www.networkingplus.co.uk

MARCH 2019

networking

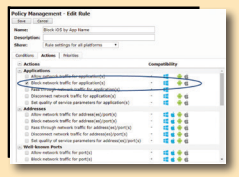
FIXED & WIRELESS NETWORKS FOR ENTERPRISE USERS

Phishing hooks UK firms
Research shows companies still being compromised
News, p2

Kitting out the countryside
RNAA promoting agriculture and more
Real World Networks, p8

Net health benefits
How HSCN can enable cost-saving digital transformation
Feature, pp11-13

See it all from the centre
Network monitoring plus expert advice
Off-the-shelf, p14



DDoS cyber attacks could cost UK economy £1bn every year - report

Distributed denial-of-service (DDoS) cyber attacks are having a bigger impact on UK businesses than ever before and could cost the UK economy more than £1 billion every year, according to a new study.

The 14th annual *Worldwide Infrastructure Security Report* (WISR), published by US-headquartered security and assurance solutions specialist Netscout, revealed that in 2018, 91 per cent of the UK businesses surveyed said they had experienced a DDoS attack, which infects a network and blocks users from accessing it for often long periods of time. The report said each attack lasted around 67 minutes in duration, with every successful one costing businesses north of £140,000 - an average cost of £2,140 per minute.

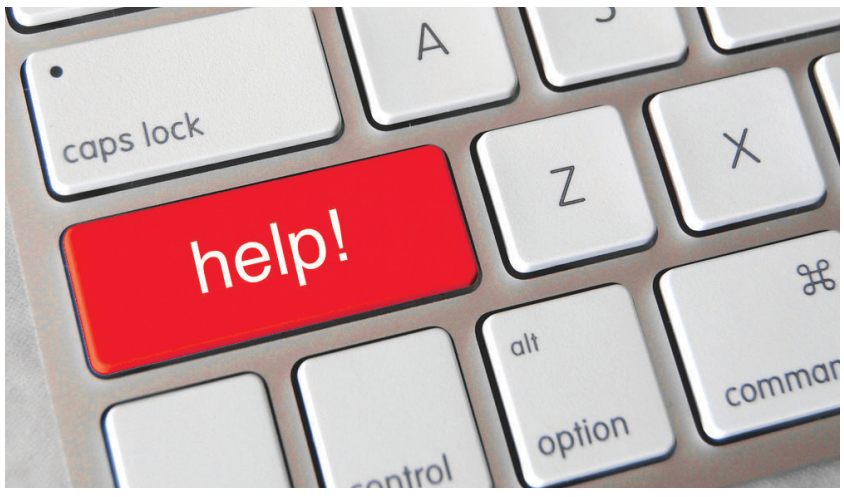
The report also said there had been a threefold year-on-year increase in the number of DDoS attacks against SaaS services, which rose from 13 per cent to 41 per cent. Attacks against third-party data centres and cloud services were up by 23 per cent.

Almost half the companies that took part in the survey said they experienced an outage of 30 minutes or more, while nine per cent were impacted for more than four hours – half the normal working day.

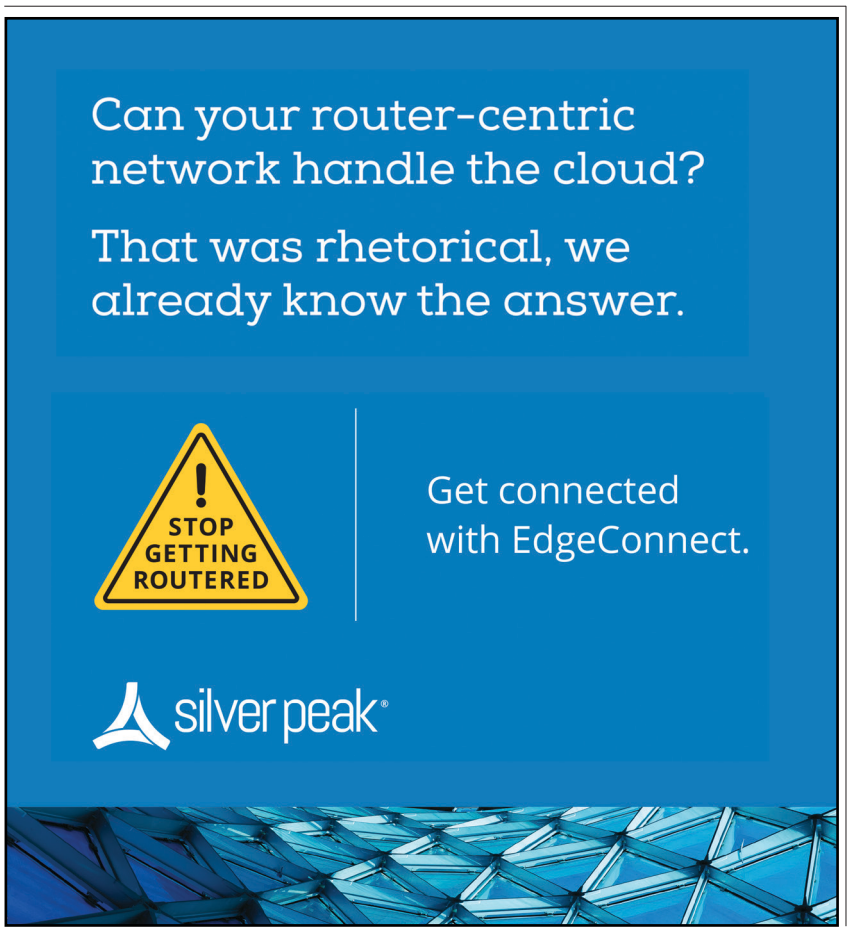
Furthermore, around 86 per cent of major UK enterprises said they were attacked at least once in 2018. The figures equate to costs of roughly £900m for large UK companies – the 8,000 with more than 250 employees - but the report said that many small and medium sized businesses are now also affected by cyber attacks, meaning that the total cost may now exceed £1 billion with no sign of that figure coming down.

The report also found that while network outages are the most obvious problem, the downtime that followed, as the result of these attacks, caused the affected businesses an array of problems.

continued on page 2



Almost half the companies surveyed said they had experienced an outage of 30 minutes or more



Telent's new solution to save police millions each year

Technology and network services giant Telent has launched a new digital evidence management product designed to save police services millions of pounds a year.

It provides 100 per cent UK sovereignty of the storage of digital evidence with all data encrypted - all held securely on Telent's public services network (PSN) accredited and UK-based cloud platform.

The Warwick-based firm developed the product with specialist policing software application provider, Innaxys.

Telent said the product will "significantly reduce" the time officers spend physically collecting CCTV images and will enable faster analysis and processing of evidence, when it comes to digital evidence such as CCTV footage, photos and videos recorded by the public, as well as body camera and dashcam clips.

Furthermore, police services will also be able to securely share evidence with the criminal justice system to ensure evidence cannot be misplaced, lost or damaged, reducing court case adjournments and delays.

Barry Zielinski, general manager for public safety and defence at Telent, said the solution was developed in consultation with UK police forces specifically to address the challenges faced by officers collecting data in the modern policing age, where there has been a huge increase in public and business CCTV use.

"This is combined with a proliferation of smartphones, dash cams, social media and body worn cameras, creating both opportunities and challenges for policing," Zielinski said. "This solution helps officers efficiently collect, manage, store and share these new digital evidence sources. "It will save officer time collecting images, reduce court case adjournments and ensure the security of digital evidence by eliminating the risk of it being destroyed, tampered with, lost or even left in public places."

Telent's list of high-profile clients includes Airbus, BT and Stagecoach. ■

Cyber attacks could cost £1bn

Continued from page 1

Revenue loss was reported by over a third of respondents (36.2 per cent), alongside other factors such as increased operational expenses (38.6 per cent), reputational impact (36.2 per cent), higher insurance premiums (31.9 per cent) and loss of customers (30.7 per cent), highlighting the longer-term damage successful attacks can bring.

Netscout chief technology officer Darren Anstee said large-scale attacks are getting cheaper to carry out, but the consequences are getting more expensive for enterprises.

"The tools to initiate DDoS attacks are cheap, freely available and easily deployed - as a result, there are over 10,000 DDoS attacks every day around the world," said Anstee "The size and complexity of attacks continue to grow and businesses must make sure their key resources are adequately protected, including in the cloud, SaaS etc. If something is important to you, it's important to hackers."

Anstee added that a cyber security skills shortage at many UK businesses did not help matters, with a number of firms having to outsource more of their security management to third-party vendors to tackle the problem.

Jonathan Anthony, investor and founder, at security vendor reactions.ai agreed and said: "In fighting DDOS, the battle is between false positives, unmatched software and hours in the day." ■

Scottish charity in IoT and tech drive

A business-backed fund to find the next generation of technology and digital experts in Scotland has been doubled from £50,000 to £100,000.

Digital Xtra Fund is a Scottish charity which supports IT initiatives that encourage young Scots to consider careers in digital technologies and close the digital skills gap.

This year's funds will support 22 computing projects across the country, ranging from IoT to app development.

The fund has distributed £550,000 in support of 55 initiatives, engaging more than 20,000 young people across the country.

Funding and support have been provided by industry partners such as Edinburgh-founded travel tech firm Skyscanner, bank JP Morgan, and the Micro:bit Educational Foundation.

Kraig Brown, partnerships and development manager for Digital Xtra Fund and Kate Forbes, minister for public finance and digital economy, with pupils from Anderston Primary School in Glasgow

"Digital skills are becoming increasingly essential for most careers, regardless of industry, so it is vital that we equip as many children as possible with these skills from a young age," said Kraig Brown, partnerships and development manager for the Digital Xtra Fund. "Our mission is to help young people in Scotland acquire vital digital skills through exciting and engaging digital skills initiatives they can get involved in. We are there to help hard-pushed educators who may not have the time or resources to teach these important skills. The demand for people with digital skills will be insatiable in Scotland in the future so we need to create a pipeline of young people with the necessary digital skills now, so that we can thrive as a digital nation." ■

Phishing hooks nearly half of British businesses

Almost half of UK businesses (45 per cent) have been compromised by phishing attacks in the last two years, according to research from Sophos.

The company surveyed 906 IT directors in western Europe and revealed that larger businesses were more likely to be compromised by phishing attacks, even though they were more likely to conduct phishing and cyber threat awareness training.

The UK fell victim to phishing at a similar rate to those in France (49 per cent) and the Netherlands (44 per cent), with just 25 per cent of Irish respondents saying they had fallen victim to phishing in the last two years.

The research further revealed that 54 per cent of UK organisations had identified instances of employees replying to unsolicited emails or clicking on the links contained within them.

"Phishing affects everyone and is one of the most common routes of entry for cyber criminals," said Adam Bradley, UK managing director, Sophos. "As organisations grow, their risk of becoming a victim also increases as they become more lucrative targets and provide hackers with more potential points of failure. Given the frequency of these attacks, organisations that don't have basic infrastructure in place to spot people engaging with potentially harmful emails and whether their systems are compromised are likely to encounter some really significant problems."

Bradley said enterprises should block malicious links, attachments and imposters before they reach end users' inboxes, "and use the latest cybersecurity tools to stop ransomware and other advanced threats from running on devices even if a user clicks a malicious link or opens an infected attachment". ■

Research further revealed that 54 per cent of UK firms identified instances of employees replying to unsolicited emails or clicking on the links contained within them

Topolytics analysing UK waste

Scottish data and analytics firm Topolytics has partnered with the Ordnance Survey to monitor and track all of the UK's waste.

The former was selected by the Department for Environment and Rural Affairs (DEFRA) to design a "smart" system to capture the more than 20 million movements of waste from their sources through to final processing or disposal.

Topolytics has started designing the system on its WasteMap analytics platform that makes waste management more cost and resource efficient. It takes and processes data from many different sources and applies data science, mapping and geographic analytics to identify and qualify the sources, types and movements of different materials – making the waste system visible and verifiable.

The system will track all slow-moving and hazardous waste from homes, local authorities, businesses and the construction sector.

"We are excited to be partnering with the Ordnance Survey on delivering a powerful and practical solution for the UK's environmental regulators and waste managers," said Topolytics chief executive officer, Michael Groves. "Our combination of waste industry experience, software development, data science and geospatial analytics is a powerful mix." ■

EDITORIAL:
Editor: Robert Shepherd
roberts@kadiumpublishing.com
Designer: Sean McNamara
seanm@kadiumpublishing.com
Contributors: James Hayes, Gerry Moynihan

ADVERTISING & PRODUCTION:
Sales executive: Andy London
andrewl@kadiumpublishing.com
Production: Suzanne Thomas
suzannet@kadiumpublishing.com

Publishing director: Kathy Moynihan
kathym@kadiumpublishing.com

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

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

Printed in England by The Magazine Printing Company
© 2019. All rights reserved·

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

KADIUM

THE WORLD ACCODRING TO...

Thorsten Kurpjuhn, European security market development manager, Zyxel

AI is the future of network protection

The reliance on IT systems from hotels, schools and businesses across the UK in general has grown immeasurably. Nearly every member of staff now needs a PC and laptop to carry out their day-to-day tasks. Guests, pupils and suppliers all need to connect their myriad devices to access networks. In a world where technology underpins everything we do, there is a continual need to spin multiple plates to ensure operational efficiency across the network.

The overwhelming amount of data present on a network and the growing number of connected mobile devices, as well as and the ever-increasing risk of cyberthreats, means that the role of network managers in the UK is now a very different beast than before.

The biggest challenge for UK network administrators is now dealing with the sheer volume of cyberthreats. High profile global incidents – including the WannaCry epidemic in May 2017 – demonstrate the lasting impact that cyberthreats can have. Since then there has been a 46 per cent increase in new variants of ransomware, making it increasingly difficult for those in charge to protect their networks.

Also, cryptocurrencies have seen cybercriminals adopt more sophisticated tactics to attack UK businesses. In 2018, the Cyber Threat Alliance reported a 459 per cent increase in the rate of illegal crypto-jacking, suggesting that businesses are yet to implement effective measures to combat the threat.

In the midst of these pressures, how can UK businesses combat everything that is thrown at them? Enter artificial intelligence (AI).

AI might sound like a futuristic concept, but its application within network security management is vital. The application of AI within a network firewall adds a valuable layer of self-learning to the monitoring and management process. Effectively, it provides a dedicated pair of eyes and ears across the network. A firewall bolstered with a layer of AI can recognise a threat in real-time, quarantine and analyse it, helping the system to effectively respond and defend against future attacks.

The demands on the network are constantly changing, so it makes sense for its management to also evolve and scale. Doing so ensures that networks operate at optimum efficiency. Also, the network administrator can stay one step ahead and focus on maintaining operational excellence, rather than spending time repairing damage caused by malware attacks.

Far from dismissing AI, embracing the benefits of machine learning for network management is the next natural step for small UK businesses. Simply trusting your firewall will only get you so far.

CyrusOne goes 100 per cent green

CyrusOne has announced that its London I and London II data centres are now running on a 100 per cent renewable energy tariff.

Comprising a combined 23MW of IT power, the London I data centre in Slough and London II facility in Prologis Park, Stockley, are now served by Hudson Energy, an independent provider of electricity and gas to businesses across the UK.

CyrusOne said the move will transfer energy annual usage equivalent to 52,000 households to zero-emissions sources.

Data centres have often been criticised for damaging the environment due to the speed at which they consume vast amounts of power and this move has seen CyrusOne buck the trend.

Both London I (above) and London II data centres are now served by Hudson Energy, an independent provider of electricity and gas

"As large energy users in the UK, the data centre industry is in a strong position to effect change in terms of how green energy is priced and made available," said Tesh Durvasula, president – Europe, CyrusOne. "Traditionally, green energy tariffs have been priced at a premium, but as more users demand their energy from renewable sources, the rates we can negotiate are decreasing rapidly.

Durvasula added that the company would continue to explore ways in which to "maximise the efficiency and resource usage in our data centres so that we can pass those benefits along to our customers".

Water conservation has been a significant factor in how CyrusOne designs and builds new data centres, the company said. ■

Network efficiency a top priority for UK businesses

A survey of UK business found that network efficiency is top priority for optimising data centre performance. The report, conducted by Futuriom, spanning medium to large enterprises across the UK, revealed high interest in software-defined virtualisation and network optimisation strategies. It found that processor offload and SmartNICs are now the favoured solution for improving data centre performance – while deploying more servers is least favoured. Above all it concluded that the network, a key engine of performance to the cloud, needs specific adaptations to keep up with data centres that have ambitions to be cloud-scale. Other findings include: the recognition that network optimisation technologies are a key way to improve data centre performance. Companies in China and the USA also took part in the survey. ■

CFS to deliver services to Europe

Critical Facilities Solutions (CFS) US, the data centre cleaning and infrastructure services provider across the Atlantic, has formed a UK branch to deliver services in Europe, the Middle East and Africa (EMEA). CFS UK will be headed up by operations director Gary Hall and Mike Meyer, managing director, CFS UK. The duo has combined sector experience of almost 45 years, having been senior members of 8 Solutions where they delivered data centre cleaning and services. Hall also serves as chairperson for the UK's Data Centre Alliance's anti-contamination committee. ■

Global Switch chooses banks for IPO

Data centre operator Global Switch has selected CLSA, Goldman Sachs and JPMorgan as sponsors for its Hong Kong initial public offering (IPO) of up to $1 billion. Founded in 1998 and owned by Britain's billionaire Reuben brothers, Global Switch operates 11 data centres spanning Europe and Asia. The company said in January it had "resolved to commence preparations for a public listing on a leading international stock exchange in 2019, subject to market conditions". The IPO was first suggested in July 2018, when a consortium made up of six Asian investors acquired a 24.99 per cent stake in Global Switch for £2.1 billion. ■

BT deploys LoRaWAN and IoT for new project

BT has joined forced with Northumbrian Water to deliver a smart water project and improve its network performance in north-east England.

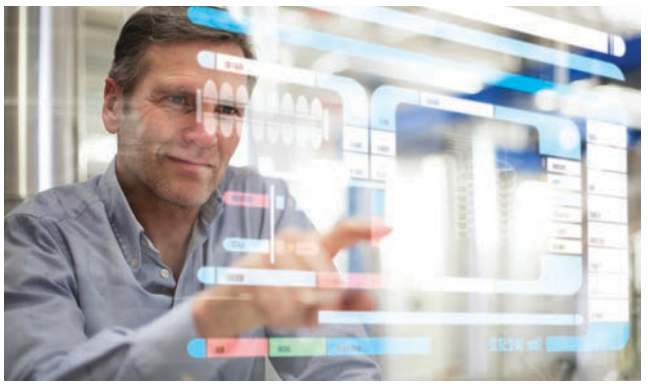
This scheme will see around 150 sensors deployed in pipes in the water network across the Sunderland area for six months, as part of a 12-month pilot study.

Smart sensors will capture and process data on a range of factors, such as how the network is functioning, while providing real-time operational insights into water flow, pressure and quality.

Northumbrian Water will be able to use the technology for the benefit of its customers and the environment, identifying issues such as burst pipes or leaks more quickly and easily than before.

The company will also have a better understanding about how the network can impact on water quality changes and allow it to manage this proactively.

"BT will be connecting around 150 sensors from across Northumbrian Water's water network to its LoRaWAN network, providing Northumbrian Water with deeper insights into aspects such as water quality and pressure," said Andy Bridden, client delivery director for IoT, BT. "The operational insights that the data will provide will allow Northumbrian Water's engineers to better understand how the water network is performing, so the engineers can be deployed across the network more effectively and efficiently." ■



Northumbrian Water will be able to use the technology for the benefit of its customers and the environment, identifying issues such as burst pipes or leaks more quickly and easily than before

NAO criticises government failings over cyber-attacks strategy

The National Audit Office (NAO) has criticised the government over "failings" in the way it is planning to protect the UK's critical infrastructure from cyber-attacks.

According to a report by the public spending watchdog, the Cabinet Office made errors when it established the National Cyber Security Programme (NCSP) in the autumn of 2016 and has claimed the government now does not know whether it will be able to meet the programme's goals, or adequately protect UK citizens, businesses and infrastructure from cyber-attacks post 2021.

Although the NAO noted some successes, including the establishment of the National Cyber Security Centre (NCSC) in 2017, it said it remained unclear whether the programme, which was designed to establish a "focal point" for cyber security activity across government, would achieve any of its wider strategic outcomes by 2021.

This was due, in part, to difficultly in dealing with the evolving and complex cyber security landscape, and also because the Cabinet Office had not properly assessed whether the £1.3bn of funding ringfenced for the NCSC – out of the £1.9bn total for the strategy –was enough.

Amyas Morse, the head of the NAO, said that the government had "demonstrated its commitment to improving cyber-security", but that there is uncertainty about how it will fund these activities after 2021.

"Government needs to learn from its mistakes and experiences in order to meet this growing threat," Morse said. ■

Administrators 'unprepared' for domain migration

Only 28 per cent of gov.uk domains have enabled email authentication protocol DMARC (Domain-based Message Authentication, Reporting and Conformance), in line with UK Government Digital Service (GDS) advice ahead of the retirement of the Government Secure Intranet (GSI) platform.

Security vendor Egress revealed a lack of preparation from several government email administrators in preparation for the domain migration, which left domain users open to phishing attacks and has forced departments to migrate to the public cloud.

The findings also contrast with central government departments, where the majority have implemented DMARC according to the National Cyber Security Centre (NCSC).

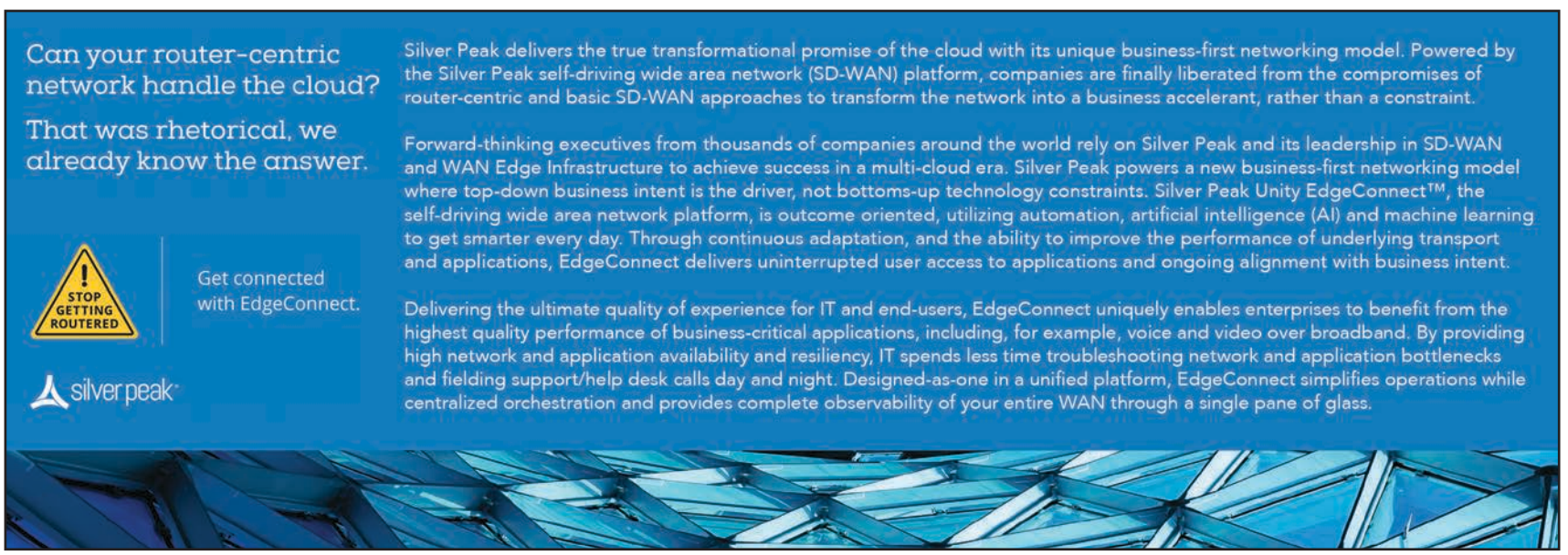
DMARC is an important part of the NCSC's active cyber defence initiative, which was set up to shield the UK from attacks. It provides an email validation system designed to detect and block email spoofing, which ensures that people can decide if a message has emanated from a legitimate sender or source. Fake emails claiming to be from the government, including non-ministerial departments like HMRC, have become a major problem in the fight against cyber-crime. However, the DMARC protocol can help deal with these emails if it is adopted.

In addition, of the 28 per cent that had enabled DMARC at the time of the study, over half (53 per cent) set a policy to "do nothing" — which could effectively clear the way for business email compromise attacks and allow email buffering, while spam and phishing messages would populate recipient inboxes.

Egress said that would mean that a mere 14 per cent of government domains use DMARC effectively to stop phishing attacks.

"It's quite startling to see that so many public sector organisations have not yet enabled DMARC effectively and therefore cannot provide full assurance over their email network's ability to withstand phishing attacks," said Egress chief technology officer Neil Larkins. "With only one month left before the GSI framework is retired, it's critical that organisations heed the advice laid out by GDS."

Egress said it analysed more than 2,000 email domains. ■



microlease
Now part of the Electro Rent Corporation

VIAVI
(FORMERLY JDSU)

Simplifying your transition from 1G, 10G & 100G

Are you ready for 100G?
Viavi's industry leading network test solutions make it easy to move to 1G, 10G and all the way to 100G

With network operators supporting ever growing demand by upgrading their core networks to 1G, 10G and 100G, you need to stay ahead of the game. Viavi network testers are the industry leading handheld solution you can rely on to test throughout the service life cycle, including fiber characterization, service activation, troubleshooting, and maintenance.

Available from 1G to 100G with the same, familiar, user-friendly interface, Viavi testers make the transition to 1G, 10G or 100G easy. With options to buy, rent or lease, Microlease has the smart solutions to help you futureproof your test inventory with Viavi's industry leading technology. And with 10% off new products*, there's no time like the present to update your kit.

Call us now and receive a **10% discount on new Viavi 1G, 10G or 100G test equipment.*** Please quote code **NWP10**

020 84 200 200
info@microlease.com

microlease.com

Rent | Buy New | Buy Used | Financial Solutions | Asset Optimisation

*Offer available for the purchase of new, or rental of selected Viavi equipment for 1G to 10G to 100G testing. Offer applicable from 1st April to 30th June 2019. Quote code NWP10 when enquiring. Microlease reserves the right to withdraw the offer at any time. Full terms available on request.

UKCloud receives cash boost for multi-cloud platform expansion

UKCloud has received a £25m cash boost from Cisco Systems-backed Digital Alpha Advisors to support the expansion of teams and technologies behind the multi-cloud platform.

The public sector IT specialist's technology was created to provide a secure, scalable and cost-effective cloud platform to drive and aid the digital transformation of public services nationwide.

It is also a strategic move for Cisco in the UK, as it will have a new route to market with UKCloud through joint sales and marketing activities.

Simon Hansford, chief executive UKCloud, said the investment from Digital Alpha "demonstrates" its confidence in the former's differentiated business model and gives it potential to scale, accelerate growth in the UK public sector saving taxpayer money, and drive "better insights" for decades to come.

"Importantly, our alignment with Cisco is a force multiplier, enabling our product development and helping us further differentiate from our competitors, enabling us to accelerate our investment in sales, marketing, customer experience and new markets," he added.

Digital minister Margot James said: "We are committed to making the UK the best place to start and grow a digital business and I'm delighted to see UKCloud attracting funding from international investors to scale up their operations. This is another vote of confidence in our talented sector and will help us maintain our reputation as the leading destination in Europe for inward investment." ■

baramundi

One Management Software For All End Devices

IT development is soaring at an ever-growing pace. As the performance and variety of devices increases, so do the administrative requirements.

Our white paper shows you how to automate routine task:

- Distribute operating systems and applications
- Detect vulnerabilities and automating updates
- Inventory hardware and software
- Manage mobile devices

How to automate routine tasks with baramundi

Download free white paper
www.baramundi.de/auto-network

Slow uptake on cloud by UK police forces

Police forces across the UK have been urged to adopt cloud computing, in a freedom of information (FOI) report.

The survey, carried out by US-based cloud software multinational Citrix, found that migrating to the cloud could help free up valuable resources for the most underfunded and overstretched forces in the country.

It approached 43 forces – and of the 24 that responded, 75 per cent said they still access and manage their data and applications on-premise.

In total, 71 per cent of forces currently store less than a quarter of their data and applications in a cloud environment, while an additional 13 per cent said that none of their data and applications are stored "in the cloud".

The findings jar with the "cloud first" policy introduced by the government back in 2013, which recommended all public sector organisations should consider the cloud above all other solutions when procuring new or existing services.

However, there were some positives to be taken from the data. The report found that 88 per cent of forces said they were considering investing in cloud infrastructure and technologies such as software, platform or infrastructure as a service (SaaS, PaaS or IaaS) within the next 12 months.

Furthermore, over two thirds (67 per cent) said they planned to outsource or downsize their physical IT infrastructure in favour of a cloud model within the next twelve months, with 25 per cent already having done so. ■

DfT starts Google Cloud migration

The Department for Transport (DfT) has shifted its first in-house application to the Google Cloud Platform, which is the start of a much broader migration process.

It has moved its version of the LENNON application (Latest Earnings Networked Nationally Overnight) to the platform as a first step in a six-month transformation process. LENNON is used by the railway industry.

The plan was outlined in a blogpost by Luke Radford, head of CIO Advisory at the DfT. Radford said that it followed a discovery exercise with Google and was part of a move to close the department's data centres.

Digital staff has been working with the DfT's rail technical and data management team, Google and its partner Cloud Technology Solutions on migrating the LENNON system.

While the project is still in progress, processing speeds have been dramatically reduced with the time taken to execute a query cut from hours to less than 20 seconds. It is also making it possible to run multiple queries simultaneously.

Radford said the cloud version should free up a lot of time, improve security and provide for frictionless back-ups and maintenance.

"For DfT's Digital Service, this project has demonstrated some huge benefits of using Google Cloud Platform," Radford said. "I hope and expect that this experience will enable us to further improve our efficiency through the transformation of similar applications." ■

THE IoT CONNECTION News, opinion & developments from the world of the Internet of Things.

UK cities start pilot project

UK cities Manchester and Edinburgh have begun to take part in smart city pilot projects with other cities on the continent, under the Europe-wide Synchronicity programme.

Manchester City Council is working on three projects aimed at channelling IoT technology. They include the Lighthouse Cities project, in which the city will aim to improve energy efficiency on its university and civic estates.

The project is part of a broader one on energy, mobility and ICT in which it is working with Eindhoven in the Netherlands and Stavanger in Norway. Manchester is also working with Eindhoven and Porto in Portugal on the SmartImpact project focused on governance, organisational and financing issues in the adoption of smart city solutions. Each city is developing an integrated action plan as guidance for future efforts.

These are underlined by the CityVerve project, for which the English city has provided an IoT demonstrator area since 2016.

City of Edinburgh Council is working with Bilbao in Spain to measure and reduce noise pollution.

The Scottish city is using IoT technology and linking the outputs to data from other sources through the USMART data integration and insights platform.

People more important than IoT

People, not technology or IoT, must be at the core of smart city planning and transport networks or the UK risks creating divided and socially exclusive communities nationwide, a new report has warned.

Rethinking Smart Futures by PwC and London Transport Museum, in collaboration with international law firm Gowling WLG and the global transport and security company Thales, has outlined a new vision for smart cities that are socially inclusive and focused on people, enabled by transport and powered by IoT, technology and data.

The report identified the challenges to achieving this vision and called for central and local government, the public sector and private industries to join forces to take forward key recommendations.

Gowling WLG Partner and head of rail, Giles Clifford, said the advancement of technology should not be the end in itself, but a means of underpinning the delivery of a vision that's focused on people.

"The Rethinking Smart Futures report reflects a series of round table discussions held over the course of 2018 as part of the London Transport Museum's Interchange thought leadership programme," he said. "One central theme that emerged from the report is that if smart cities are seen simply as a purely technological concept, focussed on delivering developments such as the internet of things for their own sake, rather than harnessing those developments to meet human needs and ambitions, we will not be making the most of the opportunities to create a smart future for the UK that is focused on people."

Some of the key points outlined in the report include defining a shared vision for the UK's smart future and re-defining measures for success, creating trusted and regulated processes and networks for data-sharing that are resilient to cyber-attacks and collaboration between central and local government, with the private sector, to invest in and fund local schemes that support "blue-sky" innovation.

Grant Klein, UK transport leader at PwC, said the biggest priority in making a smart city work is to get everyone aligned to a common vision and purpose which is focused on the needs of people. "This will inevitably include data sharing agreements that will support and deliver the best, joined up services for that city's citizens," he added. "This will in turn connect multiple services and activities, and it is here that the IoT has an underpinning role to play."

Interactive information board

PHOTO CREDIT: THALES

Is there room in the real world for IoT?

MARK WHITEHEAD, sales and marketing manager at DAJO Solutions

Is IoT the biggest thing since the internet or just a fad perpetuated by hollow tech start-ups with no real substance?

That second option is unlikely. According to a 2015 report by global management consulting firm, McKinsey and Company, IoT could account for 11 per cent of the world's GDP by 2025. Not only that but it will touch on every aspect of our lives, business, social, health, travel, shopping, even our homes. However, it isn't a done deal.

Synching barriers

For a start, we need a uniform framework that everyone can work with. And there just isn't at the moment. There are numerous communication networks, protocols and languages that do not integrate effectively with one another. Think of a Russian with a phone trying to communicate with a German who has a pen and paper.

The problem is, historically, equipment hasn't had to communicate outside its own mini system. This meant many manufacturers developed their own proprietary systems catering to their own specific needs. Some of these frameworks did develop beyond their initial scope into something that is more widely distributed, but they are still far from universal.

This lack of requirement for interconnectivity from users meant that equipment was selected on its ability to perform a specific individual function, rather than its ability to communicate with other systems. This further exacerbates the problem, with legacy equipment having to be considered and possibly onboarded as part of any IoT initiative.

Security barriers

The more connected we become, the more opportunities there are to connect with us. That's great when those connections are legitimate, but how do we identify and deal with the threats? How do we shore up the vulnerabilities when we don't know what the vulnerabilities are? And whilst hackers focus on getting better at exploiting vulnerabilities, legitimate organisations have to be able to defend against a vast variety of threats, spreading their resources over a wider area.

Manufacturers of connected devices have a responsibility to ensure their products are as secure as possible, but they cannot be held accountable for things outside their remit. Many system vulnerabilities will come from the architecture of the system, often being unique to a particular combination of devices. In these situations, it will fall to the owner of the application to resolve those vulnerabilities.

Skills barriers

There is already a massive skills gap in this industry. But to fully exploit IoT, organisations are going to have to embrace new engineering disciplines. Keeping abreast of a set of capabilities and associated skills that are developing much faster than any other area of engineering.

This in itself is a risk as these skills, at least initially, will be in great demand. If they are lost to an organisation for any reason, they will at best result in a loss of momentum, at worst they could leave the organisation in an extremely vulnerable position. Either commercially or in terms of security.

Mitigating these risks will require innovating thinking, an engaging culture, and a proactive learning and development programme.

Individual organisations can only do so much to overcome these issues. Creating workarounds and customised solutions that work on a one-off basis. For a more effective and overarching solution someone needs to take charge and set out some guidelines that deliver an effective set of standards that everyone can adhere to. Sadly, this is some way off.

The impact IoT will have on any given organisation depends massively on what their objectives are, how much of a priority they make it and how much qualified and effective resource they dedicate to it.

In essence there are two main objectives that IoT can support:

Developing organisational infrastrcuture

IoT has the flexibility to be implemented modularly into any organisation. Eventually even going so far as to link every department, enabling you to find hidden correlations between them, no matter how seemingly unrelated they might be. In turn, this information can allow you to enhance efficiency, spot trends, and enhance communication.

Developing products and capabilities

Ensuring that your customers have access to the data generated from their use of your products is a great way to enhance value and ultimately, market share.

In doing these, you need to consider whether there are existing protocols used in your organisation, if there is an opportunity to gain valuable user information, how the user will connect the device to the network and who owns, pays for and has access to the data.

Implementing any kind of IoT project is a massive departure from the industrial norm and has to be taken seriously. It also has to be viewed realistically, these things take time to research, specify, design, prototype (redesign and re-prototype) before they can finally be considered for implementation. Ensuring you have adequate project and contingency planning in place is an essential part of the development process. Only you can know what priority the project should have, and at what pace you want it to move. These issues need to be addressed before the project begins in earnest, and appropriate levels of funding and man power have to be dedicated to them.

It would be extremely difficult to estimate the benefits of successfully implementing beginning to end IoT capability into an organisation, mainly because those that have done it have kept the results firmly under wraps.

The repercussions of poor implementation are less discernible, a slow creeping stagnation. A lack of growth, the root of which is hard to pinpoint, because its origin is something missing, rather than something present. A stagnation that leads inevitably to decline, as products are overtaken by those of competitors with better functionality and connectivity.

However, as big data becomes more accessible to smaller businesses thanks to cloud innovations from Microsoft, IBM and many others the benefits of IoT are becoming more and more attainable to smaller organisations.

That's because the overall objective of IoT is to connect into an existing data framework to enable greater transparency and therefore understand how to grow more efficiently and effectively. In order for that to happen there has to be a virtuous circle of engagement between IoT, big data, and the process development initiatives within the organisation.

New IT kit is just the ticket

Farming, entertainment and sporting venues had different IT needs... here's how they were met

Kitting out the countryside

The Royal Norfolk Agricultural Association (RNAA) is a registered charity dedicated to promoting the image, understanding and prosperity of agriculture and the countryside. In order to achieve this, it hosts the Royal Norfolk Show - the county's annual two-day agricultural event.

Unlike in the good old days when the most cutting edge piece of kit at these events were cameras, today people are equipped with some of the smartest devices on the market. That means internet connectivity is a basic necessity.

However, with limited infrastructure in place, to provide wireless access for corporate connectivity on a day-to-day basis as well as guest access, the RNAA realised it was in need of a completely new system. The shows require connectivity for both wired and wireless devices, that need to be controlled and on-boarded in a secure and simple to manage way. Areas where wireless coverage is required for the shows are predominantly in the main arena, which can have footfall of up to 50,000 people per day.

From an RF perspective this could cause a number of issues with interference, channel planning and capacity so the RNAA called DigitalAir Wireless for help.

The first stage, or "plan phase", was to conduct a wireless RF survey and develop a physical network design.

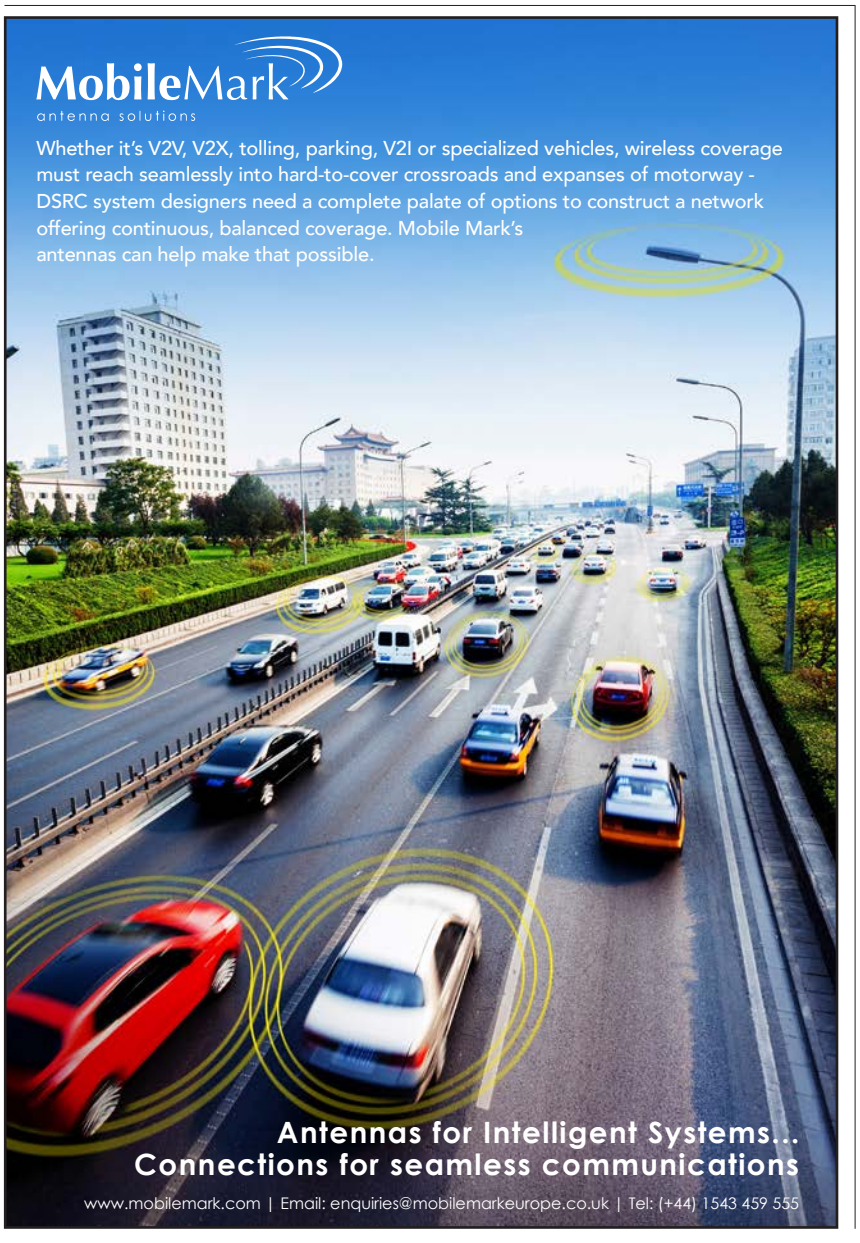
This provided physical access point locations, detailed information on the mounting of the access points as well as annotated photos.

Moving into the "design phase", DigitalAir provided a low-level design document which detailed the necessary information for the integration of the new network with the RNAA's existing infrastructure. This encompassed how DigitalAir was going to configure both the WLAN and the guest onboarding solution, as well as aspects of the LAN in order to integrate the system seamlessly.

The recommended solution was based on the Ruckus high capacity access point models which where R710, R510 and the T301n, with the Ruckus T301n access points being deployed to the Arena.

By using these APs and making use of the Ruckus T301n's internal 30-degree sector antennas to create small contention areas, it minimised co-channel interference from neighbouring APs and provided a managed area of RF for devices to connect to. The network, on a cloud-based architecture, was commissioned to the standard of the pre-approved LLD.

The network has now been utilised for a number of RNAA's high profile shows with great success. The Ruckus Networks system has exceeded the coverage and capacity expectations, whilst the guest platform has remained flexible to the demands of each show.



Cirque gets the Vegas treatment in Manchester

When it comes to entertainment, Cirque du Soleil needs little introduction. With a Las Vegas residency and The Beatles LOVE show to its name, they don't come any bigger when it comes to theatrical producers.

In September 2016, Cirque returned to Manchester after a five-year hiatus – for its spectacular show Amaluna (loosely based on William Shakespeare's The Tempest). That meant there was a lot of work to be done in order to provide a network infrastructure that befits Cirque's status as a showbiz juggernaut.

Open for a month across September and October, the performance was based in a big top next to the Trafford Centre. The open space was ideal for the show, but it didn't have the infrastructure of The Mirage.

Cirque relies on an internal, site-wide internet connection to access its intranet and technical documentation, run the box office POS, keep on top of the team's emails, and communicate with headquarters in Montréal, Canada.

Since the show was located in a big top on a piece of open land, there was no existing internet infrastructure for the troupe to connect to. Cirque needed a reliable internet connection as soon as possible while the team prepared the site before starting to rehearse for the show.

Event Support UK, the live event company working alongside Cirque, selected Telcom to carry out the work: within a week from the first call, a Telcom engineer team mounted a 25-metre mobile mast able to receive ultrafast internet and distribute it around the show's perimeter.

Our team brought our own infrastructure to the site, connecting the land to ultrafast internet via our hybrid fibre-wireless network. Site-wide internet became available during the weeks of preparation and throughout the 5 weeks Amaluna was showing live in Manchester.

Thanks to the connection, the troupe and staff was able to stay connected to HQ in Canada, access the shared database and run its box office as if it was on the strip.

Edwardian era football ground gets IT makeover

Brentford Football Club has an Edwardian era stadium in an up-and-coming part of west London. However, unlike most modern stadia that are built on wasteland away from homes, such as Arsenal's Emirates Stadium or West Ham United's London Stadium, Griffin Park has remained in a residential part of the capital since it was built back in 1904. Needless to say, the developers and owners were not thinking about internet connectivity at the time.

So, when the Championship club decided to host its MatchPlus 50/50 online charity game, blanket stadium Wi-Fi coverage was a must if it was to go ahead.

The first step was to identify and employ a company with solid experience in this space. Brentford chose nearby Simpli-Fi, which specialises in providing temporary and permanent Wi-Fi and IT solutions for the events, leisure, construction & education sectors. The perfect partner then for what the football club needed to achieve.

Simpli-Fi accepted the contract and then was charged with providing Griffin Park with Wi-Fi and internet connectivity for the numerous tablets and ticket purchasing machines. The firm provided the popular Ruckus external high-powered access points, which were installed strategically around the 12,763 capacity stadium to make sure there were no black spots. In short, Simpli-Fi had to provide the stadium with complete coverage.

Wanting to add what it describes as "complete peace of mind", Simpli-Fi provided this through a three-year managed service making sure that all onsite support, remote monitoring and helpdesk support is covered. This also allowed MatchPlus to spread the costs over a three-year period.

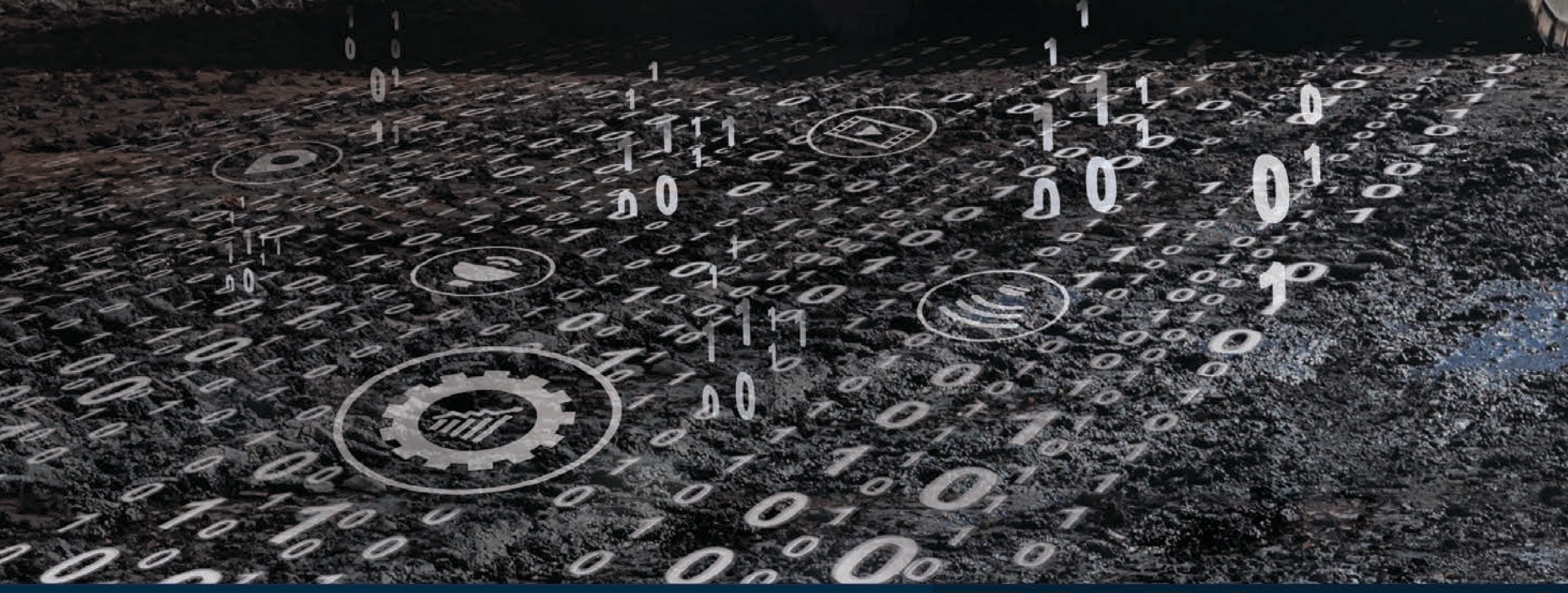
Now 115 years on from when it was built, the 20th century Griffin Park has 21st century connectivity, meaning it's perfectly poised to stage big events on and off the pitch.

TIRED OF MACHINES **DROPPING DATA?**

Time to Drop Your Network.

If operational data is important to you, then only a mission-critical network will do.

With Wi-Fi mesh, when equipment moves, it loses connectivity, dropping valuable insights into machine health, performance, and productivity, and causing production to grind to a halt.



Don't leave data behind: make your move to the 'never break' connectivity of Rajant Kinetic Mesh®.

Find out why the world's top mining companies rely on Rajant Kinetic Mesh® networks for the continuous, fully mobile connectivity required to power today's data-driven mining operations.

See what Rajant can do for your mine's productivity.
Request a proof of concept at **www.rajant.com/datadriven.**

RAJANT

© 2019 Rajant Corporation. All rights reserved.

Remote Management Technology

Power Distribution Units

AC Power

Racks & Integrated Solutions

Services

Software & Controls

Row/Rack Cooling

FREE GOOGLE HOME MINI

WHEN PURCHASING ANY QUALIFYING VERTIV PRODUCTS*

For more details, visit:
VertivCo.com/GoogleHomeMini

*Terms and conditions apply.
Offer valid until the end
of the quarter.

VERTIV.

COME AND SEE US AT DCW ON STAND D1362

RACK-SEC R-EDGE
A NEW GENERATION OF MONITORING & ACCESS CONTROL.

ISO 9001:2015

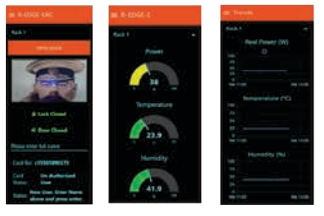
Mention DCIM and your world gets complicated, surveys, multiple site visits, meetings with IT and facilities departments. Then the development costs, hardware installations, set up and training. Ongoing licensing costs for server and software support, maintenance etc. When all you really need is sight of your rack temperature, humidity and power utilization. Your site BMS will give information to the facilities department on failure of equipment. Which could take time before it filters down to the IT teams affecting their environment. Using a combination of our R-EDGE devices to monitor your equipment and their environment we can create a cost affective solution MINI DCIM with no ongoing license fees. Featuring an easy to read live dash-board, which will alert you via email and or SMS instantly.

R- EDGE-M
- POE enabled
- Monitors the status of any critical equipment that has fault indicators and switching utilizing dry contacts
- Easy to read dash board with live 24 hour display
- Alerts change of status by email and SMS.

R-EDGE-ENT
- All the features of the R-EDGE-E with an on-board high resolution digital camera will record image of person opening the protected rack door.
- Email & SMS notification.

R-EDGE MASTER UNIT
We can build the dash boards to show multiple racks, equipment and environments utilizing our master control unit.
We can customise our devices to accomodate most interfaces

R- EDGE-E
- Temperature & Humidity Sensor displays on the dash board
- Email and SMS alerts at pre set thresholds
- On-board trending graphs for reports
- Add the power utilization, for monitoring on the dash board
- You will need an intelligent PDU with an SNMP connection again alerts at pre-set levels.



R-EDGE-EAC
- All the features of the R-EDGE-ENT
- The EAC unit monitors and controls racks utilizing retrofit electronic swing door/doors handles.
- The handles are fitted with an RFI proximity reader and can set up to read your existing site cards.
- Email & SMS notification.

USP's
- No licence fees
- SQL server space not required
- Minimal set up costs to multiple devices
- Uk manufactured and supported

info@rack-sec.com | 0800 0098100 | www.rack-sec.com
DESIGNED, MANUFACTURED AND SUPPORTED BY A UK COMPANY

Net health benefits

Transition to the Health and Social Care Network has been a challenge for NHS network managers and their service provider partners. Now it's time to see how HSCN can enable cost-saving digital transformation in public healthcare, writes JAMES HAYES

The mass migration from the outgoing N3 network to the new Health and Social Care Network (HSCN) infrastructure is one of the UK's biggest technological initiatives: that such an important NHS ICT project has attracted so little media coverage is a reflection of how successfully the roll-out has been managed by the parties involved, from overseeing agency NHS Digital, through to the service delivery providers, and ultimately, its healthcare sector customers.

The replacement to N3 – the IP-based VPN that had connected NHS England and Scotland locations and 1.3m employees since 2006 – went live in April 2017, and user migration between the two broadband networks is now largely complete. Designed and built by NHS Digital in partnership with suppliers and customers, HSCN connects England's health and social care practices' data exchange needs via connectivity procurable from a choice of 26 registered Consumer Network Service Providers (CNSPs) – in contrast to the BT-owned/managed N3.

CNSPs must achieve two stages of HSCN compliance. Stage one primarily demonstrates that they can deliver HSCN connectivity in a way that meets the obligations and standards set out by in the HSCN Obligations Framework. Stage two compliance is achieved when suppliers provide NHS Digital with detailed solution design info, and successfully connect to the HSCN central services (including the HSCN Peering Exchange). Once compliant and up-and-running, CNSPs are equipped to take their services to the new buyers' marketplace and re-establish relationships with healthcare sector customer, existing and new, including the NHS and its supply chains.

Network managers in the NHS have been too busy over the last 12 months to publish progress reports on the restructurings they have had to effect at their end of the change; CNSPs, meanwhile, are, again, well-placed to provide perspective on how this transition has proceeded. Networking+'s review of HSCN roll-out in the February 2018 issue heard from CNSPs as they prepared to embark on the last 12 months of the transition schedule, and detailed how, in addition to the technological challenges faced by NHS network managers, their colleagues dealing with service procurement were also on a steep learning curve, as they become accustomed to new market conditions.

Reports from a changing frontline

"Procurements for services have progressed in line with expectations," says Mike Thomas, managing director, Innopsis (trade association for suppliers of digital infrastructure and services to the UK public sector). "It's a good sign that the number of suppliers is higher than anticipated. It demonstrates the attractiveness of the market. There have also been sales of HSCN services in addition to the migration of N3 circuits, which again indicates whole market expansion as a result of HSCN."

"As with any large and complex data network migration involving multiple customers, suppliers and a legacy transition network, it takes a lot of plan-and-prep to migrate these services, especially those that provide critical health and social care," Sam Winterbottom, head of public sector sales, Gamma, points out. "The majority of the N3-to-HSCN procurement activity, conducted and awarded over the last 12 months via aggregated procurements, is the relatively straightforward bit. Customers and suppliers who have won HSCN aggregated procurements, are now primarily focussing on this migration activity."

According to Martin McFadyen, head of public sector at Virgin Media Business, nationwide roll-out of HSCN is still mixed: "Some parts of the country have steamed ahead, while other parts are playing catchup," he reports. "Many of our projects are already complete, but there is still work for the NHS to do."

HSCN is "being delivered – however, to state it is 'largely completed' would be a little optimistic," agrees Gareth Ricketts, major accounts-health lead at Capita IT & Networks. "[But] for such a large migration, the overall picture is positive."

"Many of the organisations that have already migrated already benefit from higher bandwidth connectivity at a much lower operational cost than the legacy connectivity," according to Iain Shearman, managing director at KCOM NNS. "As more organisations migrate, NHS Digital will be able to decommission larger parts of the legacy network. This will accelerate cost savings to the NHS and will deliver tangible ROI." More on ROI later.

No pain, no gain

The journey to this brave new added-value communications environment has, of course, thrown-up some pain points along the way, observes Thomas. "The lack of updates to the site records [for the] three years prior to HSCN procurement and the scale of the estate being migrated, has meant that the quality of the information and the requirements were significantly different to those initially reported in many areas," Thomas says. "The result is that time has been spent making sure the sites exist, have the correct addresses, and the services requested are appropriate for the requirements. This has meant that a number of sites have been able to procure better services than anticipated, often for less than budgeted."

The basic connectivity has "caused few issues", says Ricketts. "The main 'pain points' for NHS infrastructure managers have been the overlay services, like voice

"Procurements for services have progressed in line with expectations."

Mike Thomas, managing director, Innopsis

and teleconferencing." The issue with overlay services has been highlighted by the supplier community for years, Ricketts acknowledges, but warns that without a central solution to the problem, the current national provision could splinter into a series of smaller Community of Interest Networks, "which could mean these services are both more expensive, and less integrated, across the country."

"The other key pain point is probably around the actual migration of circuits from the Transition Network to HSCN in itself; the migration of existing IP addresses would be one example," Sam Winterbottom at Gamma says. "De-risking this migration process is vital, and NHS Digital have gone a long way to ensure migrations are as risk-free as possible."

"The biggest pain point in transitioning to HSCN is overcoming the legacy of having separate health and social care organisations. The benefits can only be fully realised by taking a joined-up approach, but this requires structural and cultural shifts," says McFadyen. "Smaller organisations have told us they don't have the right skills and knowledge to manage the change. They're looking for guidance on the services that should be replaced, and how to access funds to manage the transition."

"Customers and suppliers who have won HSCN aggregated procurements, are now primarily focussing on this migration activity."

Sam Winterbottom, head of public sector sales, Gamma

"From my discussions with network managers, all of us have been on a learning path to understand the split between the bandwidth of a tail circuit at a site and the size of the bandwidth required to connect to the HSCN core," says Gamma's Sam Winterbottom. "In some conversations I have had, most of an organisation's data traffic is between their own sites, and so they simply don't need their HSCN bandwidth to match the bandwidth of each individual tail circuit."

"Network managers do know their networks inside out, and add real value when sharing operational insights," says McFadyen. "They also understand how their organisation is evolving, and what pressures and challenges that will mean for their network in future. When organisations 'think big' about how they deliver services in future – using the HSCN as an opportunity to transform operational capabilities, for example, and offer new services like virtual consultations – there's more scope to add value."

Connectivity change opportunity?

When it comes to an appetite for HSCN user organisations to see adoption as an opportunity to revamp their broad ICT structures, no conspicuous trend seems yet to have emerged. Virgin Media Business's McFadyen describes it as "a mixed bag" with NHS organisations (and their suppliers) falling into one of three groups: the first perform simple like-for-like replacements which tend to miss some of the wider opportunities. The second group invests in its wide-area network at the same as HSCN, and benefits from greater choice and competition in the market which, ultimately, helps drive down its costs. And thirdly, there are those organisations that take a strategic approach, take a step back and procure an environment for the future which takes full advantage of the HSCN opportunity.

"A culture of incumbent extension has been the norm in the main, whereby BT and Virgin have maintained the current service provision, with a 'soft' switch from N3 to HSCN," explains Ricketts. "Therefore, we have not seen many large-scale reviews of enterprise communications. This is partly because of the need to maintain service and partly because the holistic review of a [given] Trust's enterprise communications requires too many people to put aside time and resources they don't have."

However, migration from N3 to HSCN has offered "a chance for healthcare organisations to review their connectivity requirements," avers Gamma's Winterbottom – and that has meant a complete review for some of those organisations. "The requirements for bandwidth have increased in comparison to those being delivered through N3. And, it has been a good time to review; as the 'internet first' policy gains momentum and more and more services move to the cloud, an organisation's bandwidth requirements will increase."

Health-social care integration

"Where organisations are still at various stages of migrating to the new network, there are some clear needs identified in terms of what IT needs to deliver," reckons Jason Hall, director at BT Health, writing in the 2018 iGov 'Connectivity across the NHS Survey Report'. (The survey polled a cross-section of IT job roles across NHS, Clinical Commissioning Groups, and the wider healthcare sector.) "The need to do more for less is a key focus for customers in thinking about their IT strategy. HSCN offers huge opportunities as a platform for health and care organisations to underpin digital transformation strategies and [fundamentally] transform how healthcare services are delivered."

The iGov report also found more than 50 per cent of its respondents to be reviewing their IT strategy in the 2018-2019 timeframe, and looking for collaborative options – often with social care organisations, adding additional complexity to the HSCN implementation challenge.

"For such a large migration, the overall picture is positive."

Iain Shearman, managing director, KCOM NNS

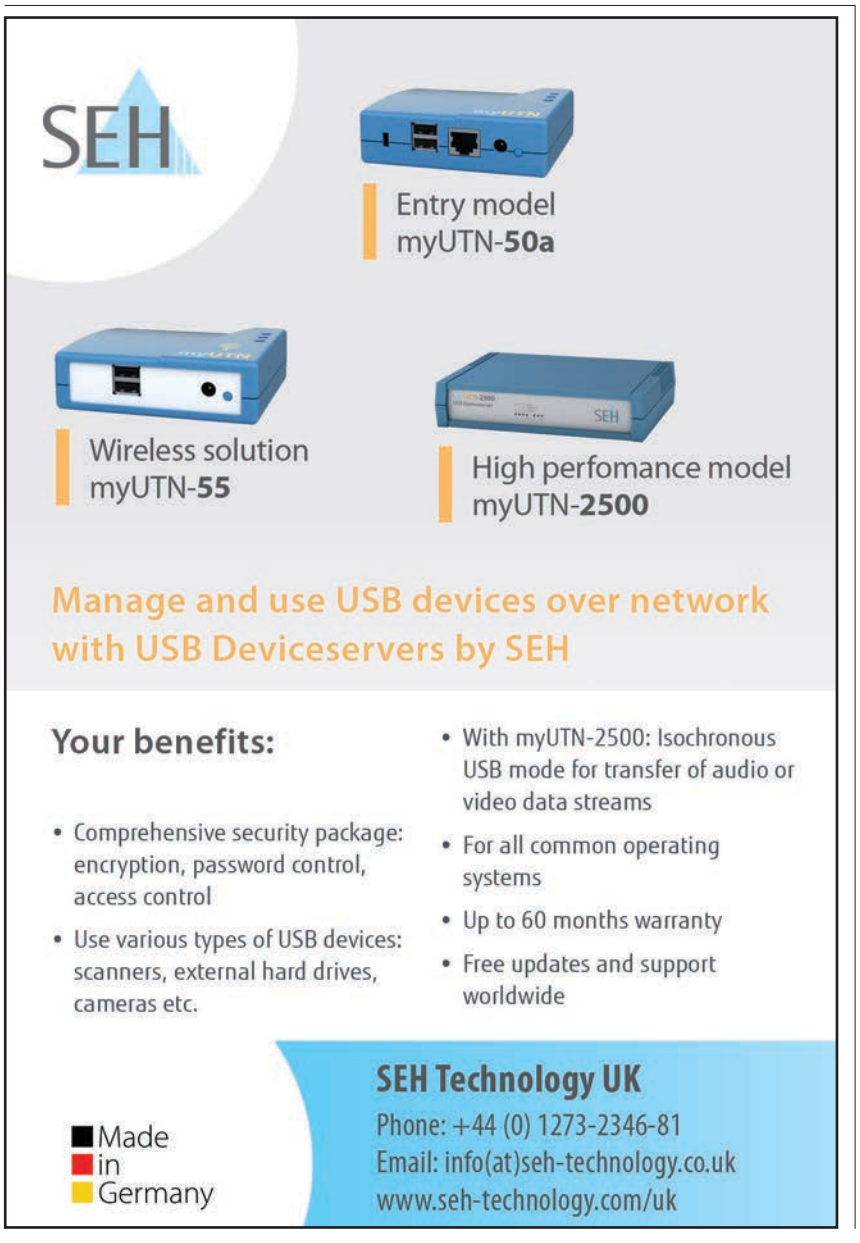
"From a commercial perspective, the drive for more bandwidth has been helped by the introduction of multiple suppliers in a competitive HSCN marketplace, which has resulted in lower costs for more bandwidth," says Gamma's Winterbottom. "We hear this daily. However, the conversation around requirements has changed. Tail circuit bandwidth at each site does not necessarily mean that the same HSCN core bandwidth is required. There is a little more scoping discussion required to find a solution that best fits than there was under N3."

"We took part in the main waves of aggregated procurements for HSCN migrations, mainly throughout the first half of 2018. We were somewhat surprised to find that nearly all these large procurements contained hardly any actual HSCN connectivity. Most of these procurements – around 80% – were for inter-site connectivity, joining together outlying clinics, hospitals, social care, and education sites," says Darren Turner, general manager at Carelink. "While we could compete on providing actual HSCN connectivity, we had a significant commercial disadvantage for inter-site connectivity, where network providers with infrastructure already in place were able to offer rock-bottom pricing. So yes, almost without exception, healthcare organisations have taken this opportunity to migrate their entire network infrastructure."

"In the early stages, much of the emphasis has been on the connectivity

"Some parts of the country have steamed ahead, while other parts are playing catchup."

Martin McFadyen, head of public sector, Virgin Media Business



delivery," says Iain Shearman at KCOM NNS. "As the project gathers increasing momentum, however, the focus is now moving to how HSCN can be utilised as an enabler for the NHS strategic digital transformation programme."

Return-on-investment

"On the basis of the pricing levels that were winning some of the large aggregated procurements – and assuming the migrations are completed as scheduled – I expect a pretty rapid ROI to come in a combination of actual savings and increased performance," declares Darren Turner at Carelink. "We were seeing bandwidth charges 80-90 per cent lower than the rates we'd become accustomed to on N3."

"The closure of the N3 Transition Network points-of-presence, and the reduced budget requirements experienced by the organisations who have migrated, will deliver the HSCN ROI," says Thomas. "However, this would just be in the terms of 'like-for-like'. In addition to the fiscal savings, the increased capability, increased supplier market and the increased sets of services and overlay services will add a further level of benefit."

The introduction of stratified competition into the NHS market via the HSCN has meant a major reappraisal of connectivity charges, says Ricketts, which in the main has considerably improved the ROI for the NHS: "This program by this measure has been a great success and considering the scale and criticality of the network, such a relatively smooth transition must be applauded." However, although basic costs have been reduced, "the chance to tackle the bigger issues and move towards the strategic goals of 'Internet First' and 'Cloud First', were never really addressed."

In this context, the fact that expenditure savings are dependent on HSCN's operational life expectancy, and that emergent connectivity technologies will likely see the NHS undergo further digital transformation as it progresses into the 2020s, should be factored into any longer-term ROI expectation.

"The NHS can demonstrate value right now," avers McFadyen. "HSCN provides clarity to suppliers, supports interoperability, offers greater choice and encourages competition in the market – essential to driving down cost and price. It also provides an opportunity for third-sector community organisations to play a role in a holistic care system. Even this early on the transformation journey, and using only the coarsest measure for value (price paid), NHS customers are already realising truly significant savings. And the benefits start as soon as customers take their first steps."

"Over the next 12 months, once migrations away from the HSCN Transition Network and onto HSCN proper have kicked in, the NHS will be able to demonstrate significant return-on-investment, agrees Winterbottom. These migrations "would never happen without the hard graft of health organisations and their IT managers. They have been working closely with their internal stakeholders and suppliers to make it happen."

Winterbottom adds: "There are a lot of moving parts to be considered, and progress has been slower than expected – but let's not forget, it has never been done before!" ■

An early HSCN adopter

Humber NHS Foundation Trust provides a range of services to around 60,000 people in the Hull and the East Riding of Yorkshire region. It employs 2,500 staff across 70 sites. The Trust's acquisition of geographically-distant new sites, plus the ever-increasing demand for enterprise network and internet access, prompted it to use the launch of HSCN as an opportunity to review its then network provision. Migration to a HSCN-based solution enable it to rationalise its legacy infrastructure, which has led to greater capacity, cost savings, and additional resilience for both Humber and the smaller, local Trusts it provides support services for, Humber reports.

An increase in the number of sites with network connectivity means that frontline staff can deploy the applications patients require, supported by faster access to clinical information during consultations. This has led to increased patient awareness of some of the systems and services available over HSCN – and heightened demand.

By early adoption of HSCN connectivity, and with support from NHS Digital and technology partner KCOM, Humber devised what it calls a 'novel networking solution'. This has allowed more open access to health information, protected by HSCN's security-enhanced features. In conjunction with other developments this has reduced time wasted for corporate and clinical staff. This leads to less frustration with underperforming connectivity and increased satisfaction and health outcomes for patients and staff, reports report Paul Wright, IT operations manager at Humber.

"The implementation of the new network across East Yorkshire has enabled staff to work in an agile fashion, reducing the time spent travelling across the county, supporting an ageing network infrastructure," says Wright. "It allows trust IT support staff to work more closely with our colleagues in other trusts, building relationships to help us to improve the service we provide for interconnectivity across our supported trusts."

Humber NHS foundation trust head office

See it all from the centre

Products that promise to keep your network safe. And SEAN HERBERT explains how the Industrial Internet of Things (IIoT) has made security even more important

In recent years, the number of endpoints to be monitored in corporate IT networks has increased massively.

One of the reasons is that more businesses are embracing Industry 4.0, where industrial plants, factories and even construction sites are now equipped with internet connected devices and machines.

This high level of connectivity, referred to as the Industrial Internet of Things (IIoT), means that both IT and OT (operational technology) managers must provide continuous and reliable monitoring of not only employee laptops and devices, but all the connected machines and automated systems that are present within the manufacturing process.

As these non-traditional endpoints serve as additional doorways for cybercriminals to access, it is imperative that administrators can immediately identify weak points and distribute necessary patches to protect the network against security threats.

If administrators monitor endpoints manually, mistakes may occur unnoticed, and existing vulnerabilities can be missed. This is especially true within industrial environments, where OT managers are more reluctant to use software patches as changes to machinery can potentially involve re-certification and production delays. Accordingly, both IT and OT managers need an endpoint management solution that is hassle-free and easy to use.

To properly monitor and secure the increased number of endpoints in corporate IT or production environments, businesses should strive for a centralised approach.

From a single viewpoint, administrators would be able to manage all connected devices, automate routine tasks as well as deploy and update applications and patches. Administrators need to be able to monitor the entire network setup and structure and automatically catalogue all network devices, configurations, installed software, and the drivers for endpoint subsystems.

A centralised viewpoint could enable both the technical and organisational level of a business to get a transparent and traceable overview of all endpoints within the network, which is necessary to ensure efficient corporate IT. With Industry 4.0 growing exponentially, IT teams need to be able to scan the IT environment for any irregularities or vulnerabilities, including incorrectly configured user-owned hardware and unpatched or unlicensed applications, as a breach could have catastrophic consequences for national infrastructure.

An automated, centralised approach to network monitoring has the potential for IT and OT managers to save valuable time and secure management of ever evolving endpoints to ensure all future industries, even beyond 4.0, are secure.

Sean Herbert is UK country manager at Baramundi

Security is at risk in six out of 10 companies because they cannot check when their employees connect mobile devices to third-party networks. And nearly 50pc of mobile workers spend most of their working hours logged on to public Wi-Fi and carrier networks with iOS, Android and Windows mobile devices.

More than half of companies surveyed did not require users to connect to a corporate network through a secure VPN.

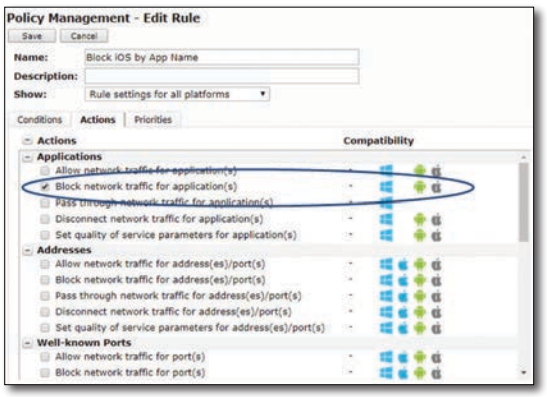
Quoting these survey figures, **NetMotion Software** has added an "aware" feature to its *Mobility* software as well as new visual dashboards to its *Mobile IQ* product.

This, it says, will secure and manage mobile worker access to web applications and domains across any network.

For example, if a user roams to an unsecure Wi-Fi network, dynamic web filters can automatically enable encryption or block web application and domain access to protect the user and prevent security risks.

The main features in the "aware" release include dynamic web filtering which, says NetMotion, provides awareness and controls access to unsanctioned domains and websites, ensuring worker security and productivity; full visibility into the web resources accessed by users, devices and applications; enforcement of security and compliance policies for any network; and biometric authentication enhancements including facial recognition for increased user and device security.

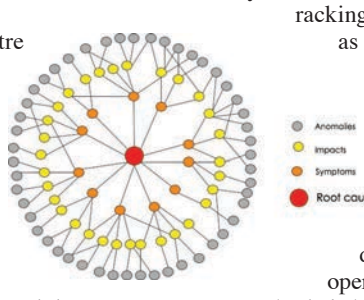
NetMotion says the new visual dashboards in Mobile IQ give unique visibility and security control over the web resources being accessed by users, including the devices and applications.



In the latest update to *Apstra Operating System* (AOS 2.3), the company has added what it calls "root cause identification".

This, says **Apstra**, finds the underlying reason for identified problems by studying system telemetry in real time.

AOS, described as intent-based data centre automation, works with a wide range of switches and switch operating systems.



Apstra says it understands not just the structure and elements of the network but also the intent of the architect and the operator; that is, what the network is required to do.

It compares the intent with actual network behaviour, using this information in real time to automatically pinpoint and isolate problems – such as grey failures, performance degradation, and new outages without a mass of false positive alerts.

Root cause identification then digs down to identify the source of the problem.

Apstra says the AOS user interface enables operators to design, build, deploy and operate a spine-leaf network in days, rather than months. This includes racking, stacking, cabling, as well as validating that all design intent is met, and continues to be met, in real-time.

AOS, it says, helps users to automate their networks as a single system, not as complex individual parts. It decouples network design, implementation and operations from the physical (underlay) and virtual (overlay) network infrastructure, using whichever hardware and switch OS is chosen.

AOS, says Apstra, can be deployed in modern data centres -- both new and existing -- across multiple vendors. It operates at the management plane and controls devices and switch operating systems through their published open APIs.

New from **Riverbed** is a product which the company says transforms network data into cybersecurity intelligence.

Called *SteelCentral Advanced Security Module*, it is said to provide essential visibility and forensics for broad threat detection, investigation and mitigation.

Riverbed says it uses full-fidelity network flow analytics to capture and store all the data needed for forensic analysis. It delivers insights and empirical evidence to detect and investigate advanced threats that bypass typical preventative measures, as well as those that originate inside the network.

Designed for security operations teams, the new software module is said to offer a wide range of threat detection features.

It raises alerts if the user's system communicates with blacklisted communications -- such as known malware download sites and command and control sites – allowing prompt investigation and action.

It also quickly and accurately identifies a broad range of DDoS attacks so customers can make informed decisions to end interruptions simply and seamlessly.

In addition, says Riverbed, the module automatically identifies threats that generate unusual patterns, such as unexpected new services, hosts or connections.

And SteelCentral proactively searches for hidden security threats on a network before they affect the business.

It also provides full historical details so customers get the complete scope of the attacks, reducing the likelihood that future attackers will get the data they want.

As well as network monitoring, NetProfiler provides insight into cloud usage, answering such questions as what resources are in use, who is using it, are cloud resources being used efficiently, are unknown costs being incurred, and helps to fix problems.

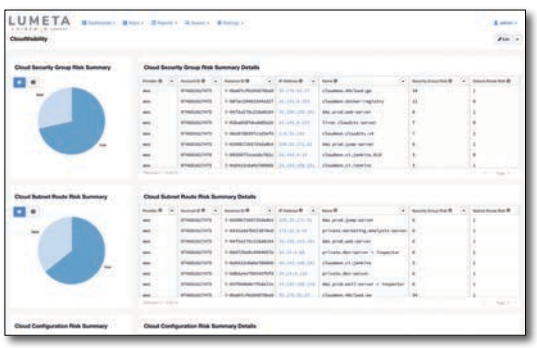
Now that companies are likely to use more than one cloud provider, **FireMon** has introduced *Lumeta CloudVisibility*.

Developed from its predecessor, Lumeta Spectre, it is said to offer real-time infrastructure visibility, change monitoring and leak-path detection.

It does this, regardless of cloud platform, for physical, virtual, software-defined, on-premise and hybrid environments.

Lumeta CloudVisibility is designed for large enterprises that require seamless visibility of assets from Layer 2 to the cloud.

FireMon said it means that security teams can ensure the right policies are applied to every asset, identify leak paths that are vulnerable to attack and easily identify suspicious network behaviour. They can then achieve continuous security across their hybrid enterprise and be much more adept at managing change in the future.



Lumeta CloudVisibility is available in an enterprise edition, as well as a free "community" edition so that organisations can try the tool. The enterprise version of Lumeta CloudVisibility is now available for pre-order; the free download will be available in April.

In addition, Lumeta CloudVisibility Community Edition featuring multi-cloud capacity, higher account key limits and bundled support options will be available for users who download from the FireMon website.

Cloud platform marketplace users will find the Lumeta CloudVisibility Community Edition in the Amazon Web Services (AWS) Marketplace later in April, followed by the Microsoft Azure Marketplace and the Google Cloud Platform (GCP) later this year.

Lumeta, recently acquired by FireMon, was spun out of Bell Labs in 2000.

New training aims to help beat the cyber crooks

Concern about the shortage of professionals with skills to combat cyber threats has prompted the founding of the Professional Development Institute (PDI).

It offers free online self-paced training, including videos, to members and associates of the International Information System Security Certification Consortium, abbreviated to (ISC)2.

A spokesman said the PDI could be thought of as the Open University for top-up cyber security training.

The consortium, founded in 1989, claims more than 140,000 members. About 28,000 are in Europe, the Middle East and Africa, with most in the UK where it has seven chapters and an office in London.

It was set up to establish single curricula and certification; until then a number of associations organised their own.

Applicants take one of 12 paid-for training courses and then sit an examination to achieve certification. The best known is the Certified Information Systems Security Professional (CISSP). Then the annual subscription is 125 US dollars.

The CEO of the consortium, David Shearer, said: "The Professional Development institute is recognition that cyber security education is a lifelong journey and that achieving professional certification, while important, is only one step along the way."

It says that making PDI courses available in an easily-accessible online format would help members maintain a work-life balance.

During the next two years, 18 additional staff are expected to be hired to develop PDI, adding to the 160-plus already in place at the organisation. And a 765 sq ft video production studio is planned at the consortium's HQ in Clearwater, Florida.

All of the consortium's courses are available to non members at "competitive" prices.

Hot topics for engineers

DevOps and network automation are the new hot topics in networking, reports Systems & Network Training (SNT) which is running its updated DevOps for network engineers course starting on May 13. The five day event costs £2,917, including lunches and refreshments, and will be held at the company's HQ near Redhill, Surrey. It will cover Ansible, Git and Python along with NETCONF and RESTCONF. And the company says the new Ansible 2.7 networking enhancements are included.

SNT has also developed a range of courses for network engineers in areas which they may never have had to explore previously, including the subjects in the May course and Linux and Jenkins. The company also offers LINX accredited training.

LINX is the London Internet Exchange, a not for profit company with 800 members, where SNT has held taster sessions at member events. Demand at these events in part prompted the new courses.

New academy for SMEs

Nine out of 10 data breaches are caused by human error, despite raised awareness of the problem.

Quoting this estimate, Xcina has set up an academy to offer SMEs online and classroom courses ranging from cyber awareness and GDPR refreshers to packages for future topics such as Making Tax Digital. Prices start at £25 per licence.

Xcina Academy, built on the company's ecommerce platform, also provides a learning management system (LMS), which has a real-time dashboard outlining progress made across customers' companies. This is designed to support governance assurance and compliance for GDPR and other regulatory frameworks.

There are plans this year to expand into regulatory and business risk management services such as virtual data protection office (vDPO) and an online apprenticeship scheme.

It will also address the recent senior manager and certification regime, which introduces a duty of responsibility on all senior management to take reasonable steps to prevent and detect regulatory breaches.

Xcina, part of Shearwater Group, has offices in the City of London, Penarth and Preston.

IN BRIEF...

■ Newly launched, Knowledge Center promises online training which is vendor neutral, saves on training budgets and allows self-paced study.

It has been set up by Cloud Security Alliance, a not-for-profit organisation which has 90,000 members worldwide, including a chapter in the UK.

Membership is free; the courses offered by Knowledge Center cost $495-$895. Among them are the certificate of cloud security knowledge and cloud governance and compliance.

■ The UK's tech and IT professionals are now more likely to blow the whistle on an employer's misbehaviour in the wake of scandals in the sector, with almost a quarter (23.6 per cent) now willing to quit their job should a similar scandal strike their company. That is according to research from job site Indeed. It found that almost half (46.2 per cent) of staff said they were more likely to report any wrongdoing than they were before the scandals came to light. More than a third (36.1 per cent) of those aged 16-24 said they would leave their job should a scandal strike. That figure far exceeded the quarter (24.8 per cent) of those between 25 and 44-years-old and the tenth (9.2 per cent) of those aged 45 and over. Some 44.6 percent said a sexual harassment scandal was the most likely to cause employees to leave their company, ahead of tech-based scandals (43.2 per cent).

■ Manchester tech firm UKFast has created 100 new apprenticeship roles within its IT, software development and customer service programmes, "in a bid to supercharge the region's tech talent pool". The scheme has seen more than 80 apprentices graduate in the last three years, with 18 per cent of the company's workforce being current or former apprentices. UKFast has employed four full-time teachers to run the programme. Founder and chief executive officer Lawrence Jones said he wants to scale the apprenticeship programme to meet the growing need for programmers and software developers, internally and within the wider tech community.

TeraStation™

The Securest NAS for Businesses.

With VIP Service and lifelong technical Support.

TeraStation™ 3010

Cost-effective NAS solutions for SMBs

- Available in 2- and 4-bay desktop or 4-bay rackmount versions
- Fully equipped with NAS hard drives
- Total capacities from 2 to 16 TB

TeraStation™ 5010

Scalable High-Performance Network Storage

- Integrated 10GbE ports
- Partially/fully equipped with NAS or Nearline (TS51210RH) HDD and available as 2-, 4-, 8-bay desktop as well as 4-/12-bay rackmount version
- Total capacities from 4 to 120 TB

TeraStation™ WS5020

Ideal NAS for Windows-based environments

- With Windows Storage Server 2016
- Integrated 10GbE port
- Available as 2- and 4-bay desktop or 4-bay rackmount version
- Total capacities from 4 to 32 TB

VIP SERVICE

24h HDD-REPLACEMENT

TeraStation Advanced Replacement

3 YEAR WARRANTY

5 YEAR WARRANTY

UPS DROP-OFF SERVICE

IP EXPO MANCHESTER

Visit us on Stand **N314**

www.buffalo-technology.com

BUFFALO™