean for enterprises in plain English?

“The one-word answer is ‘uncertainty,’” says Bill Gornall-King, partner at law firm Boyes Turner. “Most of the GDPR provisions have been incorporated

in the DPA 2018, but the key question to answer is, with the UK being a third country from 1 January 2021, will EU member states be permitted to transfer personal data to the UK as now (and bear in mind that vast quantities of European data are processed in UK data centres)?”

Gornall-King further argues what is needed is an EU ‘adequacy decision’, adding that the recent Schrems II decision of the European Court of Justice (ECJ) in the long-running dispute between Austrian lawyer Max Schrems and Facebook Ireland, which has seen the dismantling first of the EU-US safe harbour as well as its replacement ‘Privacy Shield’ could cause the UK difficulties in achieving ‘adequacy’ in view of the UK’s own surveillance laws and its membership of the Five Eyes Alliance. “The UK faces the stark choice of maintaining current high privacy



standards or the lower standards of the USA and elsewhere,” he says. “If the UK moves towards the latter it will be problematic for businesses to move personal data to (or through) the UK.”

However, Tim Brown, vice president, SolarWinds holds the belief that not much is likely to change for enterprises. “If an enterprise is GDPR certified it should receive the new certification without too much trouble,” he says. “The UK’s interpretation of GDPR is likely to resemble the current model so enterprises should expect to continue following similar requirements, such as satisfying data subject right requests. The rules aren’t likely to be rewritten; it’s the processes of administration, controls, and penalties that are likely to be updated.”

It’s a view shared by Olivier Subramanian, account principal at Contino, who says

GDPR has been a big step forward in data protection and the management and organisation of information. “However, this change has come at a cost and created a great deal of uncertainty when first introduced,” he says. “If the UK pursues an independent data protection policy it is difficult to predict what the benefits will be. However, it is clear to me that a different policy will bring change, cost and uncertainty to the business world.”

Although the 2018 legislation allows organisations “to continue business as usual” without having to interpret a new or different law to the EU, Neil Thacker, CISO EMEA for Netskope, says it also allows the UK to maintain good terms with the EU and supports and simplifies future trade agreements.

“However, that said, a major challenge will be the changes and ruling by the EU on international data transfers,” he says. “At the end of the transition period and starting on exit day, the UK will become a third country, so a data transfer agreement will need to be established before data can flow freely between the UK and EU and vice versa. It is yet to be confirmed whether the EU will immediately give the UK an adequacy decision or indeed, any decision at all. Alternative options do exist, with many organisations already ensuring they have any data transfers covered by legal contracts with their service providers. These contracts with their providers and data processors will likely include Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) which are both considered valid on a recent ruling by the CJEU.”

For Rick Goud, founder and chief executive officer at Zivver, a secure digital communication provider, the ECJ decision is very relevant for UK data protection because this incident could potentially impact future data adequacy decisions countries seek with the EU.

“When the current GDPR is no longer binding in the UK in 2021 (from 1 January) and new data protection legislation is introduced, the transition can be done smoothly if the regulations are functionally similar,” Goud continues. “British lawmakers were, after all, involved in crafting the original GDPR, so any deviations should ideally be minor. A synergistic approach to data protection would greatly help facilitate data flows between the UK and its largest trading partner, the EU, posing minimal disruption for businesses and cross border commerce. Additionally, many companies have already developed their processes and invested in their systems to be GDPR compliant since it came into effect over two years ago. Put plainly, organisations have enough on their plates these days, and lawmakers can help by limiting any changes to GDPR regulations in the UK to those that are strictly necessary.”

As you can imagine, there are a number of established law firms and pop-up “experts” ready to help enterprises who still can’t see the wood for the trees. Conexus Law, a specialist advisory firm is urging companies to prepare for the strong possibility that the EU will fail to agree that the UK has an “adequate data protection regime” after the transition period at the end of the year. The firm says it means that businesses will face barriers transferring personal data to and from the UK to EU countries under GDPR.

“The UK’s use of mass surveillance techniques, our Investigatory Powers Act and our membership of the Five Eyes intelligence sharing community has raised particular concerns with the EU – especially in relation to the sharing of data with the US, and even more so given the recent Schrems II decision on the Privacy Shield scheme,” says Conexus Law founder Ed Cooke. “What is clear is that once a decision has been made then companies will need to move quickly to ensure they are not severely impacted.”

Cooke adds that failure to reach an agreement would mean that companies will need to look at alternatives such as Standard Contractual Clauses and binding corporate rules. He reiterates that merely relying on consent is not really an option for most businesses.

“Each of these options has its challenges with consent generally viewed to be unworkable as it can be revoked at any time,” Cooke says. “Standard contractual clauses were upheld in the ECJ in its judgment on Privacy Shield, but the judges did cast some doubt on whether or not these offer suitable protection in all cases without businesses adopting further practical measures such as encryption, to ensure the protection of personal data.”

Does that mean businesses should be

**“At the end of the transition period and starting on exit day, the UK will become a third country, so a data transfer agreement will need to be established before data can flow freely between the UK and EU and vice versa.”**

Neil Thacker,  
CISO EMEA,  
Netskope



**A significant component of the Covid recovery plan involves location tracking of patients and “contact tracing,” or logging details about the people who have come in contact with infected individuals**

worried? Gornall-King says the Schrems II case “has thrown another grenade into the room anyway” and as its findings have yet to be fully reconciled with current practice across the EU (and UK). “The message to businesses is not to panic but to take advice and action,” he adds.

Cooke concurs and says his firm is advising companies to start preparing now. He recommends that companies should already have a full audit of what personal data they collect and where it is stored and transferred to, including back-ups that may be held by cloud-based providers with datacentres all over the world. This audit needs to include all suppliers and partners that data is shared with. Then, the next stage is to look at standard contractual clauses and decide whether further measures are required based on the specific data being transferred. If not, consideration should be given to additional methods such as encryption,” argues Cooke.

“It seems that an adequacy ruling under GDPR is being used as a Brexit bargaining chip in relation to other unrelated diplomatic negotiations taking place,” he concludes. “Unfortunately, businesses may end up bearing the brunt of this and I would highly recommend that they start to prepare now.”

It has already been noted that the UK will need adequacy to GDPR if it wants full access to the EU markets and Mark Ruchie, vice president, chief information security officer for Entrust, says the “overall global trend” is that countries are increasingly focused on protecting information and ensuring consumer privacy. He adds that as countries create their own data privacy and protection regulation they have used GDPR as the model, citing Brazil and the US state of California as examples of jurisdictions that have recently enacted data protection regulation.

“Regardless of the regulations, organisations need to focus on protecting PII, healthcare data, bank and credit information or any other sensitive data,” Ruchie continues. “Organisations can solve these problems by encrypting all of their data and ensure strong identities for their employees to access their networks. This solves two main problems: 1) Strong identities (backed by a certificate) prevent bad actors from accessing the networks, applications and data. 2) Also using new technologies like passwordless authentication and single sign-on reduces the friction for employees when accessing networks and applications, improves security and, in some cases, elim-

inates passwords and replaces them with biometrics. Encryption ensures that if a data breach were to occur the information would be encrypted and useless to any bad actor. Also in GDPR and other regulations, if the data was encrypted it is very likely to be exempted from data breach notification since such protection de-risks the impact on individuals’ rights and freedoms. Encryption or lack of it (depending on the data at risk) can also be one of the important consideration factors for the data protection authorities in awarding financial penalties in the case of a data breach. For security-minded organisations, designing a data privacy program that complies with more mature regulations, such as the GDPR, will allow them to stay nimble and adjust more quickly as new regulations come into force—rather than having to constantly scale up.

The primary challenge, since the GDPR was enforced, is that the internet allows for data to flow freely across borders and for many organisations that use the cloud – aligning these data flows with contractual agreements has been difficult. Thacker says that today, every organisation is mandated to maintain an up-to-date Record of Processing Activities (ROPA) both under Article 30 of the EU GDPR and section 61 of the UK DPA 2018. “In summary, a ROPA is an inventory for all personal data an organisation holds, where it is held (geolocation etc.) and what data controllers / processors are used. With large enterprises consuming over 1000+ cloud apps (and every cloud app provider likely to be a data processor) maintaining this record and understanding which provider has a valid contract covering data transfers is not a simple task especially with shadow IT being commonplace for most organisations,” he says. “For enterprises across the UK and EU, now is the time to ensure their ROPA’s are regularly updated and that visibility is sought into every new data controller / data processor agreement. In addition, employees should be educated in real-time when they attempt to upload personal data records to a cloud app that does not have a valid agreement in place. Technical controls such as a Next-Generation Secure Web Gateway (NG-SWG) and / or a Cloud Access Security Broker (CASB) that align with the organisations ROPA and can be used to identify and apply this level of control.”

However, Goud implies that there may not be a blanket rule for all in that sector specific data protection standards are evolving.





“When it comes to data protection legislation, many of us tend to think of the GDPR or the DPA, but there’s much more to be aware of than that,” he adds. “That’s because industries such as healthcare and legal are rapidly adopting their own standards to facilitate secure digital communications for their specific needs. We’ve seen this recently in the Netherlands, where a new standard for exchanging ad-hoc digital communications in the healthcare sector, known as the NTA 7516, was introduced earlier this year. The legal sector also has plenty of incentive to transform how communications can be safely exchanged, as many law firms still rely heavily on fax machines or mail couriers to send communications. Establishing these new standards can help companies transform how they interact with their contacts, while creating new opportunities and cost savings potential. You can expect to see more of this in the UK, the rest of Europe and beyond in the coming years.”

Regardless of what laws are in place, security remains key for enterprises and so many will want to know what they could expect to happen now that the UK is no longer part of the EU.

Should enterprises have security fears as a result of Brexit, or is that just more scaremongering being pedaled by the editors on Fleet Street?

“Change always creates opportunities – for businesses it offers a chance to grow or scale, but for the bad guys it is an opportunity for them to profit off uncertainty,” says Brown. “Look no further than Covid-19 which saw a sharp increase in phishing, ransomware attacks, and other scams. But enterprises shouldn’t have specific security fears; rather they must be wary that the UK will be undergoing change which can create gaps and opportunities that weren’t there before.”

Still, Brown says the UK should feel pressured into introducing new knee-jerk legislation and shouldn’t evaluate if the GDPR regulation works, but if the model works. “For example, do penalties work as a deterrent, do the administration processes work and is the method of reporting accurate?” he continues. “If the UK finds that the model isn’t working, this offers a chance to evoke change to help mitigate specific concerns. The UK must also consider if the regulation is purely a privacy initiative or if it could drive the economy as well. The new regulation could state that all data collected must remain within the UK, for example. Not only would this spur the number of data centres and equipment required, but also create jobs. Yet this pressure to review and perhaps change processes will come from those within the UK.”

Nevertheless, it’s already getting interesting ahead of the end of the Brexit transition period. The afore-mentioned Facebook last week threatened it might not be able to provide its platforms in Europe under new regulatory changes, it has threatened. The company said it would not be able to operate on the continent if it cannot move user data between Europe and the United States. Indeed, the Irish Data Protection Commissioner has suggested that it would enforce a European Court of Justice ruling that would mean such data transfers would breach (GDPR).

The general consensus is the concept of GDPR will prevail in the UK regardless of what deal is signed. “While the name might change, and processes might become more effective, the privacy rights will remain,” says Brown. “The notion of maintaining privacy and data protection, which underpins GDPR, is essential, and is a model which is

being implemented around the world.”

Nevertheless, there’s no navigating the fact that GDPR is still going to be relevant post-Brexit and Nigel Thorpe, technical director, SecureAge reinforces that any organisation that works with European businesses or consumers will still need to comply in order to continue operating in the territory. The UK will also retain data protection legislation which, in the short term at least, will continue to look a lot like GDPR.

“Whatever the future means in terms of changes to UK or European data protection, the principles of GDPR remain good business principles,” says Thorpe. “What consumer is going to trust an organisation which has poor controls over their personal data? And ‘security by design’ is just good business sense. In today’s world of

**“British lawmakers were, after all, involved in crafting the original GDPR, so any deviations should ideally be minor.”**

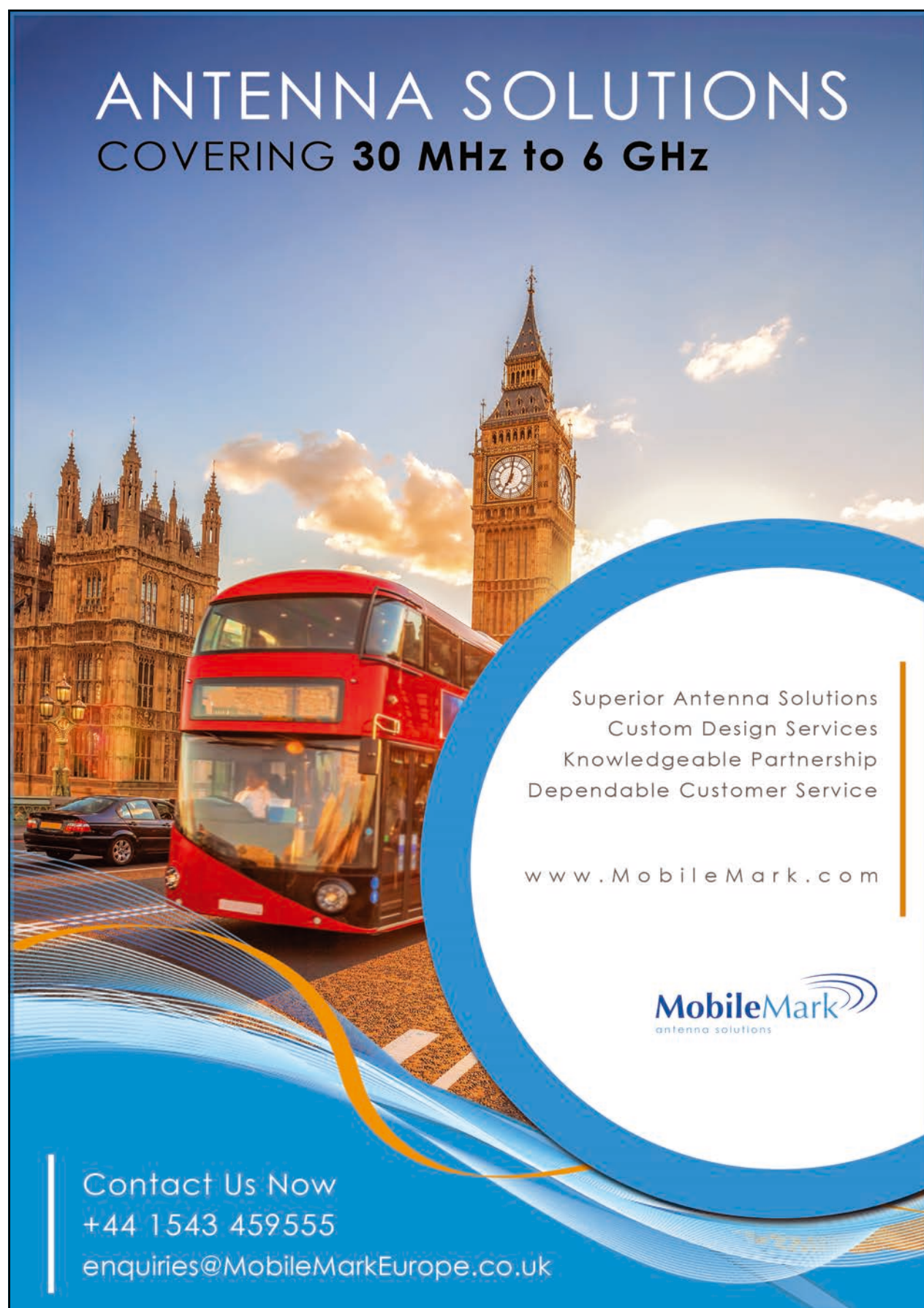
*Rick Goud,  
founder & chief executive officer,  
Zivver*

immediate news coverage, customer trust in an organisation can be lost in seconds, so doing all that is possible to mitigate security threats is an essential investment.” No doubt, things will be a lot clearer in early 2021. Even if there is still lots of uncertainty. ■



# ANTENNA SOLUTIONS

## COVERING 30 MHz to 6 GHz



Superior Antenna Solutions  
Custom Design Services  
Knowledgeable Partnership  
Dependable Customer Service

[www.MobileMark.com](http://www.MobileMark.com)

**MobileMark**  
antenna solutions

Contact Us Now  
+44 1543 459555  
[enquiries@MobileMarkEurope.co.uk](mailto:enquiries@MobileMarkEurope.co.uk)



# Full marks: new IT aids learning

## No blackboards: colleges and schools report on how tech is transforming education



### New IP system increases safety in schools

Loughborough Schools Foundation, a group of four independent schools and a nursery, with a total of just over 2,500 pupils.

Three of them share a campus: the all-boys Loughborough Grammar, founded in 1495, which has 849 pupils (and 74 boarders); Loughborough High, with 650 girls; and Fairfield Preparatory which has 506 pupils.

Loughborough Amherst School, founded in 1841 as Our Lady's Convent School, has 359 pupils; and a day nursery looks after 64 children.

The foundation had two separate phone systems and decided it needed a single product which, importantly, would provide features such as classroom lockdown, campus-wide messaging and a lock-out and lock-in function.

It also wanted a system to enable staff to more efficiently communicate with each other, pupils' families and emergency services.

An evaluation was carried out by the foundation's IT director, Richard Smeeton.

The foundation engaged Evoke Telecom, based nearby, which installed an Avaya IP system which connects more than 600 Avaya handsets in classrooms and offices in the four schools.

Now staff can communicate through traditional phones, simultaneous SMS messages, as well as through screen pops on computer terminals and broadcast messages over speakers and digital radio. The system has the ability to carry out both lockdown and lockout instantly across every campus, potentially including the ability to control electronic door locks. This is functionality that wasn't possible with the disparate mix of phone systems and handsets the Foundation was using previously. And the system has been programmed so that pupils cannot use it for external calls.

Mr Smeeton said: "Not only can we now give parents better peace of mind, but because external communication is now much more efficient, school admin staff have been reporting how much easier it is to find pupils who missed registration."

"Our IT support has also been transformed with direct contact reducing ticket numbers and resulting in faster resolution and less wasted lesson time. It is simply not acceptable that students often have more means of effective communication between them than teachers..."

"Above all, we believe that student safety and effective school operations shouldn't be held back by a lack of investment."

Pictured: the £2.1m Parkin Sports Centre on the campus, designed by A+G Architects and built by Stepnell.



### Online made easier thanks to update

With more than 11,000 students, Bournemouth & Poole College (BPC) is the largest provider of further education and apprenticeships in the region. Its core focus is on work skills, so that students are well placed for their chosen careers.

The college uses a free and open source learning management system called Moodle. Following student feedback, the college decided to modernise its Moodle digital learning environment (DLE) with more engaging features for both staff and students.

Although its main website carried the latest news and events students did not visit this website while accessing the DLE.

The college turned to its DLE provider CoSector – University of London to update its Moodle platform to include features such as a new learning resources section and a modern looking front end.

It also needed continued hosting and support so it could continue to be used in a variety of ways. For example, students needed to be able to upload their work from different platforms, make edits and submit it for marking within a particular timeframe. Teachers needed to be able to access work submitted from any location, at a time that suited them.

CoSector managed the migration and upgrades, ensuring all content was secure. BCP says that with all important links in one place means educators and learners can access all the key information in the same place at the same time.

Now data can be accessed at any time regardless of device and the college reports that teachers can now mark and grade student assignments – and insert comments and annotations – far more easily.

Students have simplified access to research materials and campus facilities, such as Box of Broadcasts (BOB), which allows them to watch and record TV programmes suggested by their lecturer. Information from the student union and college events is now available when students access the DLE – particularly beneficial for career opportunities, as they are notified when recruiters are to visit.

The college's technical officer, Keith Ball, reports that the upgrade aided learning during the pandemic. Some students were loaned computers and given SIM card hubs for use in rural areas without internet access.



### Imperial College's data moves out of town

Imperial College London, which gained its royal charter in 1907, has its main campus in South Kensington, in Exhibition Road near the Victoria and Albert Museum.

It also has campuses in White City and Sunninghill, Berkshire, and teaching hospital throughout the capital.

There are 19,000-plus students (half postgraduates) and 8,000 staff, half of them academic. Alumni include Sir Alexander Fleming, H.G. Wells, Brian May (Queen guitarist), Peter Higgs (Higgs Boson) and Sir Roger Bannister (runner).

In addition to technology used by teachers and students in their fields of study, the college uses systems such as virtual and blended learning which means it is heavily reliant on technology.

The head of ICT service operations, Paul Jennings, said that when he joined in 2014 the college had underinvested in its data centre.

He said: "Firstly, both of our data centre facilities were situated on the same campus which gave us an obvious single point of failure".

Its data centres had already suffered from power outages, and cooling and UPS failures, and even water damage from building work – causing not only a temporary loss of service but knock-on effects to productivity and research.

Imperial faced a choice: build or buy. They knew that outsourcing to a third colocation party provided the best protection against increasing data centre complexity, cost and risk. And relocating would free expensive space for teaching and learning.

Colocation, Imperial thought, would add resilience, helping to address reliability concerns, increase and improve disaster recovery and support business continuity.

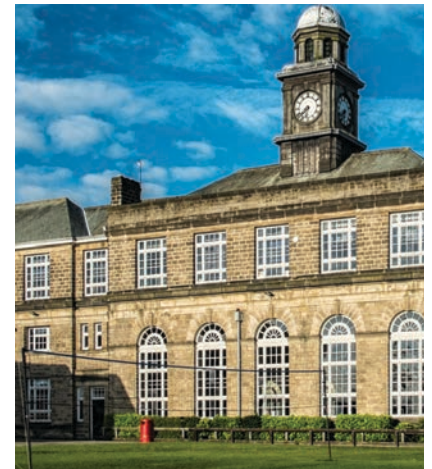
When outsourcing with multiple connectivity options, the potential for carrier failure would be reduced. And in the event of disaster, it would be the providers' job to restore the system.

Imperial contracted Virtus Data Centres and in a three-year programme is moving its data centre to a site in Slough called London4.

The facility is part of a shared research institution framework agreement, brokered through Jisc (formerly the Joint Information Systems Committee) which, says Virtus, ensures value for money.

Jisc is a Bristol-based not-for-profit company set up in 1993 to support technology in education.

London4 has another 23 university and research tenants including The Francis Crick Institute, University College London, University of Bristol and Kings College. And it has a direct connection to Janet (Joint Academic Network).



### Wireless worries calmed with new kit

Harrogate Grammar School has a 1:1 learning scheme which means each of the 2,000 students has an iPad for use both within and outside the classroom.

However, the high-density use of WiFi with its previous networking equipment brought constant helpdesk requests from users frustrated at failing to gain access. Students lost valuable lesson time when it could take them up to 10 minutes to log on.

The Red Kite Learning Trust, which comprises Harrogate Grammar School and 12 other schools, contacted an IT specialist, NetProtocol, which has two facilities in Lancashire: Bury and Morley.

The trust's head of IT, David Burns, said: "Ultimately, we wanted to achieve a wired-like experience in a densely populated wireless environment. That is to say, students and staff needed to be able to access all given resources within 30 seconds of entering a classroom, anywhere on the site and at any time."

NetProtocol's wireless lead, Paul Rylett, said the first task was to model the environment: "How did the iPads operate? What applications were critical? How did they move around the site? And so on. We also performed a detailed survey... a critical part of any successful wireless deployment."

"The building is around 100 years old in places, but modern glass fronted in others – it has every type of wall material you can imagine that will affect the wireless propagation."

"We also faced environmental challenges; the school is surrounded on all sides by a densely populated residential area – as well as the largest radar station in Europe (RAF Menwith Hill) based just along the road."

Other key considerations were how to accommodate the needs of individual year groups as well as those of staff, BYOD, guest on-boarding and internal mobile devices.

NetProtocol first installed the new technology in one school block for testing before rolling it out site-wide. It uses Cloud IQ from Extreme Networks and an access point (Extreme's 305C) was placed in the centre of each classroom to handle 30-plus devices. The power of each was configured to create a coverage cell for the room and to minimise cross channel interference from other rooms.

The trust plans to roll out similar technology at a further three schools in the coming months and to another nine schools within two years.



# Digital disruption and the move towards MVNO services

Kushal Shah, business development director of mobile at BT Wholesale looks at how energy providers can survive and thrive in 2020

In today's society we are more connected than we have ever been. From smart phones to smart cars, and even smart homes, we all rely on constant, pervasive connectivity. Utility companies are beginning to recognise the inherent potential of the home services sector and how it could impact energy consumption patterns with smart metering and IoT at the core.

84% of the UK energy sector market is pursuing or planning to pursue new business opportunities related to increasing the amount of data services they provide – but, why? It all comes down to three main themes that are continuously discussed by executives in the UK energy industry: customer retention, maintaining margin and increasing wallet share. The Ofgem website demonstrates just how competitive the market has become over the past few years. Suppliers are jostling for position and that increasingly means evolving to find an edge to keep up with and incorporate technologies such as IoT.

## Data-driven decisions

The UK energy industry is undergoing major consolidation. Between the period of June 2018 and March 2019, the number of listed suppliers fell by 14%. A turbulent market and more active consumers switching more regularly mean both traditional and challenger energy and utilities companies need a differentiator that not only improves customer stickiness but also brings in new revenue.

Data is the currency of our future and those that collect, analyse and provide valuable, rapid insight from data to the homeowner are set for a good foundation for growth. Indeed, whoever controls the flow of data will be the winners in the battle for the connected home of the future, but the opportunity for utility providers is even bigger than this.

Utility providers not only have the market space to develop smart products (themselves or via partnerships) incentivising energy efficient behaviours, leading to more cost-effective rates and a more attractive proposition for homeowners. They also have the opportunity to leverage all-encompassing telecom providers to become the epicentre of the IoT smart home of the future; selling

energy, broadband, fixed line, mobile and IoT connected devices – all through one easy-to-consume application for consumers. This is where the future is headed, and whichever brand is bold enough to make a play for the smart home could well lock out the competition and reap the rewards.

## The evolution of the MVNO

The evolution of utility providers is closely intertwined with the MVNO model. A Mobile Virtual Network Operator (MVNO) provides a telecommunications service using the physical infrastructure of a Mobile Network Operator (MNO), of which there are four of in the UK. What the market has seen is existing brands with substantial reputation and a drive to capitalise on their customer base providing MVNO-style connectivity services in order to pursue additional revenue streams and increase customer loyalty. Take the supermarkets, for example; many have their own mobile service, which are all operated across MNOs' networks.

This is only going to increase, driven by the rising significance of IoT. New brands are relying on the networks for data-only transmission and it's supporting a growing ecosystem of connected devices, from machines and smart metres, to cars and airplanes.

In regard to utilities, brands that can offer customers more home services are going to slowly start increasing customer wallet share by becoming the provider of the 'smart home'. Utility Warehouse on the EE Network is an example of a company that has successfully been on this journey for while. As such, we will see existing utility providers using their recognition to expand remit to include more traditional mobile connectivity solutions, through acquisitions or partnerships with data-driven brands.

Furthermore, with the likes of Google and Amazon already in our homes through Nest and Alexa, these tech giants are increasingly taking a 'platform approach', similar to supermarkets and their connectivity, to attempt to become a go-to supplier for a multitude of different services.

## IoT in the public sector

As well as the impact IoT will have on the private energy sector, other areas such as councils and housing associations will also benefit from



A Mobile Virtual Network Operator (MVNO) provides a telecommunications service using the physical infrastructure of a Mobile Network Operator (MNO), of which there are four in the UK

better connected solutions; meaning another avenue of opportunity for utility companies with a forward-thinking approach.

While most mass market consumer home IoT products are designed to primarily benefit just the individual household, social housing tech also can offer more civic or aggregated benefits to the landlord or council. For instance, smart devices can enable social landlords to access terabytes of granulated data across potentially thousands of homes to identify physical problems and prioritise interventions.

We're also seeing how IoT can make a difference on our streets. For example, in Bradford and Birmingham, integrated IoT sensors within street furniture are measuring air quality in real-time. Data is then available for analysis by Bradford City Council and a group of researchers and scientists in Birmingham, led by the University of Birmingham. With the air quality monitored, there is now the opportunity to manage it, reduce the sources of pollution and create a healthier city – something that could in turn reduce demands on the NHS and make savings for social services.

Yet, budgets are tight for everyone these days, particularly so in the public sector. There are pressures on local authority bud-

gets while demand for services in social care, housing and community safety are increasing, especially in light of the current pandemic. Therefore, as with the utilities, customers – in this case local councils – ideally want to buy multiple services from one supplier, as it's often cheaper and less hassle. So, as IoT technology becomes more common on our streets, there will be more energy providers looking outdoors and shifting to incorporate MVNO services, such as internet connectivity, offering converged services that will make it more accessible for all councils.

## Connectivity for growth

Ultimately, as energy and utilities companies look to increase customer retention and wallet share, expect to see them diversifying and offering more converged services outside of their traditional remit. With so much competition, the industry is being forced to evolve and incumbents are looking to see how a data-led approach could work for them as they look to fend off growing competition. Those providers who can begin to forge relationships and enter the home through new avenues, will be able to cater for a greater number of customer needs and become the go-to utilities supplier.

## INDUSTRIAL IoT

### Connected Antenna Solutions

Reliable Antenna Solutions for Data Monitoring and Remote Control. 4G LTE & 5G-ready Cellular Solutions as well as Cellular/WiFi/GNSS Multiband Applications. Embedded, Fixed Site and Mobile Antennas.

Contact Us Now  
+44 1543 459555  
enquiries@MobileMarkEurope.co.uk

  
antenna solutions





[www.MobileMark.com](http://www.MobileMark.com)



# Identifying best fit scenarios for alternatives to OEM network maintenance



*Mihaela Dinu, networking and server product manager, EMEA, Curvature*

There is, of course, a direct correlation between asset age and your maintenance options opening up. Generally, this range is three to five years after the end of sale announcement to really start exploring options for significant contract savings. Leading analyst firms say that TPM contracts can offer customers 50% to 70% savings off OEM support net prices.

Regardless of age, there are things to be aware of when contracting out of networking maintenance direct from your manufacturer. Curvature's methodology has been designed to help customers manage the total cost for support and maintenance of its networking assets, while mitigating risk. Our hybrid approach suggests only placing items under Original Equipment Manufacturer (OEM) maintenance that are heavily dependent on subscription services and/or software updates that are only available with an OEM support contract and migrating the remainder of equipment to Curvature's NetSure maintenance program. This method will result in significant cost savings without degradation of support and usually provides a far superior experience. A no-obligation consultation with Curvature will quickly result in a clear definition of which support model matches your organisation's current equipment and technology roadmap. This will be achieved via Curvature's ClearView report.

The first stage in any hardware lifecycle management process is to set the stall with a complete understanding of all components. Our ClearView hardware support assessment service rapidly ascertains at what stage the networking asset sits within its lifecycle noting key milestones. These milestones usually take the form of logging End of Sales dates (EoS) and End of Software Maintenance (EOSW) release dates (this is where no new updates of software will be released and the OEMs only response to a maintenance request for hardware is routed through a Technical Assistance Centre to send a replacement). Manufacturers often add end of support terminology including Last Date of Support (LDOS), End of Support (EoS), End of Service Life (EoSL) – usually after this date, you are on your own.

Alternatively, the Curvature hybrid approach is aimed at examining the customers network and making a maintenance decision based on the type of product, SLA required, and long-term business needs of the customer.

OEMs prefer to have a constant cycle of product releases, coupled with forced maintenance support; issuance of EoL notices; issuance of End of Software Maintenance; issuance of EoS notices, and finally, a forced equipment upgrade. Identifying EOS milestones and EoS support options in advance means a greater freedom of choice. When you have visibility of the approaching milestones and support options, your organisation is in a position to make an educated choice going forward. You will be in a position to understand where it makes sense to pay the premium fees for manufacturer support, and where you have the opportunity to extend the product lifecycles, reduce Opex, and delay/ defer capital expenditure by leveraging third party maintenance.

The ClearView tool uses a clear identification system to highlight the most optimal networking devices in a holistic overview of networking assets, right across the estate. The end analysis provides an unbiased view of risks and recommendations to either stay with manufacturer support or, go ahead and consider an independent support strategy derived from a complete maintenance audit. It is free, conducted

remotely and presented without obligation.

We include information on the individual item's lifecycle status as well as item eligibility notes that speak to why an item is best suited for Curvature (green), optional for Curvature (amber), or recommended for manufacturer support (red). While sometimes it is safe for drivers to proceed on an amber light, sometimes it is unadvisable. The same applies in the Network TPM world. An amber flagged item for Customer A may be an absolute move to TPM; while Customer B would never think of moving the same item to TPM.

The ClearView process starts with an asset inventory list, uploaded by part number or description into Curvature's proximity analysis and database matching portal to deliver a secure support feasibility listing. This list is audited at a line level, checking inventory logs where required for specific items to generate a detailed strategy recommendation for each device. The resultant asset report shows the traffic-light colour coding for networking devices, flagging which should stay under manufacturer support versus which can/should be moved to a more cost-effective, independent support plan, with

any risk levels detailed for consideration.

Then, detailed exploration will determine together how you currently use your equipment and what your future IT strategy looks like. It helps Curvature recommend without bias the right manufacturer-neutral strategy for your IT hardware assets. Lastly, we quantify and identify an immediate reduction in \$\$ OpEx and flag known scenarios or gotchas that we frequently see where the manufacturer may be suggesting premature hardware upgrades. Armed with this level of data and recommendations, you decide the rest.



# Critical Communications Week 2020

## THE NEW VIRTUAL EXPERIENCE

### REGISTER NOW

### 2-6 NOVEMBER 2020

**INTERACTIVE EXHIBITION**

**WORLD-CLASS CONFERENCE**

**ENGAGING ROUNDTABLES**

**& EXCEPTIONAL NETWORKING**

**PRESENTED BY**








[www.criticalcommunicationsweek.com](http://www.criticalcommunicationsweek.com)

 @CritCommsSeries   
  TCCA Critical Communications Series





# Essential UPS elements to understand

Alex Brew, sales director, UK & Ireland, Vertiv

**T**he cost of downtime varies widely by industry: 86% of respondents to a 2019 Statista survey put the cost at \$301,000 per hour or more and more than a third (34%) said downtime cost them \$1m per hour or more.

From that perspective, a relatively modest investment in a UPS is like an insurance policy against far more costly downtime and data loss. There are some questions that also need addressing.

## Determine the size of the load that needs UPS protection, and hence, the capacity of the UPS

Step one is assessing which IT or electronic devices warrant UPS battery backup protection and the power required by each device so that you can calculate the required UPS capacity. The power consumption of IT servers, computers and workstations, and networking equipment are obvious places to start. Still, you might also want to include other devices that are critical to the day-to-

day operation of the business, e.g., point of sale equipment and security systems, among others. Assess what applications each component supports and how the loss of that application will affect your organisation.

For each device to be connected to the UPS, determine the power consumption (watts) of that device. Power consumption can typically be obtained from the equipment nameplate or manufacturer documentation.

The required UPS capacity is the sum of the power consumption of the devices to be connected to the UPS.

## Assess the required UPS runtime for critical devices and applications

Step 2 is to determine the desired UPS runtime for continued operation in case of a power failure. If you have a generator for extended backup power, the required runtime of the UPS may only be a few minutes (~5 minutes) to safely start-up and transition to the generator.

On the other hand, your primary goal may

be to have enough runtime (~5 to 10 minutes) to safely shutdown servers and workstations to avoid any data loss or corruption.

Or, for some applications, such as networks and Internet access (very critical these days), you may want to have one to two hours of runtime to be able to ride through most outages.

Keep in mind that, in general, the more equipment you connect to a single UPS, the shorter its overall runtime will be. An alternative may be to use separate UPS' for certain applications.

## Determine the number of outlets

Add up the number of devices that you need the UPS to support, and make sure the UPS has enough outlets to meet your immediate needs, and also leave some room for growth.

Alternatively, you can use a power distribution unit (PDU) to provide additional outlets, but be careful not to overload the UPS.

Some UPS models also include outlets that only support surge protection. These outlets do not provide battery backup. Make

sure you understand the features of the UPS you are buying and that it has enough battery backup outlets to meet your needs.

## Consider installation requirements

UPSs come in a variety of sizes and form-factors. Tower models are standalone units that sit on the floor, or a desk or shelf, and often backup desktop computers, servers, and routers in an office environment.

Rack-mount UPS models are typically designed to fit in a standard 19-inch IT rack along with other IT equipment. Rack-mount UPSs vary in size, and their height is measured by how many vertical slots it occupies in the rack. Each space is known as a "U" and measures 1.75 inches.

UPSs designed to use lithium-ion batteries tend to be smaller and lighter than similar models that use traditional lead-acid batteries, enabling you to fit more backup power capacity in the same space – or the same capacity in a smaller space.

### PRODUCTS

**I** Replacing an older UPS with **Eaton's** recently introduced new model would give a return on investment in two-three years, says the company. Its three-phase 93PM G2, Eaton's second-generation 93PM model, is modular and scalable: power units in steps of 50 or 60 kVA



can be added without system downtime or affecting the critical load. Features include remote monitoring with cybersecurity protection; HotSync to eliminate the loss of communication between UPSs which causes a UPS to go on by-pass effectively removing the backup system; and pre-designed, pre-tested and pre-installed components, said

to be safer and cheaper than additional external protection. Eaton says 93PM G2 has the lowest TCO in its class: double conversion efficiency of up to 97 per cent lowers operating and cooling costs; its Energy Saver System (ESS) improves efficiency levels to above 99 per cent; and the Variable Module Management System (VMMS) helps to achieve high efficiency even when load levels are low, typical in redundant UPS systems. [eaton.com](http://eaton.com)

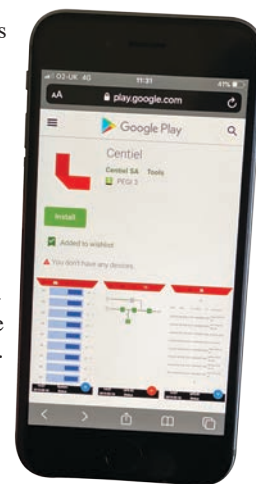
**I** In an upgrade to its Value Pro UPS range, **CyberPower** has given them a new look and added more outlets. It says data line protection with high-speed transmission ensures networking devices are safeguarded while supplying 1Gbps speed to transmit data. And it says its GreenPower technology intelligently reduces power use. It is compatible with PowerPanel management software which provides PC graceful shutdown to prevent unexpected data loss; it supports UPS status monitoring, event logging and power settings to protect connected devices. Other features include auto voltage regulation to combat incoming fluctuations; designed in tower form factor it has a large LCD panel and function buttons, which display power, battery and load status, and allows users to easily configure UPS settings; surge protected outlets; a configurable alarm to alert users of unexpected issues; and generator compatibility

**I** **Synology**, UPS models with an extended power range have been introduced by Schneider Electric. Its Galaxy VS range with internal smart battery modules now extends from 10kW to 100kW. In addition, the company says, it introduces support for internal N+1 module level redundancy, improving system availability by up to 10 times. Schneider says internal battery modules improve availability with added battery flexibility and monitoring, redundant battery strings and self-configuration. This,



it says, means critical loads are always protected with predictable runtimes and battery redundancy. It claims that Galaxy VS with internal batteries is now the highest density UPS in the industry. In ECOconversion mode, it is said to offer 99 per cent energy efficiency saving the price in two-three years (model dependent). Other features include: compact design and full front access; critical components as modules to aid servicing and fault tolerance; ease of management – with global visibility of performance and status – thanks to EcoStruxure IoT software, supported by a 24/7 service bureau. [synology.com](http://synology.com)

**I** **Centiel** UPS models can now, thanks to Bluetooth, download usage information including status, alarm and event logs to smartphones and tablets. It has added Bluetooth capability to its modular UPS model, CumulusPower, and its stand-alone UPS, PremiumTower. Centiel says the app allows technicians to connect to customers' UPSs via Bluetooth, to download historical data. Data is pushed from the UPS to the smart device through an intuitive interface. This information is automatically organised into a file that can be either archived or shared by email. Commands cannot be given to the UPS for safety reasons. The app also works at a module level for CumulusPower. Centiel, base in Switzerland, says the app is ideal for service providers who want to become less dependent on a wi-fi connection for data sharing and to alleviate the need to use PC-based software. It is currently available for Android phones with an update expected over the next few months for iOS users. [centiel.co.uk](http://centiel.co.uk)



to stabilise unstable voltages in case of mains outages. There are 12 models in the range with power capacities of 700VA to 1600VA. [cyberpower-system.co.uk](http://cyberpower-system.co.uk)



**I** Now in more compact housing, Protect C and Protect D UPS models from **AEG** are said to offer a simplified user interface and greater power. Both range from 1,000 to 10,000 VA, with five models for the Protect C tower series and six for the tower or rack-mounted Protect D. AEG says that, with a power factor up to 0.9 for the models up to 3,000 VA and up to 1 for the 6,000 and 10,000 systems, they offer enhanced reliability and more power in a

smaller footprint than the former range. Both series, says the company, operate at high efficiency, up to 95 per cent at typical IT equipment load (50-100 per cent) and 98 per cent in Eco mode for 6000 and 10000 models, for lower energy costs. And both have an S-version, offering a higher capacity charger for longer autonomy times. UPS parameters are shown on a graphic LCD screen and the control panel allows direct configuration. [aeg.co.uk](http://aeg.co.uk)



**I** In a complete revamp of its UPS range, **Piller Power Systems** has introduced the UB-V series. It says that new technology offers up to 98 per cent efficiency, self-monitoring and no maintenance downtime, centred around a new control platform developed over four years. The technology is the fifth generation of Uniblock, which Piller says is the most reliable available. Power ratings for the UB-V are from

1100kVA 1MW to 3600kVA 3.24MW in both battery and kinetic energy storage versions. Piller, based in Germany, says it is a real alternative to increasingly sprawling multiple



static UPSs and improves reliability by a factor of five. Additional reliability is achieved by using fewer components – there are no power capacitors or electric fans. Ride

through for minor outages and voltage fluctuation is provided by electrically coupled dynamic energy storage or by batteries. Standby gen-sets, in case of catastrophic power failure, are remotely located. Piller plans to offer 5MW "single-entity" medium voltage products by 2025 and up to 10MW by the end of the decade in a collaboration with an Italian company. [se.com](http://se.com)





# Please meet...

*Jon Lederman, vice president, artificial intelligence, Rajant*

## What was your big career break?

My big break has been founding and launching two startups, which are SonicCloud and Spinor. Immeasurable lessons come from starting your own company. Being an entrepreneur pays back incalculable dividends in self-actualization, dealing with success and failure, ethics, and working with people. The best you can hope for is to work with great individuals who share your vision and work tirelessly to achieve it for the right reasons.

## Who did you most admire growing up?

Being a musician, I admired John Lennon (and still do) for his brilliance as a songwriter and artist as well as his sense of humor, wordplay - probably above all his honesty and acerbic wit. I also admired visionary entrepreneurs, such as Steve Jobs and Steve Wozniak. Finally, I look up to revolutionary scientists, like Richard Feynman, for his brilliance as a physicist, yet down-to-earth approach and zany sense of humor.

## If you had to work in a different industry, which one would it be?

That's a difficult question. Most likely, I'd have been a physics professor. By nature, I love learning, and the physical world is endlessly fascinating. Much of life can be rather boring and mundane, but science is an endless well of intellectual gems.

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

If you're going to do something, it better be great or don't bother. Those are words I aspire to.

## Which rival do you most admire?

There are many people I admire for an array of reasons. As an entrepreneur, you have to be in it for one reason - to build something great. If you're lucky, you have an opportunity to do something that can make some impact in the world to change things for the better. That's the best you can hope for. The environmental crisis facing this planet is in my opinion at the top of the list as it threatens not only the richness of nature that we often take for granted but our own. Elon Musk is a person who is an entrepreneur for the right reasons, and the beautiful technology his companies are building truly has a chance to enact social and environmental reform.

## What makes you admire people?

I admire qualities in people rather than people themselves. Generally, I admire people who are brilliant and creative and make some positive change in the world through those attributes. Most importantly, I admire people with the courage and perseverance to achieve their goals in the face of adversity. It could be an entrepreneur, scientist, artist, or social engineer or anyone else really.

## What law would you most like to change?

There are lots of laws I would change. The uneasy tension between the democratic ideal and our form of capitalism underlies much of the ills of this country and the world. More concretely, laws protecting animals and the environment should be paramount. Also, the tax system is completely broken. We need more laws guaranteeing the ability of anyone to achieve a higher education regardless of means. That's a win-win for individuals and society as a whole.

## If you could live anywhere in the world, where would it be?

I love swimming and being near the water, so anywhere close to the ocean that is simultaneously close to cultural meccas is ideal. I still love Cambridge, Massachusetts, because it is one of the last bastions of bohemian intellectualism - and the best street music in the world.

## What would you do with £1m?

I'd spend all of it on my startups. Perhaps, I'd set aside some for a '63 ES 335.

## What's been the best technological innovation in your lifetime?

There are so many - and so many that have not lived up to their promise because they've been applied for nefarious purposes. I'd say GPS is one that doesn't get the recognition it deserves. To me, GPS is on par with the printing press for it offered humanity for the first time the ability to navigate anywhere on this planet. In that sense, it led us out of the darkness in the same way the printing press did. Plus, it's the only invention that I'm aware of that

relies on both Einstein's theories of Special and General Relativity as an essential component of its operation.

## What will you do when you retire?

I have no interest in ever retiring. You are lucky if you love what you do. For me, that means solving interesting and hard problems in creative ways. I'll always be doing that, so retirement is not an option. So, for me, conventional notions of retirement would be anathematic. Plus, golf just doesn't do it for me.

**W:** [www.ramanpower.com](http://www.ramanpower.com)  
**T:** +44 (0) 203 950 8988  
**E:** [info@ramanpower.com](mailto:info@ramanpower.com)

**VERTIV**  
PLATINUM PARTNER

## HOW CRITICAL IS YOUR POWER?

**Don't Wait to Back Up Your Power**

**Vertiv™ Liebert® GXT5 750VA - 20kVA UPS**

- Unity Power Factor – PF = 1.0 provides more active power
- High Efficiency – Up to 95% with lower heat dissipation
- Full protection – Protection from outages, sags, surges, spikes, etc
- TCO – Longer life time and run time of the batteries
- Remote Connectivity – Monitor via the network

UPS Model	Size	Rating	kVA	Outlets	Price
GXT5-750IRT2UXLE	2U	1-Ph	750VA	(8) C13	£ 434.00
GXT5-1000IRT2UXLE	2U	1-Ph	1kVA	(8) C13	£ 524.00
GXT5-1500IRT2UXLE	2U	1-Ph	1.5kVA	(8) C13	£ 694.00
GXT5-2000IRT2UXLE	2U	1-Ph	2kVA	(8) C13	£ 928.00
GXT5-3000IRT2UXLE	2U	1-Ph	3kVA	(8) C13 & (1) C19	£ 1,237.00
GXT5-5000IRT5UXLE	5U	1-Ph	5kVA	(6) C13 & (2) C19	£ 1,868.00
GXT5-6000IRT5UXLE	5U	1-Ph	6kVA	(6) C13 & (2) C19	£ 2,180.00
GXT5-8000IRT5UXLE	5U	1-Ph	8kVA	(4) C13 & (4) C19	£ 2,827.00
GXT5-10KIRT5UXLE	5U	1-Ph	10kVA	(4) C13 & (4) C19	£ 3,409.00
GXT5-16KIRT9UXLE	9U	1-Ph	16kVA	Hardwired	£ 5,083.00
GXT5-20KIRT9UXLE	9U	1-Ph	20kVA	Hardwired	£ 6,224.00

**UPS Accessories**

Accessories	Description	Price
RDU101	Network card	£ 184.00
RMKIT18-32	Rack mounting slide kit	£ 62.00
SN-T	Temperature sensor	£ 58.00
SN-TH	Temperature / Humidity sensor	£ 88.00
GXT5-EB36VRT2UE	External battery cabinet for 750VA - 1kVA	£ 432.00
GXT5-EB48VRT2UE	External battery cabinet for 1.5kVA - 2kVA	£ 501.00
GXT5-EB72VRT2UE	External battery cabinet for 3kVA	£ 584.00
GXT5-EB192VRT3U	External battery cabinet for 5kVA - 10kVA	£ 860.00
GXT5-EB384VRT6U	External battery cabinet for 16kVA - 20kVA	£ 1929.00

**Discover Universal Connectivity**

**Vertiv™ Geist® PDU**

- Combination Outlets – C13 & C19 in one providing total flexibility
- Locking Outlets – Secures power cord to avoid accidental downtime
- Colour Coded Outlets – Easily identify load per circuit breaker
- Upgradable & Hot-Swappable – Interchangeable monitoring device
- Remote Connectivity – Monitor via the network

PDU Model	Type	Rating	Feature	Outlets	Price
VP8853	Input Monitored	1-ph 32A	Standard	(36) C13 & (6) C19	£ 417.00
VP8858	Input Monitored	1-ph 16A	Standard	(18) C13 & (2) C19	£ 363.00
VP8886	Input Monitored	3-ph 32A	Standard	(30) C13 & (12) C19	£ 925.00
VP8881	Input Monitored	3-ph 16A	Standard	(36) C13 & (6) C19	£ 544.00
VP8953	Outlet Switched	1-ph 32A	Standard	(20) C13 & (4) C19	£ 756.00
VP8959EU3	Outlet Switched	1-ph 16A	Standard	(21) C13 & (3) C19	£ 686.00
VP43903	Input Monitored	1-ph 32A	Combi Outlets	(36) C13 & C19	£ 428.00
GI30150	Input Monitored	1-ph 16A	Combi Outlets	(36) C13 & C19	£ 408.00
GI30146	Input Monitored	3-ph 32A	Combi Outlets	(36) C13 & C19	£ 830.00
GI30149	Input Monitored	3-ph 16A	Combi Outlets	(36) C13 & C19	£ 578.00

**PDU Accessories**

Accessories	Description	Price
GTHD	Temperature, Humidity, Dewpoint sensor	£ 73.00

## NEED OUT-OF-BAND ACCESS?

### Minimise Downtime & Remediate Troublesome IT Devices Remotely

**Vertiv™ Avocent® ACS Serial Console Server**

Serial Console Model	Description	Price
ACS8008DAC	8 Port Serial Console Server w/ dual AC PSU	£ 1597.00
ACS8016DAC	16 Port Serial Console Server w/ dual AC PSU	£ 1905.00
ACS8032MDAC	32 Port Serial Console Server w/ dual AC PSU	£ 2335.00
ACS8048DAC	48 Port Serial Console Server w/ dual AC PSU	£ 3102.00

**ACS Adapters**

Adapters	Description	Price
ADB0036	RJ45 Female to 9 Pin Female Serial Adapter	£ 7.50
ADB0039	RJ45 Female to RJ45 Male Serial Adapter	£ 7.50

**Vertiv™ Avocent® MPU KVM over IP Switch**

KVM over IP Model	Description	Price
MPU108EDAC	1 User, 8 Port KVM over IP switch w/ dual AC PSU	£ 1321.00
MPU2016DAC	2 User, 16 Port KVM over IP switch w/ dual AC PSU	£ 2889.00
MPU2032DAC	2 User, 32 Port KVM over IP switch w/ dual AC PSU	£ 3257.00
MPU4032DAC	4 User, 32 Port KVM over IP switch w/ dual AC PSU	£ 4362.00
MPU8032DAC	8 User, 32 Port KVM over IP switch w/ dual AC PSU	£ 5407.00

**KVM over IP Cables**

Cables	Description	Price
MPUIQ-VMCHS	Server Interface Module for VGA & USB	£ 92.00

**Contact Raman Power Technologies Today To Discuss Your Project & IT Requirements**

**W:** [www.ramanpower.com](http://www.ramanpower.com) **T:** +44 (0) 203 950 8988 **E:** [info@ramanpower.com](mailto:info@ramanpower.com)

Please note that all prices shown exclude VAT at 20% and may change without notice. Our standard terms and conditions apply.



★ Free UPS Health Check

★ Reliable

★ Free Power Audit

★ Installation & Maintenance

**APC**

From  
**£2024**  
ex. VAT



**APC Smart-UPS SRT 1.5kVA  
Online 230V with Network Card  
(UPS) (3U) (Lithium-Ion) -  
SRTL1500RMXLI-NC**

Reduce your carbon footprint with an  
energy efficient and long lasting UPS.  
Able to support a couple of servers.

**2-3 users**

**0800 978 8988**  
Free 24x7 Support

**APC**

From  
**£6031**  
ex. VAT



**APC Galaxy VS 10kVA Double  
Conversion 400V (UPS) -  
GVSUPS10KB2HS**

Ideal for server rooms and heavy  
machinery with a small footprint. A  
quality backup power solution.

**10 users**

**0800 978 8988**  
Free 24x7 Support

**APC**

Call for  
price



**APC Galaxy VS 50kVA Double  
Conversion 400V (UPS) -  
GVSUPS50KB4HS**

This UPS is a great choice to backup  
a whole office or multiple heavy  
machinery or a small data centre.

**50 users**

**0800 978 8988**  
Free 24x7 Support

**riello ups**

From  
**£69**  
ex. VAT



**Riello iDialog 800VA Offline 230V  
(UPS) - IDG 800**

Built for the home office with proven  
reliability. Perfect for people working  
at home or self-employed.

**1-2 users**

**0800 978 8988**  
Free 24x7 Support

**riello ups**

From  
**£420**  
ex. VAT



**Riello Sentinel Pro 2.2kVA Online  
230V (UPS) - SEP 2200**

Ideal UPS for networking and backing  
up multiple computers off one UPS  
device. It is popular among offices.

**2-3 users**

**0800 978 8988**  
Free 24x7 Support

**riello ups**

From  
**£2064**  
ex. VAT



**Riello Sentinel Dual 8kVA Online  
(UPS) - SDU 8000 TM**

This is one of our higher range UPS that  
is used for server rooms of larger offices  
and can back up multiple servers.

**10 users**

**0800 978 8988**  
Free 24x7 Support

For more information or stock availability, contact us on:

[criticalpowersupplies.co.uk](http://criticalpowersupplies.co.uk)

**0800 978 8988**

[sales@criticalpowersupplies.co.uk](mailto:sales@criticalpowersupplies.co.uk)