www.networkingplus.co.uk

MAY 2017

networking

FIXED & WIRELESS NETWORKS FOR ENTERPRISE USERS

On the buses
Datto keeps Reading Buses running after repeated ransomware attacks
News, p3

The power to deliver
Networks to help the energy sector keep the juice flowing
Real World Networks, p8

Cyber security
In the face of rising threats, how can you keep your precious data safe?
Feature, pp10-13

Switchcraft
The latest switches to support today's bandwidth hungry networks
Off-the-shelf, p14

IBM builds its most powerful universal quantum processors

IBM says it has now successfully built and tested its most powerful universal quantum computing processors. The commercial prototype will make its debut as the core for the first *IBM Q* early-access commercial systems.

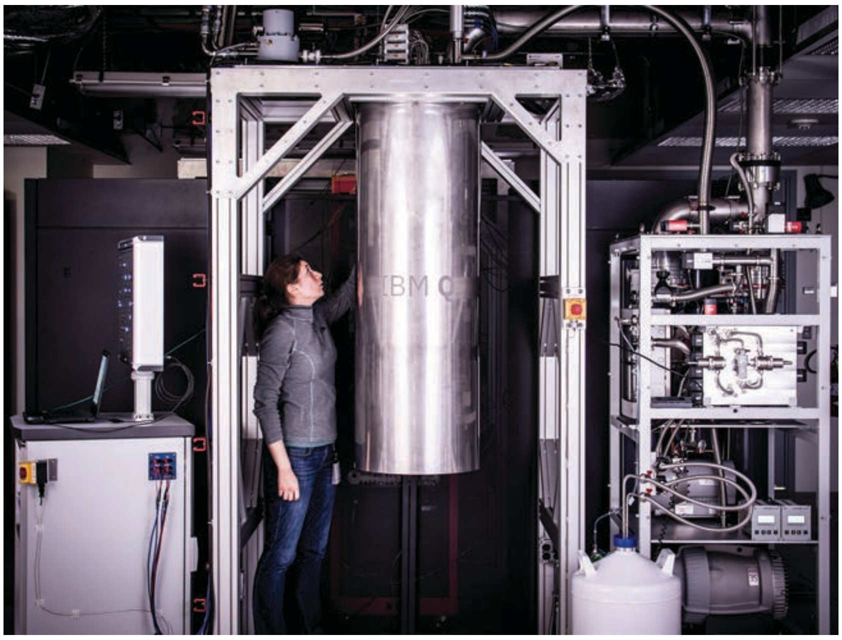
Under the *IBM Q* initiative announced earlier this year, the company plans to develop the world's first universal quantum computing systems for business and science applications *(see News, March 2017)*. It claims this will create the foundation for solving practical problems that are too complex for today's most powerful classical computing systems.

According to IBM, future applications of quantum computing could include cloud security where the laws of quantum physics are used to enhance the security of private data in the cloud. It could also help optimise business by providing improved solutions to complex problems found in supply chains, logistics, modelling financial data and risk analysis.

In mid-May, IBM unveiled two new processors. They include the company's first prototype commercial design with 17 qubits. It is said to leverage "significant" materials, device and architecture improvements to make it the most powerful quantum processor so far created by the company.

IBM adds that it has been engineered to be at least twice as powerful as what is available today to the public on the *IBM Cloud*, and will be the basis for its first early-access commercial systems.

(continued on page 2)



An IBM researcher examines a cryostat with the new prototype of a commercial quantum processor inside.

PHOTO: ANDY AARON, IBM

Government and financial sectors top targets for cyber attacks

Cyber attacks on governments around the world doubled in 2016, increasing from seven per cent in 2015 to 14 per cent. Attacks on the finance sector also rose from just three per cent in 2015 to four per cent of all attacks in 2016.

The manufacturing sector came in at third place at 13 per cent, while the retail sector, which topped the list of all cyber security attacks on all sectors in 2015, moved down into fourth place (11 per cent).

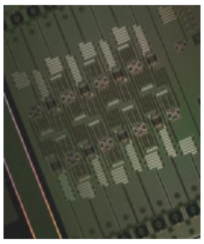
Those are the findings from NTT Security's latest *Global Threat Intelligence Report*. It was compiled from network data collected from 10,000 clients worldwide, 3.5 trillion security logs, 6.2 billion attempted attacks, together with 'honeypot' traps and sandboxes in more than 100 countries.

Of attacks targeting EMEA, France and the UK accounted for the most at 11 and 10 per cent, respectively. NTT says three industries in the region were targeted in 54 per cent of all cases: finance (20 per cent), manufacturing (17 per cent), and retail (17 per cent).

The study also reveals that 63 per cent of all worldwide attacks originated from IP addresses in the US, followed by the UK (four per cent), and China (three per cent). NTT says the US is the main location of cloud-hosted infrastructure globally, and hackers often utilise public cloud to orchestrate attacks due to the low cost and stability of the infrastructure.

Of the IoT attacks detected in 2016, two thirds were attempting to discover specific devices such as a particular model of video camera, three per cent were seeking a web server or other type of server, while two per cent were attempting to attack a database. ■

Will we ever be safe? Cyber security feature pp10-13



IBM's upgraded 16 qubit processor will be available for use by researchers to explore quantum computing using a real quantum processor at no cost via the IBM Cloud.

IBM processors

(continued from page 1)

The second device is a 16 qubit processor which, says the company, will allow for more complex experimentation than the previously available five qubit processor. It is freely accessible for developers, programmers and researchers to run quantum algorithms and experiments through a new SDK available on GitHub.

IBM points out that the inherent computational power of a quantum processor to solve practical problems depends on far more than just the number of qubits. Due to the fragile nature of quantum information, it says increasing computational power requires advances in the quality of the qubits, how the qubits talk to each other, and minimising the quantum errors that can occur.

As a result, IBM has adopted a new metric to characterise the computational power of quantum systems which it calls "Quantum Volume". This accounts for the number and quality of qubits, circuit connectivity, and error rates of operations.

Over the next few years, IBM plans to continue to increase the Quantum Volume of future systems by improving all aspects of the processors, including incorporating 50 or more qubits. ■

iFusion and Interoute partner to deliver analytics at the edge

iFusion Analytics has teamed up with Interoute to deliver edge analytics.

The partnership will see iFusion's *Big Data as a Service (iBDaaS)* platform combine with Interoute's global network of interconnected 'Virtual Data Centres' (VDCs). It's claimed this will enable organisations to process data closer to the original source so that analytic insights can be delivered in minutes, rather than the hours it could take running a query using just a location-locked physical server.

"Many people still don't completely understand how big data works," says Mark Lewis, Interoute's EVP of communications and connectivity. "Previously, running queries against large databases would take hours depending on the volume of data being interrogated and the client's location."

Mark Lewis, Interoute's EVP of communications and connectivity, claims running queries against large databases can now take minutes rather than hours as before.

To provide businesses with immediate insights and information, big data will be processed at the edge of Interoute's network before being securely collected, verified and sent to a central system for archiving. The central iFusion analytics system will provide an umbrella view of all the regional inputs so big data analytics is still performed for the overall organisation.

Interoute says all data will be transferred using its low-latency, private network to protect the security and sovereignty of information. It says that if local regulations prohibit personal data from crossing national boundaries, then iFusion's local collector will anonymise the required data so that they can be rolled up safely and securely.

Interoute will also enable iFusion to run its infrastructure with a smaller team. Using Interoute's object storage and connectors, it's claimed big data applications can be cut down to a smaller size and pre-loaded as bespoke templates onto VDCs so that different types of analytics can be performed at local sites.

iFusion adds that the reach of Interoute's private cloud capability will allow it to deliver "unprecedented access to its disruptive, highly scalable analytics platform." Charlie McAlister, the firm's VP of sales and business development, says: "Our customers will be able to truly 'act local and think global' by quickly acting on data insights pertinent to the various levels of their organisation." ■

NetScout to provide network performance monitoring for Vodafone across Europe

NetScout will serve as the Vodafone Group's passive probing provider in Europe. Under a multi-year agreement announced in early May, the operator will use the *InfiniStreamNG* next-generation real-time information platform in 13 European countries in which it runs mobile networks.

US-based NetScout says *InfiniStreamNG* will provide Vodafone with a standardised, repeatable service assurance solution, and help it to analyse and enhance network performance, and improve the customer experience.

The platform is available in multiple form factors and deployment options, based on hardware, software and virtual appliances. NetScout claims the "revolutionary" architecture provides timely, accurate and highly relevant data to support service assurance, cyber security, and business intelligence, all on a single platform for both the enterprise and service provider marketplaces.

The vendor adds that this latest deal represents an important extension of its longstanding partnership with Vodafone in Europe. NetScout president and CEO Anil Singhal says: "Our robust technology delivers a pervasive troubleshooting and performance tool that Vodafone can use across all its deployed technology domains, as well as future systems, such as 5G." ■

NetScout offers various physical and virtual InfiniStreamNG models designed to cost-effectively monitor critical business services and network operations.

Nitrous and TfL launch unique government innovation plan

Nitrous is working with six startup firms and transport industry experts in a new innovation programme designed to reduce congestion, encourage public transport use, and lower pollution levels.

Developed by Tech City Ventures, Nitrous is an initiative that aims to enable the creators of new technologies to accelerate their engagement with the public sector.

Under this latest collaboration, Nitrous is working with Transport for London (TfL). By providing access to unique open data from government and industry, the programme is designed to help startups better support public sector innovation without the need for additional investment.

The programme will provide the startups with a range of masterclasses, one-to-one sessions and networking opportunities. These will provide business-critical market validation and procurement knowledge to help ensure successful future collaborations in the short and long term.

It's claimed a "significant" network of senior public sector and industry ambassadors – including C-level executives from Vodafone, IBM and Aston Martin – will gain first-hand access to new technologies while sharing their expertise to supercharge the young companies.

The six startups include: Alchera Technologies which has developed a machine learning platform that powers smart cities, intelligent infrastructure and transport systems; NumberEight which is developing AI software to contextualise the next generation of IoT and mobile devices; and TravelAi which crowdsources and analyses travel behaviour data to provide actionable insights for transport professionals, and tools to help improve customer experiences.

The others include Blubel, Faxi, and Pedals. ■

Lone workers in Nottingham now protected by ANT

The UrSOSButton connects to a user's smartphone via Bluetooth. Once pressed, it activates an app on the smartphone that in turn sends an alert back to the CCTV control room.

Automated communications specialist ANT Telecom is working with Nottingham City Homes (NCH) to roll out its lone worker solution to protect workers in remote locations. It is also providing staff with the *UrSOSButton* safety and monitoring device.

This latest deployment follows the successful installation of ANT's solution with Nottingham City Council's CCTV control room to ensure the safety of council workers.

NCH manages around 27,000 houses in the city. Its housing managers deal with anti-social behaviour, harassment and neighbour disputes, and also take part in estate inspections.

The managers will be equipped with the *UrSOSButton* which offers "simple to use" functionality, according to ANT. Pressing the button activates an app on the user's smartphone that in turn sends an alarm message back to the CCTV control room. The message contains details about who raised the alert and their GPS coordinates.

The app also initiates a phone call opening the smartphone's handsfree mic and enabling operators to eavesdrop and pick up important information at the scene so they can decide the best course of action. They can also utilise any CCTV camera they have in the area.

ANT adds that the device has low running costs as well as a very long battery life – it claims a single charge of 45 minutes could last many months and even a year or more, depending on how often the button is used.

Currently, 300 workers are already using the *UrSOSButton*, and a further 250 are expected to have it once roll out has been completed. ■

Openreach to consult on future investment in digital infrastructure

Openreach will consult with its communications provider (CP) customers on how best to enhance broadband connectivity across Britain.

The company, which provides broadband infrastructure to more than 580 CPs, will seek input on two major policy issues: building the investment case for a large-scale 'full fibre' network; and bringing faster speeds to 'not-spots' which can currently only order less than 10Mbps services.

Chief executive Clive Selley says Openreach is committed to investing in infrastructure but wants to work closely with communications providers to explore how it should proceed.

Openreach has already stated its ambition to make ultrafast speeds of more than 100Mbps available to 12 million homes and businesses by the end of 2020. However, the firm says it is keen to explore conditions which might allow it to invest in more full fibre infrastructure.

The consultation will look at the demand for FTTP, the potential benefits and costs of its larger scale deployment, and the enablers needed to support investment. Openreach is currently in a scoping phase and anticipates launching a formal consultation in the summer.

The firm has also launched a consultation with CPs on the next steps for Long Reach VDSL. Openreach claims this emerging broadband technology has been proven to increase broadband speeds over long phone lines connected to its fibre cabinets.

"Every communications provider in Britain can already access our national network on equal terms and conditions," says chief executive Clive Selley. "I'm convinced that providing a mechanism to explore investment opportunities confidentially will lead to stronger relationships and more teamwork in addressing the major challenges we face as an industry." ■

Datto helps keep bus firm running despite ransomware threat

Reading Buses was being repeatedly targeted with ransomware, and downtime was becoming a regular occurrence.

Reading Buses is using Datto's data protection and business continuity solutions after being hit by ransomware.

With more than 150 buses and 400 drivers serving the Reading area, the transport company needed a solution that could protect all of its data – including vehicle maintenance and payroll – from unforeseen events. After seeking advice from its managed service provider, Complete I.T., Reading Buses' data are now stored and backed up both on-site and in Datto's private cloud at regular intervals, and is available to be restored at a moment's notice.

The solution was called into action almost immediately on deployment when Reading Buses was able to quickly restore systems following a ransomware attack. Arriving as an email attachment, the 'Locky' virus quickly encrypted an unsuspecting staff member's computer, as well as many shared locations across the business that the users had access to.

Previously, Reading Buses would have suffered significant downtime due to the attack. But with Datto's systems in palce, the company was able to locate the infected files, remove them, and restore all relevant information from the backup. The company was operational again within minutes, and no ransom was paid.

"Providing a first class service is paramount, but downtime was becoming a more regular occurrence," said Mark Price, IT manager at Reading Buses. "We were repeatedly targeted with ransomware but we couldn't simply disregard emails from unknown senders, as we receive many enquiries each day from passengers," says Mark Price, IT manager at Reading Buses. "We needed a solution that would work in the background and enable us to restore systems quickly, ensuring our customers weren't affected, we didn't lose revenue, and our reputation was safe." ■

EDITORIAL:

Editorial director: Rahiel Nasir
rahieln@kadiumpublishing.com

Designer: Alan McClenaghan
alanm@kadiumpublishing.com

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

KADIUM

Kohler acquires Pure Power Systems

Kohler Co. has acquired Dublin-based independent UPS distributor and service provider Pure Power Systems. Following finalisation of the deal, Pure Power will become part of Kohler's UK-based firm, Uninterruptible Power Supplies Ltd (UPSL). However, it will continue to be lead and managed by its owner and founder Ian Jackson along with all its other current employees. "We've partnered with Pure Power for nearly a decade, so we're very familiar with the company's deep technical expertise," says UPSL MD David Renton. "This acquisition will allow us to give our data centre and other power protection customers throughout Ireland and the UK access to an enhanced offering of UPS products and support services." ■

London Metal Exchange expands at Interxion

The London Metal Exchange has expanded its footprint at Interxion's London data centre campus with its newly upgraded trading platform for base metals, *LMEselect*. It will also list its new *LMEprecious* products on the platform when they launch in July (subject to regulatory approval). "Interxion provides the ideal environment for our new *LMEselect* platform, with best in class power and cooling and excellent cross connect access to the exchange," says London Metal Exchange CTO John Lee. ■

Nutanix certifies APC for hyperconvergence

Nutanix has certified APC's *PowerChute Network Shutdown v4.2* power protection software for use with its *ESXi* and *Hyper-V* hyperconverged infrastructure deployments. APC says the validation eliminates the onus of responsibility on channel partners for determining the compatibility and integration of components in a multi-vendor hyperconverged system. The two firms say their alliance "delivers on the promise of hyperconvergence through a cohesive, total solution that simplifies typical IT commissioning and management". APC also claims *PowerChute* ensures a level of IT protection not previously available, providing customers with the certainty that their investment and data will be secure during an outage. ■

Neonatal unit introduces secure video messaging

Nurses can capture special moments in the baby's care diary that can then be securely accessed by the parents on any device.

The Royal Hospital for Children in Glasgow (RHCG) is now offering secure video messaging to help parents of premature babies stay connected with their child's progress during their hospital stays.

The hospital's neonatal unit (NNU) has been trialling a bespoke platform developed for the NHS by Leeds-based video technology specialist, vCreate. The personalised video initiative, thought to be the first of its kind in the UK, allows nurses at the hospital to use any device with a camera to record short video updates that can then be securely accessed by parents on any device.

vCreate says the service is managed and controlled by NNU staff at all times. Videos are stored securely on its platform with parents registering for an account. Once approved by the staff, videos are assigned to the appropriate parent account which is deleted following their baby leaving the unit.

As well as enabling parents to receive reassuring updates on their baby's well-being when away from the unit, vCreate says the service means NNU staff spend less time answering queries over phone and more time caring for children. It adds that they only record videos when they have time, the process has no impact on their clinical duties, and the videos do not contain any sensitive medical information.

The RHCG now plans to make vCreate available to consenting parents of the 600 babies it cares for each year. It is also considering extending use of the system to share more general news updates with parents.

vCreate says its aim is to bring secure video messaging to all 200 NHS neonatal units by 2018. It has launched a public appeal for corporate sponsorship to make it happen at no cost to the NHS. ■

BSI updates specs for data protection standard

BSI (British Standards Institution) has updated its specifications for data protection. The business standards company developed *BS 10012:2017* to provide best practice guidance for leaders responsible for the management of personal information systems

The revised *BS 10012:2017* standard specifies requirements for an organisation to adopt a personal information management system (PIMS). It says this provides a framework for maintaining and improving compliance with data protection requirements. The standard is also intended to provide clear guidance for internal and external assessors on assessing compliance with data protection requirements. It is applicable to organisations of all sizes and sectors.

Changes from the 2009 version of *BS 10012* include a new definition of personal and sensitive data; restrictions on profiling using personal data; and new administrative requirements for data privacy officers.

Data written under a pseudonym is now specifically covered, and there are stricter requirements for consent for processing. The revised standard also takes into account a change in the law to cover data processors.

Many of the changes in the latest version have been written in recognition of the EU General Data Protection Regulation (GDPR) which became law in April 2016. The GDPR will be directly applicable to the UK and EU member states on 25 May 2018.

"BS 10012 will provide organisations with structured guidance on implementing a common sense strategy to handle personal information as securely as possible." says Anne Hayes, head of governance and resilience, BSI. "It will also provide confidence to employees at all levels of an organisation that decision-makers take the hot-button issue of data security seriously." ■

University gains network visibility with Nexthink

The University of Derby (UoD) has selected Nexthink to improve the visibility of its IT environment.

UoD gained university status in 1992 and now serves more than 30,000 students via its sites in Derby, Buxton and online. It has invested more than £100m over the past five years in its technology infrastructure. As well as claiming to offer "first-class" campus facilities", they also enable students to participate in programmes that are provided entirely online or via blended learning.

The university has around 5,000 endpoints, which include user workstations and 1,500-2,000 mobile devices, spread across three primary sites and six satellite locations. With enrolment increasing each year, it has a pressing need to efficiently support students and faculties by quickly accessing relevant contextual endpoint and end-user data.

UoD hopes that by understanding the end-user experience it will be able to provide a superior IT service to its student community.

Nexthink says its end-user experience management system proactively monitors UoD's entire IT infrastructure and reports on important end-user related events, such as performance issues, failures, crashes and security issues. The company says its real-time and historical record of the usage and performance of services will provide unique visualisations and actionable insights to the university's IT team so that they can enhance the services provided to users.

The deployment was carried out in partnership with student technology specialist Software2. ■

OpenLink claims first with financial cloud platform

OpenLink reckons it's come up with the world's first and most comprehensive enterprise cloud platform for trading, treasury and risk management.

US-headquartered OpenLink offers trading, treasury and risk management solutions for the commodity, energy, corporate and financial services industries.

The company claims its new *OpenLink Cloud* delivers the "highest" standards of security for highly regulated, data-intensive organisations. The platform combines what's said to be the "strength and security" of *Microsoft Azure* with best-of-breed OpenLink security and tools to ensure that clients' mission-critical systems and data are protected at all times.

Developed in collaboration with more than 50 of its largest and most sophisticated energy and financial services clients, OpenLink says its cloud system has been "rigorously" tested.

It adds that *OpenLink Cloud* is supported by a robust set of custom tools and services, and is designed to help clients of all sizes get up and running quickly and to simplify management, monitoring and support of both production and non-production environments.

OpenLink's Scott Rompala reckons the platform is enabling clients to "re-imagine" their business.

OpenLink continues by claiming customers will have immediate access to "almost limitless" computing power with the introduction of the platform's dynamic scaling capabilities. It boasts that these provide "advanced data management and richer analytics that enable greater market understanding, speed and evidence-based decision-making".

Scott Rompala, head of OpenLink's cloud solutions group, says: "The real untapped benefit our clients are sharing is how this new flexibility and efficiency will allow them to re-imagine their business, take advantage of intra-day volatility in the markets, and provide accurate and real-time views of their risk and exposures to management and the board on demand." ■

Red Hat releases latest version of OpenStack Infrastructure-as-a-Service

Red Hat has announced the latest version of its "massively-scalable" Infrastructure-as-a-Service (IaaS). The open source specialist says OpenStack *Platform 11* delivers enhanced support for upgrades with composable roles, new networking capabilities, and improved integration with *CloudForms*, Red Hat's cloud management platform.

Based on the OpenStack *Ocata* software release, it's claimed the new version delivers a reliable cloud platform built on the proven, enterprise-grade backbone of Red Hat Enterprise Linux. The company reckons that it provides the agility to scale and more quickly meet customer demand without compromising availability, performance or IT security requirements.

The introduction of composable roles allows operators to create customised profiles for individual services and processes to suit their unique needs. Red Hat says this helps to improve operation and efficiency by allowing operators to scale and manage the individual services they need at any moment, rather than scaling the entire cloud.

The firm says OpenStack services can now also be composed individually and assigned, enabling operators to place components such as databases, proxies, or messaging services on specific nodes based on their unique requirements. This includes adding customised roles post-deployment to a running cloud, providing more flexibility to customers or partners as they become more successful with their cloud services.

Red Hat adds that the inclusion of *CloudForms* serves as a hybrid cloud management and monitoring platform It says this not only oversees OpenStack infrastructure components, but also the workloads running on a given OpenStack cloud.

Other features include expanded networking and NFV support. For instance, OpenStack-based VMs can now send and receive VLAN encapsulated traffic while being deployed over Open vSwitch or the OVS *Data Plane Development Kit*. ■

Druva expands global footprint in UK to align with Brexit

Druva says it has significantly expanded the reach of its public cloud offerings to better support its customers' national and regional data protection requirements.

The cloud data protection and information management specialist claims the move will enable companies to host their data in locations that best meet their specific requirements around data residency, location and transfer.

Support for the UK will be available later this year during the third quarter. Druva believes that with Brexit as well as the General Data Protection Regulation (GDPR), the UK data centre will be critical for meeting data sovereignty regulations.

"The new expansion will provide our customers with a simple and effective way to manage their data within the region, whatever changes take place after Brexit," says Rick Powles, VP EMEA, Druva.

He adds that while the Information Commissioner's Office has already indicated that it will follow the rules of the EU's GDPR, the new public cloud location will help customers align to the UK's specific data sovereignty requirements.

Druva has also announced public cloud options in two other locations.

In Canada, the company says it will enable private sector customers to manage data in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA). This federal privacy law sets guidelines on how and where Canadian citizen data is stored.

Meanwhile in Asia, Druva's new Hong Kong location aims to give customers the ability to meet the region's varying local data protection guidelines while taking advantage of the cost savings delivered by the public cloud. ■

SUSE aims to simplify and manage OpenStack deployments

SUSE has unveiled OpenStack *Cloud Monitoring*, an open source software solution designed to make it simple to monitor and manage the health and performance of enterprise OpenStack cloud environments and workloads.

Based on the OpenStack *Monasca* project, SUSE says its software makes it easy for operators and users to monitor and analyse the health and performance of complex private clouds. It claims *Cloud Monitoring* delivers reliability, performance and high service levels for OpenStack clouds, and reduces costs by simplifying, automating and pre-configuring cloud monitoring and management.

"OpenStack deployments produce a lot of complex and useful monitoring and log data," says Michael Miller, SUSE president of strategy, alliances and marketing. "As customers move to large-scale production they need operational tools to maintain their private cloud."

Miller says the *Monasca* open source project makes these data manageable and valuable for enterprise users. *Monasca* is an open-source multi-tenant, highly scalable, performant, fault-tolerant monitoring-as-a-service solution that integrates with OpenStack. It is said to use a REST API for high-speed metrics processing and querying, and has a streaming alarm engine and notification engine.

It's claimed SUSE Cloud Monitoring reduces costs by simplifying, automating and pre-configuring cloud monitoring and management.

SUSE says it worked closely with Fujitsu and other contributors to bring *Monasca*'s capabilities to its *Cloud Monitoring* platform. It is said to include a single "powerful" dashboard to manage, track, monitor and optimise complex distributed OpenStack private cloud environments.

The platform is also said to feature the ability to identify problems early with complex processing of OpenStack events, logs and metrics, advanced graphical search, and analysis of historical data using the powerful dashboard.

SUSE adds that the fully open source solution reduces costs and increases flexibility by avoiding the risk of vendor lock-in often associated with proprietary solutions. ■

The power to deliver

How datacomms networks are helping energy companies to keep the juice flowing.

ENW claws back on upgrade costs with Wolverine

Electricity North West (ENW) connects more than five million people to the National Grid via a distribution network that covers a diverse range of terrain, from isolated farms in rural Cumbria, to areas of heavy industry and urban populations such as Manchester.

As part of its aim to maximise supply quality and minimise lost minutes, the company monitors and controls its 500 primary substations via a central SCADA system connected to a data comms network. RTUs (remote terminal units) installed at the substations transmit voltages, current, switch states, transformer temperatures and alarm data from connected sensors and equipment.

But the existing data network was based on copper cabling and a very large VF serial-based solution which offered limited bandwidth (only 1200 baud), no redundancy, and insufficient resilience. ENW decided to upgrade to an Ethernet IP-based solution but was concerned that vast new fibre infrastructure would be required to support this. With around 11,000km of installed cabling potentially needing to be replaced, the size, complexity, time and cost of the project was extremely prohibitive. It was therefore essential to find a solution that could use the existing cable infrastructure wherever possible.

The answer came from Westermo and its *Wolverine* Ethernet line extenders. The company says these allow effective Ethernet networks to be created over distances of up to 15km (depending on cable characteristics), whilst enabling data rates up to 15.3Mbps. Crucially for ENW, the SHDSL technology the devices are based upon makes it possible to re-use many types of pre-existing copper cables. This meant that ENW could upgrade without replacing its vast cable infrastructure.

The line extenders have now been installed throughout the network, with around 750 being used to connect the RTUs at the primary substations. Using Westermo's *WeConfig* software tool, ENW's IT and telephony networking team are able to configure and monitor the line extenders remotely.

The vendor says ENW's DIN-rail mounting and 48V power supply requirements, typically found in the existing housing cabinets at the substations, meant that the line extenders integrated "very easily" with the existing setup.

Robin Hood establishes contact with BT

Operated on a not-for-profit basis as a wholly-owned subsidiary of Nottingham City Council, Robin Hood Energy's (RHE) mission is to provide low-cost electricity and gas to households and businesses in the East Midlands and beyond.

The company launched in September 2015 after being set up from scratch with limited resources in a vacant city centre council office. Nearly all the fledgling's business would be conducted over the phone or internet, and so it needed technology guidance that would power its business.

A contact centre would form the heart of the new company. It had to be quick to implement with the scalability to meet demand as business grew. But capital funding secured to launch the firm meant constraints on operating expenditure. It was therefore decided that a fixed-cost solution would be preferable to variable cost cloud-based technology.

"In those early days, we had little in-house technical expertise," recalls Robert Purdon, contracts manager, RHE. "We called on BT as a long-term service provider to the council to help us."

Three contact centre suppliers were considered before BT was chosen and recommended an on-premise *Enghouse Interactive Communications Centre (EICC)* as the preferred option.

BT also provided *Cisco Unified Communications Manager* as recommended by the council's IT team, and ISDN 30 lines for both the contact centre and back office functions.

EICC is deployed across two Nottingham City Council data centres in a fully-redundant configuration. Initially set up to support 12 agents, the platform quickly grew to 50 positions. It's expected to have more than 200 agents as it offers its services to other local authorities on a white label basis.

Enghouse Interactive also supplied professional services to integrate EICC with a specialist utility-company CRM system. That means contact centre agents get a screen pop-up with customer information when a call comes in. If it's a new customer, the agent can type their details straight to screen, and these are then automatically fed to the back office system without any re-keying.

Other features include a customer self-service meter reading app, and suppressing call recording when customers quote financial data in order to meet PCI DSS regulations. Potential enhancements being considered include customer post-call quality surveys, and call-back requests at busy times.

Fibre testing a breeze at North Sea wind farm

Off-shore wind farms provide an attractive location option for generating power, especially in the stormy North Seas off the UK's east coast. But they are also complex and challenging for construction and cabling installation projects. Weather and high voltage carry significant risk factors and contractors need to be wary when working on such projects.

One example here is provided by Twistnet Communications which worked with a North Sea wind farm that has not been named. Established in 2000, Nottinghamshire-based Twistnet specialises in the installation, testing and certification of fibre optic, structured, and voice cabling systems.

It was called to provide testing and certification services that required a technician to bidirectionally test links inside a high voltage electrical substation where all the communication and electrical cabling come together from the wind turbines in an onshore facility.

Given the fact that the average capacity for wind turbine projects is between 150MW and 500MW, the risks for onsite technicians are significant. A full health and safety induction was required for a Twistnet technician to test inside the electrical substation, and the cost for such certification can rise above £500 per person.

On the wind farm project, Twistnet was required to test upwards of 400 fibre links bi-directionally. The standard way to do this was to test it from one end, and then walk the OTDR tester to the other end. For this particular job, a technician would need to do that at least 800 times, which would prove time intensive and costly. On top of this, a day would be needed to complete the induction, thus adding to the time commitment.

But by using what it described as "innovative" new technology from Fluke Networks, Twistnet said it was able to simplify how its technicians work, and help improve safety while reducing costs.

It deployed Fluke's *OptiFiber Pro* with *SmartLoop* technology. This enables the testing of two fibres in a single test, eliminating the need to travel to the far end of the connection. According to the manufacturer, this patent pending process automatically separates the two fibres for individual pass/fail analysis, display, and reporting.

Using the device meant Twistnet was able to borrow a wind farm technician who could take the place of one of its team inside the substation. The wind farm technician was given quick training on installing a patch lead. Twistnet also shared what would be required to test each link bi-directionally. Communicating using two-way radios, its team guided the wind farm technician to work his way through moving a patch lead and testing each link.

Almost every successful hack begins with a vulnerability and then moves onto exploiting excessive privileges. So is it enough just to plug the gap? If only network security was that simple…

Network lockdown

In the face of rising and seemingly advanced cyber attacks, how can you keep your precious data safe? RAHIEL NASIR finds out how to put the hackers on the back foot.

The infosec community is still sifting through the evidence following the massive ransomware attack that started to hit hundreds of organisations around the world on 12 May. At the time of writing, it was still not known whether the *Wannacry* virus (also known as *WCry*, *WanaCryptor*, *WannaCrypt* or *Wana Decryptor*) was state-sponsored, orchestrated by a hacker group, or the work of a lone teenager sitting in a suburban bedroom somewhere.

So should network and data security breaches now be accepted as an everyday part of digital life where enterprises can do little to protect themselves?

"If you rewind a couple of years in IT, there was a mindset of working frantically to put procedures and solutions in place to prevent cyber security breaches," says Ajay Uggirala, director at Imperva. "Now, there is a trend building toward a tendency for people to accept that they're going to be breached with the focus shifting to how they minimise the impact of a breach. This is not the answer."

Steve Armstrong, CyberCPR Architect and principal consultant at Logically Secure, agrees: "The media are regularly reporting how large companies such as TalkTalk and Yahoo, for example, were breached by hackers. The message that many people take from this is that attackers can easily beat big companies who have invested in security.

"Conversely, look at how Hollywood portrays hackers and security experts as being able to defeat firewalls and anti-virus software in seconds. The takeaway here is that these protections are easy to defeat and that attackers can always better your security.

"So then we wonder why users are apathetic towards security. We tell users to have long complex passwords and to change them regularly. But deep down they think 'why bother? Who will this stop? What have I got to lose that hasn't been lost already?' (As a side note, both NIST and NCSC now actually recommend users DON'T time expire passwords)."

In Armstrong's view, users generally accept breaches do and will happen, either because they think an attacker is better than the company's security or because they have heard of some new exploit that no one knew about until today. "In fact, in explaining how they got breached, many a CEO will use the phrase 'advanced attacker' or 'APT' – it's their way of saying we couldn't stop it and customers accept this, even though it's usually a lie."

"We tell users to have long complex passwords and to change them regularly. But deep down they think 'why bother? Who will this stop? What have I got to lose that hasn't been lost already?'"

Steve Armstrong, Principal consultant, Logically Secure

While few would disagree that we will ever be completely secure from breaches (at least for the foreseeable future) it would be wrong to assume that there's nothing worthwhile organisations can do to maximise their defences.

For instance, Brian Chappell, senior director, enterprise and solutions architecture at BeyondTrust, believes accepting the inevitability of a breach is actually the first step toward limiting its scope. He says breaches should always be a fundamental consideration when building and expanding security solutions but adds that protection is only part of the solution. "We need to ensure that the impact of a breach (via a previously unknown vector) is also limited within the solution and that we have the ability to detect when this has happened. This is a natural outcome from good security practice but it still needs to be a focus to ensure we can be confident it's covered.

Encode Group MD Graham Mann supports this view. He says organisations and individuals have to recognise breaches as a part of normal life and become more informed. "Organisations can't simply continue to harvest data without understanding what's really needed, how long they need to keep it, how secure should it be, who should have access. Data has to be treated like any other physical asset and boards need to recognise this and take the lead. You wouldn't leave your office, plant or factory open to intruders so why leave your data exposed?”

Arms race

Why indeed. But with the cyber criminals seeming to grow ever more sophisticated, are enterprise IT security platforms only ever going to be ‘best effort’ solutions? Ian Parker, professional services consultant for Axians UK, is very decisive here. “It is a very simple answer: no. If the IT department or third party is implementing the device/platforms/service/solution, and they understand what the vulnerabilities could be, then there is no excuse if the systems are compromised. This is an arms race and has been ever since the internet was born. It is nothing new. And when cyber criminals have worked out a way to exploit a vulnerability, a manufacturer fixes that vulnerability. So begins the cycle and it will continue until we are long gone.”

Once again, this seems to imply a certain degree of futility. In some way, it seems rather like the little Dutch boy in the children's story who uses his finger to plug a hole in the dyke only for another leak to spring elsewhere. After all, and as McAfee's director of government relations Gordon Morrison points out, organisations have added layer after layer of defence to stay ahead of the latest attacks and should therefore be better protected now than ever before. Or at least that's the theory. Instead, security teams are drowning in tools and interfaces. Citing Forrester's Mastering the Endpoint report published earlier this year, Morrison says organisations now monitor, on average, 10 different security agents and switch between at least five different interfaces to investigate and remediate incidents.

Stephen Coty, chief cyber security evangelist at Alert Logic, adds to this by saying that most technologies that are used as part of a corporate security strategy are capable of catching even the most sophisticated hacker. But the problem is not with the technology – it's with the implementation. As a result, he says making sure that you're using the right tool for the right job and that the technologies are deployed in the most efficient way in the organisation's architecture are all crucial.

“To make the technology you have as effective as possible, you have to ensure that the security content and correlation logic are constantly being updated to match the ever evolving threat landscape. Also, you need to make sure that the security content is on the technologies that you actually utilise, and that it does not have unnecessary signatures or rules using up resources that can be allocated to more efficiently protect your environment.”

“Using a single supplier for security is no longer the answer. The cyber security tendering system is broken and needs to be replaced urgently.”

Graham Mann,
MD,
Encode Group

Imperva's Uggirala also points out that while the cyber attacks are becoming more sophisticated, so too are the solutions to protect against them. For example, he says more machine learning technology is becoming incorporated into cyber security and this will help IT teams with manual tasks such as sifting through alerts, deploying patches and permissions management.

But ultimately, there's no such thing as 100 per cent security, and for Mann it's always been about ‘best efforts’. Having said that, he believes that all too often organisations aren't deploying best efforts. Far from it.

“There are loads of new solutions flooding onto the market from innovative startups. The issue is few people know about them and even less are willing to purchase them. If we are to have any chance of defending ourselves against cyber attacks, we have to implement innovative solutions from wherever we can. Using a single supplier for security is no longer the answer. The cyber security tendering system is broken and needs to be replaced urgently.”

Chappell agrees that we are not doing the basics well. He says almost every successful hack starts with a vulnerability and then moves on to exploiting excessive privileges. More worryingly, he says the Verizon Data Breach Investigations Report regularly shows that “ancient” (in IT terms) vulnerabilities still exist and are still being used.

“BeyondTrust investigations have shown that only a small percentage of discovered vulnerabilities are ever used in attacks (less than five per cent on average). That's almost certainly due to the widespread use of attack toolkits which have a defined collection of exploits, and it's unlikely to change significantly in the increasingly commoditised world of cyber crime.”

The human factor

Despite what seems to be a never-ending tale of doom and gloom, businesses are not helpless in the face of such threats.

Axians recommendation is to look at the existing network, ensure that the design is future focused, and consider the type of services customers will be demanding over the next 3-5 years. "It's essential to factor security in from the very beginning and not just throw money at firewalls," says Parker. "Security can be seen as an onion; it requires many layers to be secure, not just a perimeter firewall. More visibility is needed from a security perspective as the world is now run by applications rather than online services. So application visibility with UTM functionality is almost a basic requirement."

David Emm, principal security researcher at Kaspersky Lab, advises enterprises to establish a baseline of "normal behaviour" in regards to network traffic, access and operations: "Knowing what's normal will give visibility to irregular behaviour or anomalies. A business must look for patterns or trends in unusual behaviour, and security teams must be constantly prepared for the unknown. No one thing is going to protect your organisation – the key to success in identifying breaches is not so much the tools used but the processes and policies which are in place."

In addition, Emm speaks for many when he says that to avoid attacks and mitigate any that breach the outer defences, companies should follow strict security policies. These include internet protection, applying security updates as soon as they become available, restrictions to prevent users running unknown applications and, perhaps most importantly, employee education. "After all, if staff are aware of the dangers, they can work individually and together to protect data and may have a better chance of detecting any abnormal activity on the corporate network as it happens."

When it comes to network and data security, the human factor comes up time and again. For instance, Chappell says that once the IT team has first tackled the vulnerabilities with known exploits and established control of privileged accounts, all other employees should be made standard users with a single account giving them appropriate access. "The tools are there to do this and it's not difficult. As our studies have shown, over 80 per cent of the known vulnerabilities in *Windows 7* are effectively mitigated by removing admin privileges from users. It's basic activities like these that will help make cyber crime less lucrative as access to rich data will be ever harder to gain."

Some experts say executive boards have to become savvier and ditch their appetite for risk, to a certain extent.

What becomes clear at this stage is that building an environment that safeguards an organisations' digital assets in an appropriate manner isn't just about network security. As Encode's Mann says, that's only part of the solution. "Boards have to become savvier and to a certain extent ditch the risk appetite. Organisations have to think smart and develop a strategy that extends into every aspect of their operation. Yes, that includes IT, but it also includes physical security, business unit managers, HR, legal, marketing, operations, sales, etc. All have a part to play."

All that becomes even more significant when you consider Parker's view that the most successful cyber attacks are directed at staff in non-technical departments (i.e. finance, HR, sales, etc.) by relying on their lack of IT knowledge and understanding of the potential dangers around clicking on an attachment in an email, for example.

"Very few intelligent attackers take on the IT professionals in an organisation by trying to compromise the network at the front door of their network," he says. "The IT professionals do this day in day out, and are often more knowledgeable than the attackers, so they would have protected the internal network from traffic sourced from the outside world. But then the cyber criminals can very easily piggyback on traffic that can simply pass through their security barriers and attack from the inside where it is a trusted environment."

With most attacks entering the network via the back door opened by an unsuspecting and naïve employee, Parker says the end users are the ones who need to be trained and made aware of what is a legitimate email and what should be reported to IT. He believes this would reduce exploitations considerably.

Thus, the human is still the most vulnerable part of a security strategy and, according to ANSecurity, the weakest link in any IT network are its users. "User error is often where the mistake has been made" says the company's technical director David Peters. "That's why solutions such as endpoint and email security are good systems to have in place to try and minimise the opportunity for users to open that malicious attachment or click on that malicious link from phishing emails that are becoming more sophisticated."

While all that sounds simple enough, educating staff will remain difficult until cyber security is seen as an important part of the business fabric. Until then, Chappell says organisations will just regard security as "noise" and largely ignore it unless it's impacting their ability to do their jobs.

Gareth Niblett, chairman of the BCS Information Security Specialist Group, agrees. He says employers and organisations in general are not doing enough to educate their staff as cyber is still thought of as an IT or security issue. "It's not easy, but a lot of things can be addressed through culture and support from the top of the business. Get the basics right and you will stop most attacks. Going beyond the basics should then be prioritised based on risk rather than latest cool security technology.

"A security lifecycle that covers in-depth defence, detection, response and recovery, combined with a strong focus on policy, people, and technology are the best ways to defend an organisation. Tools should follow, not lead."

Know your onions

So assuming the different parts of an organisation that have been traditionally siloed are all working more closely together, and cyber security is placed front and centre as a core business function, what next?

For Niblett, it's about understanding what assets you have that need to be protected – and this includes people, processes and services, not just boxes and wires. "Without knowing what you're protecting it will be impossible to determine the best way how. This should include (as far as possible) known unknowns, such as shadow IT, cloud/SaaS, BYOD, which may introduce additional exposures."

Many infosec specialists believe effective cyber security is about creating simple layers which result in a whole that is greater than the sum of its parts. Each

We will fight them on the breaches – right?

Large numbers of businesses overestimate their readiness to combat cyber security breaches, according to research by SolarWinds MSP.

Earlier this month, the IT management solutions specialist released the findings of a study that surveyed 400 enterprises split equally across the UK and US. It found that businesses are "gravely optimistic" about their ability to deter and cope with malicious attacks, despite the majority experiencing a breach over the last year and nearly a quarter experiencing more than 10.

The research revealed that 87 per cent of IT executives questioned are confident in their security technology and processes' resilience, and that 59 per cent believe they are less vulnerable than they were 12 months ago. Another 61 per cent are anticipating a substantial boost to their cyber security budgets and are therefore confident this position will improve.

However, 71 per cent of the same respondents said they had experienced a breach in the last 12 months. SolarWinds says these breaches are significant and shouldn't be discounted. Of the businesses that had been attacked and could identify a tangible effect, 77 per cent said they had suffered a loss, such as monetary impact, operational downtime, legal actions, or the loss of a customer or partner.

According to SolarWinds general manager John Pagliuca, one of the main reasons IT leaders feel so prepared yet still feel exposed is because people are confusing IT security with cyber security. "The former is what companies are talking about when they think about readiness. However, what they often don't realise is that cyber protection requires a multi-pronged, layered approach that involves prevention, protection, detection, remediation, and the ability to restore data and systems quickly and efficiently."

After investigating why this overconfidence is occurring, SolarWinds has identified seven basic faults:

- Inconsistency in enforcing security policies
- Negligence in the approach to user security awareness training
- Shortsightedness in the application of cyber security technologies
- Complacency around vulnerability reporting
- Inflexibility in adapting processes and approach after a breach
- Stagnation in the application of key prevention techniques
- Lethargy around detection and response

Citing IBM and Ponemon's 2016 *Cost of Data Breach Study: Global Analysis* report, SolarWinds says the cost per stolen record data is £59,000 for SMEs (fewer than 250 employees) and £724,000 for larger enterprises. It says this potential commercial impact together combined with the lack of preparedness and frequency of cyber attacks heightens the risk of an 'extinction event', i.e., a massive business failure correlating to the breach.

layer should be easy to design, easy to manage and easy to monitor. And just like physical security, this layered approach also gives more opportunity for detection of abnormal activity.

Chappell says the first key solutions using such an approach would be effective vulnerability management systems (VMS) and privileged password management (PPM).

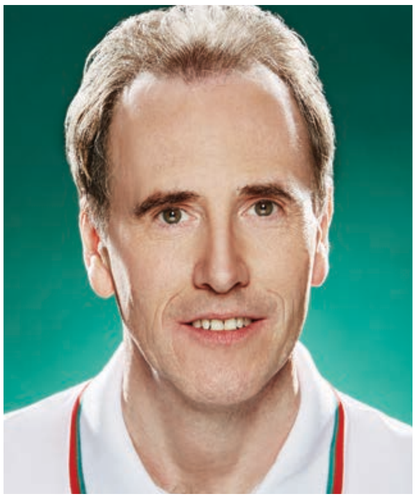
“The VMS should help target the vulnerabilities with known exploits first and foremost, those are the low hanging fruit and the most likely points of entry into your systems. Regular scanning and remediation are essential along with effective reporting that demonstrates progress, otherwise you find yourself in the ‘nothing happened’ scenario where it’s hard to show where the cyber security budget is delivering benefit.”

He continues by saying PPM enables control of shared privileged accounts and actively manages their passwords, eliminating the need for users to know the password. This also means the passwords can be of maximum length and maximum complexity, preventing brute-force and rainbow-table attacks. Furthermore, PPM ensures that any cached password hashes are out of date almost as soon as they are created.

“Starting with these two layers will lay a solid cyber security foundation on which to build the next layers, like ‘Super User Privilege Management’ (also known as ‘Least Privilege’) so we can eliminate direct privileged account use completely. Effective reporting capabilities at each layer is essential as is an overarching SIEM to bring the picture together with inter-related events producing clearer signals for actionable alerts.”

Kaspersky’s Emm is likely to agree here. He points out that it would be unwise for any organisation to assume that perimeter defence alone is sufficient to block attacks.

“What’s required is a defence in-depth approach that includes protection at all layers. It should also include effective network management (not routinely giving employees admin rights to their computers, segmenting the network to limit the impact of a breach, etc.) as well as anti-malware and other technologies. Security is no longer about protecting corporate endpoints, networks and traffic with a robust solution – it’s about a deep, multi-layered, tailored and continuous approach.”



“The key to success in identifying breaches is not so much the tools used use but the processes and policies which are in place.”

David Emm,
Principal security researcher,
Kaspersky Lab

The end game

As businesses change their IT infrastructure, the security requirements to secure that infrastructure also changes. And as Imperva’s Uggirala highlights, enterprises with a good security strategy will make cyber criminals life harder and make them look somewhere else to achieve their agenda.

But industry experts such as Axians warn that the biggest vulnerability to cybercrime is not applications, software or the devices we use to access the information super highway, it is the people using them.

Furthermore, as Thomas Seidling at Cybersmart points out, while progress and open sourcing of advanced tools mean attacks will become increasingly advanced, most of today’s breaches are actually not that sophisticated because they don’t need to be.

“BeyondTrust investigations have shown that only a small percentage of discovered vulnerabilities are ever used in attacks.”

Brian Chappell,
Senior director, enterprise & solutions architecture,
BeyondTrustt

“In the majority of cases, attacks are successful because of systems not being patched (such as the recent NHS *Wannacry* attacks, for example), or people not having received relevant training. If all companies today implement basic cyber security, such as the government’s Cyber Essentials scheme, over 80 per cent of cyber attacks would be stopped overnight.” ■

LET’S GET TO WORK ON
NETGEAR®
Resilient networking with the NETGEAR ProSAFE® M4300 Intelligent Edge Series
Cost-effective Stackable Switches with Full PoE+ Provisioning. The world’s first 1G and 10G virtual chassis platform with 10G stacking designed for mid-enterprise edge and SMB core deployments.
To find out more contact us on 0800 038 8880 or salesdesk@misco.co.uk
LIFETIME WARRANTY Hardware Warranty
LIFETIME WARRANTY Next Business Day
LIFETIME Tech Support
www.misco.co.uk
MISCO

off-the-shelf: switches

Switchcraft

Managed or unmanaged, the latest switches need the technology to support today's bandwidth hungry high-capacity networks.

Belden has released what it says is a compact yet ruggedised switch for large-scale industrial networks.

With 28 Gigabit speed ports, the full GbE Layer 3 *MSP40* is claimed to feature more interfaces than other modular compact switch on the market. Belden says these interchangeable ports enable data speeds up to 2.5Gb, but adds that with 10Gb speeds "right around the corner" the modular design of its switch means users won't need to purchase new hardware in order to adapt.

The *MSP40* is housed in high-grade metal/aluminium casing that can be mounted on DIN rails. Belden says it has been designed to operate in harsh, space-constrained environments, and reckons it's ideal for industrial applications such as along railways or in mines. The switch can operate in temperatures ranging from 0°C to 60°C, but this can be optionally extended from -40°C to 70 °C.

Along with the *MSP40*, Belden has also launched a new module for applications that require more power, such as pan-tilt-zoom cameras. It says the PoE+ module "easily" offers an additional 120W of power when needed.

The *MSP40* is available as a 3-, 5- or 7-slot device. It's claimed modules placed within these slots are completely interchangeable or 'hot swappable' without requiring a network shutdown.

Edgecore Networks' *Wedge100-32X* is a commercial product based on the *Wedge100* design submitted to the Open Compute Project. It was originally developed by Facebook as a 32 x 100GbE top-of-rack switch optimsed for web-scale data centres.

Edgecore's parent company, Accton Technology, performed the design validation for Facebook. As well as manufacturing the *Wedge100* for the company's deployment, Edgecore now offers the switch as a fully supported commercial product to enable capacity to be increased using 25G and 100G networks.

According to EdgeCore, the *Wedge 100* provides 32 QSFP28 ports that can each run at 100GbE/40GbE, or as 4 x 25GbE/4 x 10GbE/2 x 50GbE through breakout cables.

The bare-metal TOR switch can be used for data centre fabrics, and is compatible with 19-inch rack or 21-inch Open Rack systems with an Open Rack Switch Adapter.

It is also said to offer line-rate Layer 2 or Layer 3 forwarding of 3.2Tbps full duplex, and has hot-swappable, load-sharing, redundant AC PSUs or 12V DC PSUs.

The *Wedge 100* comes pre-loaded with Open Network Install Environment (ONIE) for automated loading of compatible open source and commercial NOS offerings.

EdgeCore adds that the switch's design is based on Broadcom's *BCM56960 Tomahawk* 3.2Tbps chipset, while its subsystem is the COM-E CPU module, based on the Intel *Atom E3800* x86 processor. According to the firm, the use of this standard CPU system, coupled with the baseboard management controller on the main board enables the device to be provisioned and managed with tools similar to the used by data centre operators for their server and application environments.

Zyxel Communications has unveiled a "premium" line of managed switches.

There are two models currently available – the *XGS4600-32* and *XGS4600-32F* are GbE Layer 3 switches with 4 SFP+ Uplink. The *XGS4600-32* offers 24 x GbE RJ-45 ports, whereas the *XGS4600-32F* offers 24 x GbE SFP slots.

Both offer Gigabit connectivity and feature four integrated 10Gb SFP+ slots that enable high-speed uplink connections. Zyxel says they also feature dynamic routing to simplify cross-subnet communications to "significantly" increase network coverage and resiliency.

The two models offer physical stacks of up to four units created through one or two SFP+ slots, managed as one switch. The company reckons this flexible, ring architecture stacking topology ensures the system can quickly use another stacking connection if the existing one fails, thereby offering enhanced reliability.

It adds that the switches are designed to support active-standby power redundancy allowing a backup power supply to take over in case the main one fails.

AMG Systems now has a completely new range of compact, industrial-grade 1-, 2- and 4-port media converters, unmanaged, and semi-managed switches.

The ruggedised network devices are designed specifically for deployment in IP CCTV security applications where size constraints exist and where round-the-clock reliability for high bandwidth external cameras is needed.

According to AMG, since most outdoor cameras are located beyond standard Ethernet's "normally restrictive" 90m range, all the new units incorporate SFP (small form-factor pluggable) slots for optical media or Ethernet, allowing data transmission up to distances of 120km. The firm says its wide range of compatible SFPs include multimode and single mode optical fibre and extended copper Ethernet, allowing up to 500m at 100Mbps using Cat5e.

The company reckons the new semi-managed switches eliminate multicast flooding to local Ethernet connected devices. It claims this makes them ideal for larger CCTV applications where unmanaged switches are not "sophisticated" enough to handle multicast traffic, and where fully managed switches demand an "unwelcome" overhead of individual programming, additional cost and network complexity.

With the option of 100Mbps or 1Gbps speeds and 30W of available power per Ethernet port, AMG says that PoE and PoE+ enabled cameras or other network devices can be powered directly from its switches or media converters, eliminating the need for additional camera PSUs, power cables and installation expense.

It says adds that all the models can be quickly surface mounted or simply clipped on to a DIN rail for rapid installation and servicing.

D-Link has launched its next generation of Layer 3 stackable managed switches designed to cater for a variety of sectors including enterprises users and ISPs.

The new *DGS-3630* series includes Standard Image (SI) software which supports essential functionality such as Layer 2 switching and multicast, routing, security, amongst others. For additional functionality, D-Link says the switches can be upgraded to Enhanced Image (EI) software using separately ordered licence upgrades. This adds support for full Layer 3 routing for enterprise integration, including OSPF, BGP, VRF-Lite and Layer 3 multicast.

The vendor adds that up to nine physical switches can be supported in a stack, providing fault tolerance and increasing network reliability.

Three models are currently available in the line-up: one with 20 x 10Gb ports; one with 20 SFP ports; and one with 44 10Gb ports. All three also come with four Gigabit combo (RJ45/SFP) ports, which can operate either as copper or fibre ports, and 4 x 10GbE (SFP+) ports that can be used for stacking or for uplink into the core of a network.

All the models are equipped with a rear slot for a redundant power supply. D-Link says one of the new enhancements added is 6kV surge protection on all ports to help prevent damage to the network caused by sudden power increases or lightning strikes.

Other features include D-Link's 'green' technology. This turns off ports that have no link or link partner and ensures LEDs do not illuminate when not needed; and built-in fans that automatically turn on only at a certain temperature.

Eneo has added four, high-power switches to its Gigabit switch portfolio. Although the range is optimised for CCTV installations, the firm claims it is "competitive" in any IT or data network application.

The *IAD-5SG1004MUA* and *IAD-5SG1008MUA* are two new desktop switch models. Respectively, they offer 4- and 8-port unmanaged Gb video channels, PoE budgets of 60W or 120W, and internal switching fabric capacities of 12Gbps or 20Gbps.

The four-port model has twin Gb copper uplink connections while the eight-port version has both Gb copper and Gigabit fibre, SFP uplink interfaces.

Eneo has also introduced an eight-port, rack-mount, Gigabit switch. The *IAR-7SG1008MMA*'s PoE budget is 135W and its internal switching fabric is 24Gbps. As a Level 2, managed switch, it is said to offer VLAN, port-mirroring and multicast support, and comes with two Gb copper and two Gb fibre, SFP uplink connections. The firm says rack-mount, 16-port and 24-port models will follow.

The final addition to the range is an eight port, industrial-rated, Gigabit switch for tough environments and mission critical applications. Eneo claims the *IAM-5SG1008MMA*'s fast-linking redundancy ensures network paths are reconfigured and re-routed within an "unprecedented" 50ms, should a network fail or break for any reason.

With an operating temperature range of -40°C to +75°C, the desk-mount is said to be ideal for extreme environments. It has a 240W PoE budget, 24Gbps internal switching fabric and four, fibre, SFP uplink connections. It is also Level 2 managed, supporting VLAN, port-mirroring and multicast functionality.

"Inadequate" digital knowledge among frontline council staff

Poor digital literacy among frontline local government workers is holding back change projects, according to a new survey from the Public Sector People Manager's Association (PPMA) and Eduserv, a not-for-profit provider of IT services to the public sector.

While most respondents agreed digital knowledge had improved across the council, only a minority reported significant improvements. Sixty-six per cent of PPMA members said they needed to go further in developing a plan to improve digital skills in their organisation.

Four in ten HR leaders said there had been no change in the digital skills of frontline workers and a similar number rated digital literacy of this employee group as "inadequate", significantly more than any other employee group.

While a lack of digital literacy at all employee levels was reported to hold back digital change programmes, the issue was most marked among frontline staff with 85 per cent saying it held their organisation back.

According to the study, 51 per cent of councils are bridging the skills gaps by using the support of external specialists, 34 per cent have created a dedicated plan to improve digital literacy, and 29 per cent are ensuring that recruitment and performance reviews explicitly reference digital skills.

Jos Creese, principal analyst for the Eduserv Briefing Programme and report author, says although councils are taking significant steps to improve digital skills across their organisations, those responsible for delivering services on the frontline are getting left behind in terms of understanding and adoption.

"Digital is about people more than technology, so it is vital that councils put their HR teams at the heart of planning, working with IT and digital teams to ensure the right skills and knowledge are in place to ensure digital change projects succeed," says Creese.

The *Skills for Digital Change* report was based on the views of more than 100 public sector workers as well as quantitative research from a selection of 87 senior public sector HR pros.

Balancing the IT gender gap

The FDM Group has reported an average gender pay gap of six per cent and a median pay gap of zero per cent compared to the national average of 18.1 per cent.

A professional services company with a focus on IT, FDM is an early adopter of gender pay gap reporting introduced by the government last month. This requires organisations with 250 or more employees to publish statutory calculations every year showing how large the pay gap is between their male and female workers. Companies have until April 2018 to report their figures.

Citing research from McKinsey & Co published last year, FDM says eliminating work-related gender pay gaps could add £150bn to annual GDP by 2025 through enhanced productivity and reputation.

The company claims to be the UK's largest IT graduate employer and says it's created a culture that supports diversity and inclusion that is lead from the top. It says 26 per cent of its staff and around 50 per cent of its senior managers are female.

FDM COO Sheila Flavell says: "In developing a culture that supports diversity, social mobility and inclusion, we have learned that if you measure and monitor, you can take proactive steps to understand where the issues lie and devise strategies to develop a culture that supports and improves gender parity."

Some of the strategies that FDM has developed to encourage more women into IT include: creating senior leadership roles within the business; challenging government to tackle these issues; outreach work with local schools to encourage more girls to consider a career in technology; etc.

IN BRIEF…

■ Help desk technicians tend to notch up the least amount of experience in the UK IT industry, reveals a new survey from Spiceworks. It discovered that they have a median of three years in the industry, while network and system administrators typically have seven years of experience, and IT managers clock up 16 years. Spiceworks also found that UK IT pros get more time off work compared to their US counterparts – an average of 28 days versus an average of 18 days across the Atlantic.

■ Managed service provider IT Specialists (ITS) has created a cyber security awareness kit to help businesses prepare for any security breach. It includes a white paper which explains why a unified approach is essential to ensure that all of an organisation's business technology is visible and actively protected. An IT security checklist and reference sheet of security terms are also included to help raise awareness of educating staff on best practices. According to ITS, 40 per cent of organisations that experienced a data breach in 2016 failed a compliance audit. *https://tinyurl.com/mdemxcc*

■ QA has become one of the first UK partner organisations to deliver Google *Cloud Platform* training and certifications. QA says it already has a number of certified trainers already in place and courses scheduled to run across its network of 20 training centres. It says these will enable individuals and organisations to get hands-on training across the spectrum of skills needed to architect, build and undertake data engineering and machine learning on the Google platform. *qa.com/GoogleCloud*

Netbit
DISTRIBUTION

Your No.1 Distributor for Networking Kit

TRADE ONLY

19" FLOOR CABINETS

Eco NetCab

Available
600x600
600x800
800x800
600x1000
800x1000

18U from £**203**	36U from £**282**
22U from £**233**	42U from £**300**
27U from £**259**	47U from £**370**

Assembled in the UK
Next Day Delivery

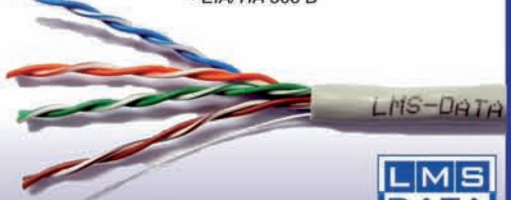
305M BULK CAT5e & CAT6

PVC
LSHZ
CAT 5e
CAT 6
External

25 YEARS WARRANTY FROM LMSDATA BOX 305M

- 24AWG CAT5e / 23AWG CAT6
- Fast Feed Box & Metre Marked
- 4 Unshielded Twisted Pair (UTP)
- EIA/TIA 568 B

CAT5e PVC Solid (Grey)	£**36.95**
CAT5e LSZH Solid (Purple)	£**39.95**
CAT6 PVC Solid (Grey)	£**56.95**
CAT6 LSZH Solid (Purple)	£**58.95**



LMS DATA

PATCH CORDS

	CAT5E	CAT6
0.5m	£0.20	£0.48
1.0m	£0.30	£0.60
2.0m	£0.45	£0.79
3.0m	£0.65	£1.09
5.0m	£0.99	£1.49
10.0m	£1.87	£2.87

Available
Grey / Green
Red / Purple
Blue / Orange
Yellow / Pink
Black

- 100% Copper
- Stranded Cat5e for flexibility
- Injection moulded strain relief boot
- Ideal for Gigabit Ethernet Networking

PATCH PANELS

- TIA-EIA-568A/B2.1
- Quality pressed steel construction
- Gold over nickel plated contacts
- KRONE Compatible

	CAT5E	CAT6
1U 24 PORT UTP (HORI)	£7.60	£8.49
1U 24 PORT UTP (VERT)	£16.65	£23.40
1U 24 PORT STP (VERT)	£17.55	£25.50
1U 48 PORT UTP (VERT)	£25.80	£35.80
2U 48 PORT UTP (HORI)	£15.95	£21.90

LAN SWITCHES

Dynamode

Product Code	10/100 Switches	Price
SW50010-D	Dynamode 5 Port SOHO 10/100 Switch N-Way Desktop	£4.00
SW80010-D	Dynamode 8 Port SOHO 10/100 Switch N-Way Desktop	£5.00
SW160010-R	Dynamode 16 Port 10/100 Switch N-Way Rackmount	£20.15
SW240010-RV	Dynamode 24 Port 10/100 Switch N-Way Rackmount	£23.00
Product Code	**GIGA Switches**	**Price**
SWG50010-D	5 Port Gigabit Switch - Desktop	£11.50
SWG80010-D	8 Port Gigabit Un-Managed N-Way Switch Desktop	£14.50
SWG240010-R	24 Port Gigabit Un-Managed N-Way Switch Rackmount	£64.00

WALL CABINETS

- Colour : Black
- Shelf included (9/12/15/18/21U)
- Removable side panels
- Bag of M6 Cage Nuts

6U from £**34**	15U from £**64**
9U from £**48**	18U from £**78**
12U from £**61**	21U from £**85**

450mm & 550mm Depths Available

PCMCIA

Wireless 802.11n
PCMCIA
300Mbps

£9.10 +VAT

USB WIFI

Wireless 802.11n
USB Adapter
Mini Size

£3.50 +VAT

PCI WIFI

Wireless 802.11n
PCI Card
300Mbps

£8.50 +VAT

USB WIFI

Wireless 802.11n
USB Adapter
3dB Antenna

£5.50 +VAT

HDMI CABLES

1.5m HDMI-HDMI w/Eth&ARC	£1.10
1.8m HDMI-HDMI w/Eth&ARC	£1.67
2.0m HDMI-HDMI w/Eth&ARC	£1.77
3.0m HDMI-HDMI w/Eth&ARC	£2.06
5.0m HDMI-HDMI w/Eth&ARC	£2.57
10m HDMI-HDMI w/Eth&ARC	£6.61

HDMI SPLITTER

2 Port HDMI Splitter Hi-Speed	£17.22
4 Port HDMI Splitter Hi-Speed	£27.78
8 Port HDMI Splitter Hi-Speed	£54.44

VGA CABLES

1.5m SVGA M>M & M>F	£1.10
3.0m SVGA M>M & M>F	£1.66
5.0m SVGA M>M & M>F	£2.57
10m SVGA M>M & M>F	£4.31
20m SVGA M>M & M>F	£9.95
30m SVGA M>M & M>F	£12.11

EURO MOD

£0.56 +VAT

EXTEND YOUR WIFI SIGNAL

Extensive Range of Omni & Yagi antennas

IP CAMERA

withWiFi

FROM £29.50 + VAT

QUANTITY ORDERS WELCOME!

Call Our Sales Team On ☎ 0845 375 2128

With Next Day UK Delivery on 99% of all stock items and a dedicated customer focused account manager - you've got to give us a go!

For our full range of products Please visit www.netbit.biz

email:sales@netbit.biz