

IN DEPTH:
The cable
guys
p8-9

The pressure of data protection

How a move to the cloud doesn't change everything

Fredrik Forslund, Bianco, p7



Managing rapid IoT adoption

A look at how to cope with the IoT takeover

Martin Hodgson, Paessler, p13



SD-WAN & agile networks

How businesses can use tech to underpin their growth

Martin Bosshardt, Open Systems, p15



Travelex 'held to ransom' by New Year's Eve hackers



Foreign exchange operator Travelex became the latest global business targeted by a ransomware gang known as Sodinokibi, as many holidaymakers were heading abroad over the festive period.

Hackers demanded payment of £4.6m and threatened to release up to 5GB of customers' personal data. The company, which has over 1,200 branches and 1,000 ATMs spanning more than 70 countries, said it is "making good progress" recovering from the attack on New Year's Eve.

There was also a knock-on effect as a number of high street banks all rely on Travelex for foreign exchange services. Those that confirmed they were unable to offer online exchange services or process orders for foreign currency, included Barclays, HSBC and Clydesdale and online financial services firms

First Direct, Virgin Money and Tesco Bank.

Travelex and the other financial institutions are understood to have been disrupted for more than three weeks. Staff at the former resorted to pen and paper after the website was taken offline.

The company said a phased global restoration of systems was now under way and some of its customer-facing systems were up and running again.

Khushil Dep, founder of cyber security, cloud and agile domains specialist Daemon Dreams told *Networking+* that the second major cyber security incident in two years to befall Travelex "is interesting" for different reasons. "From the statements made by the company we may infer that primary and secondary systems were not as segregated as they might have been," he said. "The traditional business continuity approach applied by most is built on the belief that a soft-

ware or hardware failure shall be what calls secondary systems into use."

Dep added that while good practice demands logical, network and physical segregation, most will rely on well-formed RBAC policies to segregate access between systems. "Often, however, the need to segregate or even utilise privileged access terminals is forgotten or misunderstood," Dep continued. "A carefully tailored attack can leverage this ignored shared technology base to skip between systems. The latest statement on the Travelex corporate site suggests there was no confidence that this had not happened. Further, it seems that there was a lack of confidence that the infection could not be guaranteed to have been contained to a few systems but may have been a deeper compromise."

continued on page 2

COMMUNICATIONS
TRANSFORMATION
with SD-WAN and
NEXT GENERATION
SECURITY



POSITIVE
SEAMLESS
INTERACTION
from
ANYWHERE



New Year's Eve hackers strike to shut down Travelex site

Continued from page 1

The gang, also known as REvil, claimed to have accessed Travelex's computer network six months ago and to have downloaded 5GB of sensitive customer data.

Dates of birth, credit card information and national insurance numbers are all in its possession, the group said.

Travelex chief executive Tony D'Souza it was "not appropriate" to discuss details of the attack, adding that an investigation was ongoing. "To date, there is no evidence that any data has left the organisation," he said. The firm is working with the UK's National Crime Agency and the Metropolitan Police.

The UK's Information Commissioner's Office (ICO) said if an organisation decided that a breach need not be reported, it should keep its own record of it and be able to explain why it had not done so, if required.

"Organisations must notify the ICO within 72 hours of becoming aware of a personal data breach unless it does not pose a risk to people's rights and freedoms," it said. "All organisations processing personal data should do so safely and securely."

The Travelex hackers later shut down German car parts company Gedia with yet another big cyberattack. ■

Government sees SENSE in £5m 'virtual data centre' project

A "ground-breaking" £5m research project dubbed a "virtual data centre" will use satellite images to better predict the future impacts of climate change, the government announced.

The Centre for Satellite Data in Environmental Science (SENSE) will see experts from the Universities of Edinburgh and Leeds adopt cutting-edge technology to measure rising sea levels, greenhouse gases and shrinking glaciers and forests.

Humans should then better understand climate change impacts and help shape policies on cutting emissions and contributing to reaching the UK's net zero target.

Satellite technology will help predict weather trends and identify areas increasingly at risk of flooding, as well as pollution levels in towns and cities nationwide.

"The UK is leading the world in tackling climate change and we have set the bar high, as the first country to legislate to eliminate our contribution to climate change by 2050 and the fastest in the G20 to cut emissions," said business secretary Andrea Leadsom. "This new satellite data centre will give us instant images showing us the true impact of climate change and in doing so, help us develop innovative new ways of tackling it."

The virtual academic collaboration – established with funding from the Natural Environment Research Council (NERC) and the UK Space Agency (UKSA) – wants to attract 50 of the UK's "brightest and best" candidates from environmental



The Centre for Satellite Data in Environmental Science (SENSE) will see experts from the Universities of Edinburgh and Leeds adopt cutting-edge technology to measure rising sea levels, greenhouse gases and shrinking glaciers and forests

science, maths, physics, engineering and computer science disciplines to undertake a PhD in the innovation centre.

Successful candidates will work closely with experts from the universities as well as leading Earth Observation scientists, plus 18 businesses and partners, including Airbus and Unilever, which will co-fund, co-design and co-supervise 42 of the PhD research projects.

"Earth observation satellites collect hun-

dreds of terabytes of data per day, delivering important information about how fast glaciers flow, the size of forest fires in the Amazon, and the quality of the air that we breathe," said Dr Anna Hogg, co-director of the centre in the School of Earth and Environment at the University of Leeds. "We have a fantastic opportunity to grow the community of researchers with the skills and knowledge to measure the how our environment is changing." ■



Vulnerability Management

Empower your IT

Automatically Detect and Quickly Eliminate Security Gaps

Outdated software and missing patches are open gateways for cyber attacks. You therefore need to keep track of all vulnerabilities on all computers in your company to close dangerous vulnerabilities as quickly as possible. Protect your company's IT against malware and hackers!

Our white paper shows you how to:

- Handle attacks on your firewall
- Automatically trace security gaps
- Close security gaps centrally and automatically
- Enforce Secure Settings



Download free white paper
www.baramundi.de/net+/-vulnerability

Power firm adds new cybersecurity certifications

Power management firm Eaton has added two new technologies to its cybersecurity program with International Electrotechnical Commission (IEC) cybersecurity certifications for its Gigabit Network Card and Industrial Gateway Card.

These products also comply with UL cybersecurity standards to provide advanced network protection for UPS connectivity devices. Eaton said it is the first in its industry to achieve dual certifications for rigorous IEC and UL product certifications.

The Gigabit Network Card was the first UPS network connectivity device to meet the UL standard. Now, the Gigabit Network Card and Industrial Gateway Card are also certified to the IEC 62443-4-2 standard. The technologies are designed to make it simple to connect single-phase and three-phase UPSs, while providing cybersecurity protections for always-on power in commercial buildings, industrial facilities and large data centres.

"Today's data centres, at the edge as well as at the core, need real-time monitoring and control to improve

business continuity and automate remediation of pending issues."

Eric Rueda, Eaton's line manager for software products and connectivity, power quality, EMEA told *Networking+*. "However, they also need confidence that the connected devices installed in their critical systems will ensure the highest level of protection against emerging cybersecurity threats. For years, Eaton has maintained strict procedures at every stage of the product development and sustaining processes. This cybersecurity strategy has paved the way for our Gigabit Network Card to become first of its kind to achieve both rigorous IEC and UL product certifications."

Analysts have indicated that by 2025, 41.6 billion connected devices will be generating 79.4 zettabytes of data that need to be maintained and processed. The growth of the Industrial Internet of Things (IIoT) creates a crucial need for security. Without global cybersecurity standards, IIoT cybersecurity requirements are difficult to manage. ■

EDITORIAL:

Editor: Robert Shepherd
roberts@kadiumpublishing.com

Designer: Sean McNamara
seanm@kadiumpublishing.com

Contributors: Fredrik Forslund,
Tim Thurlings, Martin Hodgson,
Martin Bosshardt,

ADVERTISING & PRODUCTION:

Sales: Kathy Moynihan
kathym@kadiumpublishing.com

Production: Suzanne Thomas
suzannet@kadiumpublishing.com

Publishing director:
Kathy Moynihan
kathym@kadiumpublishing.com

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

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

Government could face huge bill for honours leak

The government is bracing itself for fines and a compensation bill running into the millions following the disclosure of the home addresses of counter-terrorism experts and celebrities on the New Year Honours list.

Senior officials demanded an inquiry into the circumstances which led to the personal details of more than 1,000 individuals, who will receive awards, being posted online by the Cabinet office on Friday, December 27th.

The list of those whose full home address was exposed on a downloadable spreadsheet for at least 30 minutes, included nearly 40 people involved in sensitive defence and counter-terrorism work.

Among those were a number of serving military personnel alongside prominent celebrities such as Sir Elton John and cricketer Ben Stokes. Others who received honours were people helping to secure police stations in Northern Ireland and experts involved in the aftermath of the Salisbury Novichok poisonings.

Rick Goud, chief executive officer (CEO) and co-founder of secure communications provider Zivver, told *Networking+* that data breaches of all types have been on the rise

globally as organisations grapple with how best to safeguard sensitive data from both external as well as the lesser-known internal threats, usually from their own staff.

"The recent New Year Honours list data leak situation, while alarming, is hardly unique," said. "That is because this incident was caused by an employee who accidentally made the sensitive information available online for a short period of time. In fact, most data breaches are actually mistakes by staff, accounting for over 80% of reported incidents according to the Information Commissioner's Office (ICO)."

However, Goud added that the publishing of celebrities' addresses was nowhere near as bad as that of counter terrorism workers.

"I think that in the case of publishing Elton John's home address, the impact would be fairly minimal as that information is already quite accessible to the public," he added. "Many people tend to forget that it was not that long ago when phone books were circulated each year and featured the name, address and telephone numbers of most British households."

He said unlike famous people, most



The list included a number of serving military personnel alongside prominent celebrities such as Sir Elton John and cricketer Ben Stokes

government employees will not have elaborate security measures or 24-hour surveillance in place at their home address and so the ramifications of disclosing this type of sensitive information can be

extremely dire. "These individuals or their residences could become unwilling targets from both UK citizens and foreigners alike, causing a potential national security risk, depending on the situation," Goud added. ■

'AI detects breast cancer better than professionals' – research

Artificial intelligence (AI) is able to spot breast cancer better than a clinician, according to new research.

Google DeepMind partnered with Cancer Research UK Imperial Centre, Northwestern University and Royal Surrey County Hospital to develop a model, which can spot cancer in breast screenings, improve health outcomes and ease pressure on overstretched radiology services.

Initial findings published by the Silicon Valley giant in the journal *Nature* suggest AI can identify the disease with far greater accuracy, providing both fewer false positives and negatives.

The model was trained on de-identified data of 76,000 women in the UK and more than 15,000 women in the US. It reportedly lowered false positive results by 1.2% and false negatives by 2.7% in the UK, but remains to be tested in clinical studies.

When tested, the AI system processed only the latest available mammogram of a patient, whereas clinicians had access to patient histories and prior mammograms to make an informed screening decision.

"Our team is really proud of these research findings, which suggest that we are on our way to developing a tool that can help clinicians spot breast cancer with greater accuracy," said Dr Dominic King, the health lead for Google DeepMind.

"Further testing, clinical validation and regulatory approvals are required before this could start making a difference for patients, but we're committed to working with our partners towards this goal."

Breast cancer is the most common women's cancer globally, yet 20% of screening mammograms fail to spot the disease, instead returning a false negative.

Combined with a shortage of senior radiologists causing lengthy delays – figures from the Royal College of Radiologists in 2018 show the UK needs another 1,004 full time radiologists to meet demand – diseases like breast cancer are increasingly more likely to be misdiagnosed.

DeepMind hopes the use of new technologies like AI will provide the key to spotting cancer early and easing burden on clinicians.

Matthew Gould, chief executive officer (CEO) of NHSX, a new unit driving forward the digital transformation of health and social care, described the result as "an exciting step in bringing the benefits of artificial intelligence research" to patients.

"I'm proud that the UK – and the NHS – is at the forefront of this," he said. "Breast cancer screening is a key part of our prevention programme and we look forward to seeing how this cutting edge research can become part of everyday clinical practice in the NHS."




Breast cancer is the most common women's cancer globally, yet 20% of screening mammograms fail to spot the disease, instead returning a false negative

In his recent review of the national screening programmes, Professor Sir Mike Richards found IT systems "cannot support the safe running of programmes" and need to be upgraded "urgently".

He also found that breast cancer screening programmes were often given "low


priority" by NHS trusts and in some cases management systems have not been updated since the 2017 WannaCry cyberattack.

The government has ringfenced £250m for a National Artificial Intelligence Lab to improve diagnostics and screening in the NHS, including developing treatments for cancer. ■



Visualize Your Network with AI-Driven EnGenius Cloud

www.engeniusnetworks.eu



Supported Devices of EnGenius Cloud

“Transformation of the last mile is finally removing a key barrier to business innovation”



JT

Elliott Mueller, CEO
JT Global Enterprise

The last few years have seen an explosion of technologies that are changing the landscape of IT and Communications forever. The most obvious of these is the move to the cloud, with the availability of cheap, instantly available compute resource. And deriving from the availability of large amounts of this resource has been the development of AI and Machine Learning. In parallel we have moved from primarily text-based communications to a rich world of multi-media. And applications have moved from the PC to being delivered as SaaS. Together these have revolutionised the way companies do business, the way that we interact with those businesses and the networks they use. And networks are far more complex than the traditional hub and spoke with centralised control and a single breakout to the Internet. They have been replaced with a complex web of interactions as SaaS services are delivered over the Internet, while business critical applications are still delivered from the hub. There has been a missing link in all these developments that is still creating a drag on business innovation. How do we deliver the information conveyed by these interactions quickly enough over the last mile that connects business and consumers to the Internet? And if you add in Cloud Telephony and Collaboration this further increases the demands on bandwidth.

Now we are set to see the transformation of the last mile. The UK government's Gigabit Voucher Scheme for fibre, the launch of 5G services, the availability of cost-effective SD-WAN solutions, even the imminent arrival of SpaceX's Starlink Internet service will enable Managed Service Providers to deliver high-speed and more importantly, reliable connectivity to businesses. And this connectivity will be indifferent to the underlying bearers. We are moving to an era of fault tolerant business application networks overlaid on an array of technologies. This will finally allow businesses to offer WiFi Guest services that actually work; shops will be able to take advantage of real-time analytics powered by the cloud to tailor their sales strategies; we may even achieve Connectivity as a Service where you only pay for what you consume, and the SD-WAN router working with an arbitrage service to buy the best connectivity at the best price in real time. High-bandwidth, always on, connectivity has always been a limited resource. We are finally at the dawn of an age where it is available to any business.

Scottish firm gets £2m shot in the arm

Cloud computing and connectivity specialist Beeks Financial Cloud Group has received a £2 million Scottish Enterprise R&D grant to invest in automating its network. The funding contributes to the £4.2m overall spend on the project at the company's new Glasgow head office. Beeks said customer self-service and automation is “at the heart of” its strategic objectives “and is a key differentiator” in the financial services cloud computing sector. This cross-system project will fully automate Beeks' network infrastructure deployment, enhancing its ability to capitalise on the growing adoption of cloud computing infrastructure by Tier 1 financial institutions.



UK cyber security chief boss stands down

The UK National Cyber Security Centre's (NCSC) first chief executive officer (CEO) Ciaran Martin is to stand down later this year after nearly seven years as the government's cyber security boss. Martin was appointed to the board of GCHQ as security head in 2013 and played an integral

role of the establishment of the NCSC as a unit within GCHQ following the 2015 General Election. “It has been the privilege of a lifetime to set up the NCSC and lead its brilliant people,” Martin said. Martin was also named a Companion of the Order of the Bath (CB) in the New Year's Honours List.

Abertay's £5.5m cybersecurity hub

Abertay University in Scotland has officially opened a new £5.5m cybersecurity and videogames hub. The School of Design and Informatics includes a studio for experimental games and hacking projects and the centre also features a laboratory for room-scale virtual reality and augmented reality projects. Finance secretary Derek Mackay opened the hub and said: “The videogames and cybersecurity industries are two international sectors which have enormous potential for growth, so it is great to see universities like Abertay playing a key role and ensuring Scotland is able to take full advantage of that.”

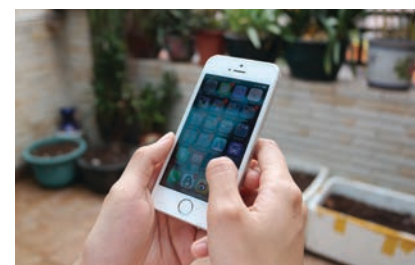
Portsmouth City Council looks to MLL Telecom

Portsmouth City Council has hired MLL Telecom to provide connectivity for its public buildings to a dark fibre network around the port city. It will run off an infrastructure supplied by City Fibre and MLL will operate a wide area network for voice and data services. The network will initially be made available to Portsmouth City Council sites and schools with a minimum bandwidth of 1Gbps and access to Microsoft Azure and the Health and Social Care Network. MLL said the arrangement could possibly be extended to neighbouring Gosport Borough Council and Southampton City Council.

Vodafone offers unlimited data plans for business customers

Vodafone is to offer unlimited data plans to large business and public sector customers, enabling them to provide employees with unlimited data, minutes and texts each month. The Vodafone Business Unlimited tariff will cater to the needs of large business clients; whilst the Public Sector Inclusive Unlimited tariff has also been introduced. Vodafone's unlimited tariffs offer business customers

unlimited data and 5G at the same price as 4G, enabling larger companies and public sector organisations “to unlock the full potential of their workforce” by removing limits on mobile data as a barrier to productivity. “Our large business and public sector customers tell us they don't want to have to predict how much data their employees will use,” said Anne Sheehan, director, Vodafone Business UK.



Boeing Defence UK sues Ark Data Centres

Military contractor Boeing Defence UK is suing Ark Data Centres over a dispute regarding the provision of services at Ark's Spring Park data centre. Boeing Defence UK, a subsidiary of embattled US aerospace giant Boeing, filed the suit against Ark subsidiary Ark Data Spring

Park Limited at the end of last year. Further details about the lawsuit, first reported by The Sunday Times, are not yet known. Ark also runs Crown Hosting, a joint venture with the UK's Cabinet Office that delivers the vast majority of the UK public sector's data centre services.

Third party UK data centre space grows by 48% over the last four-year period

Data centre raised floor expansion in the UK for the second half of last year was in line with that of first half of 2019, at around 27,000 m2, according to the 9th edition of the UK Data Centre Trends Tracker. New space announced for starting the new decade come from NTT, Virtus and xScale. Data Centre floor space in London has the largest share (32%) followed by Slough and then Cardiff. Pricing in the Manchester region has the lowest cost average – with the average rack space & m2 rates being up to 21% below the London and inner M25 rate.

Computer Misuse Act needs reform - report

Britain's cyber-defences are being exposed by the archaic Computer Misuse Act (CMA), according to a legal report. The Criminal Law Reform Now Network (CLRNN), a collaboration between academics, practitioners and other legal experts, says the Computer Misuse Act 1990 (CMA) is “crying out for reform”.

Reforming the Computer Misuse Act details how the CMA is in fact compromising the UK's cyber resilience by preventing cyber security professionals from carrying out threat intelligence research against cyber criminals and geo-political threat actors, leaving the UK's critical national infrastructure at increased risk.

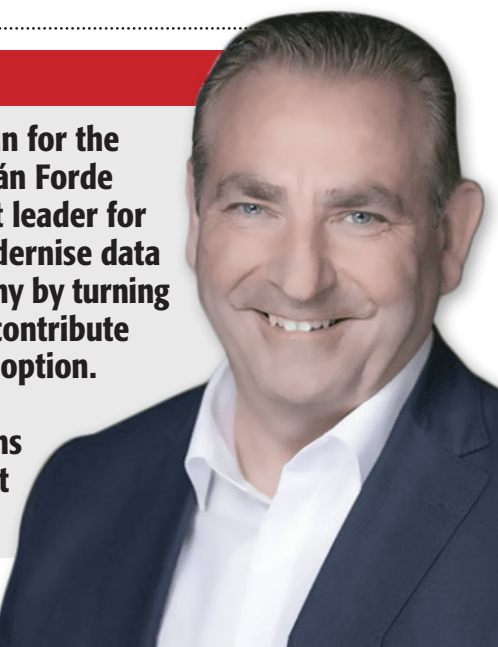
Zyxel enhances Nebula platform

Zyxel Communications has redesigned its Nebula cloud-based networking and management platform. The platform's dashboard has been enhanced with a view to improving the overall performance and usability of the cloud-managed network. New features include bright and dark modes, an array of front-end additions such as card-style widgets and WYSIWYG (What You See Is What You Get) captive portal design for Wi-Fi and gateways. The platform now comes with a Startup Wizard that supports gateway settings, ensuring faster and simpler network setup as well as a Smart Engine to easily correlate settings and events across an entire network.

Word on the web...

The data centre: hero or villain for the energy conscious world? Ciarán Forde as data centre and IT segment leader for EMEA talks about how to modernise data centres alongside your company by turning them into profit centres that contribute towards renewable energy adoption.

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



ALWAYS CONNECTED COMMUNICATIONS

with the Smart Wireless Network

**Why choose Rajant
Kinetic Mesh®** to
transform virtually any
asset into network
infrastructure?

**It's ubiquitous,
connecting people to
people, people to things
and things to things—
mobile, fixed, or both**



**It's resilient
and self-optimizes**
as assets are added or
moved, creating a fully
redundant network



**It's smart and
delivers intelligence**
in real-time with low
latency, high-bandwidth
performance



RAJANT

IF IT'S MOVING, IT'S RAJANT.

Learn how Rajant Kinetic Mesh® can bring IoT to life.
Request a **free demo** at rajant.com/np-demo

Stand and deliver

How cyber gangs are holding businesses to ransom, writes Tim Thurlings, co-founder of Bluedog Security Monitoring

Once highwaymen stalked the nation's roads, forcing travelers to part with cash at the point of a pistol. Today's Dick Turpins find their victims on the internet highway and threaten them with loss of data.

The cyberattack on Traveler demonstrates how ransomware gangs have become the new highway robbers, forcing companies to hand over millions. In the Traveler case, the attackers are thought to have demanded about US\$6m (£4.6 million). They have not only disrupted the supply of foreign exchange but have also threatened to release customers' personal data. The gang – using malware called "Sodinokibi" or 'REvil' – are even believed to have outlined their demands in an interview with the BBC.

The fact is that ransomware is now big business. The number of attacks is on the increase and criminal gangs are brazenly targeting companies in ever more daring attacks.

So what is going on?

Changes in the cybercrime market, the advent of cyber insurance and vulnerabilities in computer systems have all played a part in this new trend.

Cybercriminals have become more professional. Developers are selling ransomware on the darknet, which means they are notoriously hard to catch, and allowing the criminals who buy it to take the risk.

Ready-made ransomware kits are available for as little as €500 and the package even includes helpdesk support and video tutorials to ensure victims can access bitcoins to pay the ransom. Each comes with a unique private key, so every time someone buys a kit, a new variant of strong ransomware is released.

Once inside a user's system, the ransomware starts to spread but is only activated once the backups and many of the machines are infected, or in some cases, by a timer. At this point the company's data is encrypted and the business grinds to a halt. The attackers then make their demands.

Typically the ransom sum is carefully considered and is an amount which is lower than the cost of fixing the problem. By now, for the business, everything is costing money – productivity is at a standstill and experts are working to try to restore the network.

The attackers know that businesses have to get back on their feet or go bankrupt, and that they are insured against these types of attacks. With the insurance companies picking up the bill, the cyber gangs have created a very attractive and profitable business model.

How do they breach the network defences?

Phishing attacks are a common way for malware to penetrate company's networks, however there are some common network vulnerabilities that have provided easy access – such as BlueKeep (in Microsoft's Remote Desktop Protocol), EternalBlue (smb file share) or recently Citrix (another remote desktop like software).

EternalBlue was the weak link behind the WannaCry ransomware attacks in 2017, which brought parts of the NHS to a standstill and also the NotPetya attacks two years later which cost companies including FedEx an estimated US\$10 billion.

Citrix has encountered very recent critical problems where attackers can abuse a flaw to break into organisations networks. As the flaw seems difficult to patch, a lot of attacks have happened in a very short time span.

While there are some solutions that provide a strong defence, they are expensive, not appropriate for all situations and mainly for end-user environments like laptops and desktops. Unless we see better, more affordable solutions and ones suitable for enterprise or server parks, it is likely that attacks will increase in the coming years.

We may also see criminals using malware for corporate espionage and holding intellectual property to ransom – for example, locking up patents and other high-value assets until the company pays for them to be released.

What type of firms are at risk?

Ransomware attacks can affect companies of all sizes, however the nature of the attack tends to be different depending on the size of the business. While big companies tend to be victims of highly targeted attacks by professional crime gangs, attacks on smaller firms are more random – similar to drive-by shootings. The criminals may send out a million phishing emails, knowing that a small number of people will click through.

However while attacks on big companies make the headlines, small firms can be more at risk as they are unlikely to have the money to pay the ransom, hire experts to restore their system or have cyber insurance.

How can companies protect themselves?

It is difficult to be adequately protected against all types of attacks – the truth is that you have to detect the problem as quickly as possible. This can only be done with user behaviour analysis by using internal network traffic to spot break-ins, lateral movement and file changes throughout the network on a large scale.

It is clear that firewalls and endpoint protection are no longer adequate and businesses need to take their security to the next level by using a professional 24-hour cybersecurity monitoring service.

This will not only strengthen their defences, but also enable them to detect threats inside the network, including ransomware spreading through the system – ensuring that any problems are identified and contained as quickly as possible with minimal impact on the business.

**Tim Thurlings, co-founder,
Bluedog Security Monitoring**

The possibilities are edgeless.



DATA CENTRE
WORLD

Stand D910

11-12 March 2020 | ExCeL Convention Centre, London

Tripp Lite's micro data centre solutions make the edge computing easy, cost-effective, and most importantly, customisable to every unique user's needs.



SCAN ME

RSVP with Tripp Lite for your chance to win a £100 Amazon voucher!

TRIPP-LITE
Powering and Connecting
Your World



Connect USB devices to the network easily, safely and securely!



Questions? Interested in a test device?
Contact us!
Phone: +44 (0) 1273-2346-81
Email: info@seh-technology.co.uk

Made
in
Germany

Features

- Isochronous USB mode: transfer of audio or video data streams
- Flexible and location-independent usage of USB devices in the network
- High performance device with 3 x USB 3.0 Super Speed Ports
- USB port 3 as charging port (e.g. for mobile devices)
- Fastest transmission of USB data from the USB device to client - up to 100 MB/s**
- Enterprise security on both hardware and software levels
- Ideal for virtualized environments (Citrix Xen, VMWare oder HyperV)
- 36 months of guarantee (upgradable to 60 months) for free
- Free software updates, technical support worldwide
- For all common operating systems: Microsoft Windows, Linux, OS X/mac OS

Areas of application



SEH Technology UK

Phone: +44 (0) 1273 2346 81 | Email: info@seh-technology.co.uk | www.seh-technology.com/uk



A move to the cloud doesn't change your data protection responsibilities

Fredrik Forslund, VP enterprise & cloud erasure solutions at Blancco

Booming data volumes and new data protection regulation has made organisations feel immense pressure in the last year. They are struggling to cope, even failing to adopt basic data protection habits. Concurrently, the shift to the cloud continues, as organisations turn to cheaper and more flexible cloud solutions, rather than store and process data in-house. Moving to the cloud relieves some of this pressure – cloud providers take on some of the regulatory load – but it's important that assumptions aren't made.

Breach of data, breach of trust

A data breach can affect revenues, consumer trust, and industry partnerships as well as seriously sully a reputation. Recent breaches have garnered mass media attention, meaning organisations now not only face regulatory fines under GDPR but also questions from customers and journalists.

While moving data to the cloud provides flexibility and capacity, it doesn't remove the risk of a data breach. The cloud provider (data processor) is responsible for the security of the infrastructure itself, but the organisation using the cloud (data controller) is still responsible for the security of any data. GDPR forces data controllers to establish a legal precedent using one of six bases for data collection featured in the legislation. While data processors must also comply with new legislation, the controller will always be the principal party responsible.

A lack of knowledge of correct data management processes is exacerbated when enterprises migrate to the cloud. The 2019 Capital One breach affected 106 million people and a source with direct knowledge blamed it on "a misconfigured open-source Web Application Firewall (WAF)...hosted in the cloud". Many organisations lack the knowledge and tools required to identify and fix cloud misconfigurations like this.

Similarly damaging data breaches can be avoided with a few steps.

Plan, manage, deliver

Organisations choosing to use a cloud provider must consider both the types of data they are sharing and the whole data lifecycle. As volumes of data are increasing, so are the different types of data which require storage and management. This mass of variables can make it difficult to track data throughout its lifecycle to end-of-life. GDPR grants a right to erasure and to comply organisations must be able to securely identify, extract and erase specific data with an auditable trail on request. There are many organisations that would find this challenging, if not impossible.

Organisations are often unclear on what processes a cloud provider has in place to manage processes like data migrations, cloud exit and end of data retentions. Being aware of these is equally as important as being aware of what data is being stored. Enterprises must track and securely sanitise redundant data to ensure GDPR compliance. Cloud hosting doesn't remove that responsibility, but changes how enterprises must meet it.

Understand and assign data responsibilities

Simple changes can make a big difference. GDPR made appointing a data protection officer (DPO) a requirement for both data controllers and processors if they are a public authority, process large scale data, or hold certain data (such as criminal conviction data). In conjunction with a cloud provider, a DPO will ensure the entire data lifecycle is considered from purchase to disposal.

They will coordinate with information security teams as well as IT operations and procurement, making data protection a priority. A DPO will be also able to identify and prioritise security risks. We surveyed IT professionals and asked them to rank cloud security threats in relation to their company's budget, resources and tools. Surprisingly, one trailed at the bottom of most lists: improper or incomplete data removal. This proved that a lack of education was universal.

This attitude towards the value of data sanitisation must change immediately if organisations

want to prevent a worst-case scenario data breach. Any data breach is bad for brand equity, but a breach of data which should have been securely sanitised already is notably worse. Zero-day exploits, insider threats, and targeted phishing attacks all mean that data breaches can still happen even if best practice is followed. For data controllers, the privacy and security of all data processed in house or in the cloud, however old, is ultimately their responsibility. Tracking, managing and securely erasing sensitive data is the best way they can protect it.

Cloud providers should be subject to defined audit processes to ensure compliance with the latest data privacy regulation. Whenever storing data offsite with a cloud provider, organisations must know where their data is being stored, how it's being protected and the sanitisation processes in place. All organisations need to review their end-to-end data management process and ensure regulation conforming processes throughout. Cloud hosting doesn't remove that responsibility – it simply adds a partner to the mix.

www.excel-networking.com

PON

Delivering Connectivity, Performance and Innovation at the Speed of Light

The Excel Passive Optical Network Solution is comprised of an innovative infrastructure system designed to meet increasing demands for higher bandwidth and faster availability of data, whilst managing budget and operating costs.

Where there is a demand for high-speed connectivity and unrivalled performance across distances up to 20 kilometres, you can count on the Excel PON Solution to deliver a versatile selection of products and flexible deployment options, suitable for both residential and enterprise environments.

Discover the Excel PON Solution
www.excel-networking.com/PON-Solution

The cable guys

Data centre cable management is often said to be a complex task. Robert Shepherd seeks advice on how to keep things tidy

If you think of an enterprise as a human body, the data centre is the heart that pumps the lifeblood around it. To use another analogy, numerous issues can also plague the mechanics of the data centre's anatomy as time goes on. One of those is improper cabling, which can spell trouble for the entire enterprise, leading to things like "spaghetti" cabinets, difficult equipment installations and extended periods of troubleshooting and maintenance.

Indeed, the early days of interconnection many managers, for whatever reason, ignored structured cabling. However, as the industry standards took hold, quality generally improved.

Quite simply, the failure to properly manage this critical part of data centre infrastructure can cause serious issues, from increased operating costs to more expensive outages. Yet while cabling ostensibly requires technical skill, is that really a defence if things go wrong as a result of bad management? Mike Connaughton, technical sales manager - data centre solutions, Nexans says, depending on the data centre, it need not be such a difficult process, provided cable management is not a mere afterthought.

"With cable management in mind during the design phase, it can be made simple," he says. "But I have also seen cases where cable management was added later, for a variety of reasons, and these were more complicated. For example, I have seen a data centre that had some halls using below-floor cabling pathways and overhead cabling in other halls. The transitions were not always elegant."

Matt Edgely, commercial director, TeleData UK agrees and says the right amount of capacity, route, diversity and structural planning work must be put in at the outset. "Investing that bit more into your day one infrastructure can save a huge amount of retrospective planning and work arounds in the future - which is where a large amount of complexity can come into play," he says. "Following best practice and doing the simple things right, like auditing, labelling, removing obsolete cables etc. makes for a far less complex and a far

more effective in-house cabling system."

However, Alberto Zucchini, data centre solutions and services manager at Siemon, says cable management is one of the most challenging topics in data centres. "Many different cables (data communications, power etc.) should be arranged in a proper way, ideally have limited size and proper routing, be flexible, allow for frequent moves, adds and changes," he adds. "They should also not interfere with each other, as data centre operations should be implemented in a proper way - this requires good design in order to keep power and data separate and possibly make good use of often limited unused spaces. Moreover, bad/no labelling/colour coding does not allow for locating cables easily for troubleshooting, testing or repair, to install new equipment, or to remove extra cables after equipment has been moved or upgraded".

Airflow (I won't bore you with another human biology comparison) is another key element of cable management and Connaughton says there are two specific areas where cabling can have a significant impact. "One is when it is within the rack, sloppy cabling practices can block the direct airflow from the equipment fans," he adds. "Both the inlet and exhaust fans need to be kept clear. The use of proper patch cord management, reduced diameter cords and appropriate panels are all ways of mitigating this problem. The other is underfloor cabling can create air dams where the cool air is trapped in locations and not allowed to move to the vents below the racks. Since it is below the floor, the 'out of sight-out of mind' problem can exist. Reduced cable diameter and proper pathway fill ratios are key strategies to prevent this problem."

For Edgely, good cable management and following simple best practice guidelines such as calculated cable lengths and adhering to routes can have a huge impact on the effectiveness of cooling systems under-floor. "Bad cable management can cause barriers and uneven airflow resulting in an imbalance of forced air pressure," he adds. "It can also limit a data centre's ability to make

changes to cooling systems in the future for fear of disturbing cables."

So, when it comes to data centres, what is the most common challenge when you're kitting one out?

"Within a multi-tenanted data centre where you could be cross connecting from any rack to any rack at any time, it's making sure you have the structure and capability to do so from the outset," says Edgely. "This takes you back to the importance of planning again. Of course, there is the issue of ongoing quality control which comes down to process, people, training and management."

Connaughton's colleague and product manager Michael Wang says the most common challenge in cable management is always how to provide a scalable management solution for cabling. This is separated to cable management for horizontal/backbone cable and patch cords.

"Data centres have different types of infrastructure and installation methods," he says. "For example, enterprises as opposed to hyperscale or cloud data centres) prefer to build data centres from day one using structured cabling and pathways to handle horizontal cable and patch cords, but on the other hand, many data centres now prefer a modular approach, either for cabinets installed in PoD way or pre-loaded cabinets."

Wang says some will only adopt power and infrastructure at day one and install cabinets on demand. Therefore, the

selection of pathway is more for backbone and not for horizontal cables which could be run through pathways put direct on top of cabinets and/or inside cabinets. "The important part of a pathway system today is to allow cable to safely enter into cabinets which may not have been available from day one," he continues. "Examples include use of 'waterfalls' in FIBREROUTE or overhead patching frames. We also need to consider cable diameter. Some of the mega projects now require 144 or much higher fibre count cables, so cable makers are now designing advanced cables with higher fiber count but which are much smaller than in the past."

Density is also increasing in the cabinets - which requires management - and Wang says his firm now offers Ultra High Density (UHD) cabling not only for fibre but also for copper. "Slimflex patch cords are 30-50% smaller than before," he says. "We know that new ethernet technologies will ask for more higher density connectors than in the past so this will only be more challenging for customers. Data centres also require a lot of fan-out cable or patch cords for new ethernet applications. Solutions to handle fan-out cable and routing for those cables/cords will be important for customers."

Wang says he has seen some customers "just hang all the fan-out connectors on the cabinets" which will definitely cause

"The thing that struck me first when I entered the room was the noise of the CRAC units on the walls - they were working at almost maximum capacity."

*Paul Cave,
technical pre-sales manager,
Excel Networking Solutions*



a headache in future. “So, we need to provide robust designs for the transition point of the fan-out cable and even consider those as horizontal cables instead of patch cords,” he adds. “The ENSPACE panel is a good example to allow customers to manage patch cords in a scalable way. The concept of an individual drawer allows customers to manage patch cords according to business demand.”

Paul Cave, technical pre-sales manager for Excel Networking Solutions, says achieving the correct level of resilience within the initial design as well as providing the correct ‘expansion’ space is the most common problem. “Too many people underestimate the correct level of spare capacity with containment,” Cave adds. “This is then compounded by M&E contractors ‘value engineering’ the containment to reduce costs, too many projects design for today rather than planning for tomorrow, some DCs I have been in use for over 10 years with multiple iterations of technology upgrades and are now reaching their limit, not due to space or cooling or even power but because they cannot physically run anymore cables to them.”

Although prior-planning usually prevents poor performance, there must be a number of situations where slapdash cable management has led to data centres – for want of a better expression – ‘going under’, no?

“It doesn’t happen often, but it has happened,” says Edgely. “Shoddy management of one aspect of the data centre usually flows through into other areas and customers are savvy enough to know this and naturally this affects sales figures.”

Cave concurs and while he “cannot mention any names”, one offender is operated by a major high-street supermarket.

“The thing that struck me first when I entered the room was the noise of the CRAC units on the walls – they were working at almost maximum capacity,” he says. “The room wasn’t actually overly hot the problem was the design and highlights a couple of the points already raised. In this particular data centre, all the cables were run underneath the raised floor, this was also an air handling space with the cold air supply, no cables were routed at high level.”

Cave says that when raising some of the tiles the culprit “was obvious”. It had undergone a number of upgrades to equipment over the years but it never removed any of the old redundant cable as staff didn’t note which cables were unused.

“Whilst this data centre did not ultimately fail, it did result in a very expensive transition plan, which involved the lease of an external data hall whilst this particular one was completely redesigned and rebuilt it was a very long and expensive process,” he continues. “It must be noted that the original data centre had been first designed and built in the mid-1990s when computer equipment and connectivity was totally different and they just kept trying to fit more equipment in.”

Cave is in good company when it comes to witnessing bad practices.

“The worst example that I have ever seen was a case where the pathways were so full of abandoned cable, that there were several full-time employees whose only job was to trace and remove abandoned cable from the pathway,” says Connaughton. “It was an agonisingly slow process to watch – most of the cables had no labelling and no consistent pathway so each cable had to be manually traced from beginning to end and cut out along the way.”

Zucchinali says he once received a phone call from an installer who asked us Siemon to “retrofit” a brand-new data centre as cable management was simply forgotten. “No cabling distribution was considered

during the entire design and in absence of any structured connectivity this would have quickly created a jungle of flying patch cords all over the room,” he adds.

Although it’s obvious, or it should be, that the advances in cable quality play a key role in the job a data centre does, has the cabling new and innovative to support the cable network in a data centre?

“Not specifically that we can think of,” says Edgely. “For us, we have similar challenges to those faced 15 years ago – although there have been some positive developments in some consumables and tools.”

For Michael Adams – solution design engineer, operations at Interxion, “there are a huge amount of cabling products on the market with a range of different attributes that could support the cable networks” within a data centre. “That said, every data centre has different requirements and not every product can provide a catch-all solution. For example, MPO cabling can vary in usefulness from site to site, so we stick to the splicing method,” he says. “Where we do see value is the high density panels within our MMRs, which support our customers who have a significant demand for cross-connects.”

Connaughton says, “generally speaking”, over the past few years, a few that stand out.

“Reduced diameter cables – there is a practical limit to how small a cable can be manufactured and still be handled properly, but this reduction does a lot to help manage the cabling in the pathway. Aside from taking up less space, it also can make the cables more flexible to allow for neater bundles.”

In addition, he says, the weight reduction can simplify the pathway requirements.

“Polarity switch connectors – polarity has always been important, but as parallel optics became more popular, the fixed relationship between the fibres in an MPO/MTP connector made polarity critical,” he says. “New connector designs allow for the polarity of a connector to be altered in the field. In the past, it was common to install an additional patch cord to make this correction.” Connaughton also highlights patch panel design. “Integrating cable management into the patch panel has helped keep the panel neater, he continues. “This has shown up in several forms including angled panels and sliding trays. This has become especially important as densities have increased.”

Cave says the last development that had a key impact on DCs was the MPO (MTP) connector, which allowed for higher density fibre connectivity however that connector has been around for over 20 years. “Most major DCs are based on Singlemode fibre which effectively has unknown bandwidth, the combination of these two seem to be the way forward. We have had Category 8 and OM5 however the take-up of these has been extremely limited to say the least although Category 8 has been around since 2016 there is still no equipment that can use this, and the cost of OM5 cable and connectivity being more expensive than SM has meant it is seen as a dead-end by some.”

Apart from increased operating costs and expensive outages mentioned at the beginning of the article, there are plenty of other problems that can be faced.

Connaughton says one is “an aesthetics issue” because a cabling system that is sloppy can lead to other, harder to measure problems. He also says, “sloppiness begets sloppiness” and if management allows the cabling to be unkempt, what else will it overlook?

“This goes along with the “broken windows” theory of civic management – keeping everything neat and tidy encourages everyone to want to keep it that way,” Connaughton adds.

Last but not least, he cites utilisation rates. “While this is a contributor to operating costs, poor cabling practices can make it extremely difficult to know whether there are available ports for additional connections,” Connaughton says. “This is an area where Automated Infrastructure Management (A.I.M.) systems can play an important role.”

Cindy Ryborz, marketing manager data centres EMEA, Corning Optical Communications says signal-loss can be a common problem as moves, adds and changes are made within the data centre over time.

“Bend-insensitive fibre is an effective solution here and can exhibit up to a tenfold reduction in loss at the point of the bend when compared to conventional multimode fibre,” she adds. “This protects the system margin or power budget headroom and prevents unscheduled downtime. As well as problems related with connectivity, that may cause the failure of a single component or even the whole network failure, hence, it becomes extremely important to have clean components (connectors/adaptors) that can be used in the installation process.”

So, it looks as though we are there with cables, but don’t data centres also need to be wary of connections/adaptors? After all, the cable might be great but unless the connector is up to standard the end product won’t be great.

Well, when it comes to maintenance there’s one thing all the contributors agree on.

“Cleaning, cleaning, cleaning,” says Connaughton. “The single biggest problem in optical connections is cleanliness. Proper cleaning of the installed connector and the test lead are critical. Especially since newer and faster networks speeds tend to coincide with smaller power budgets.

Cave has the stats to back it up, too. “Fluke Research state 85% of all fibre faults is



“It becomes extremely important to have clean components (connectors/adaptors) that can be used in the installation process.”


*Cindy Ryborz,
marketing manager data centres EMEA,
Corning Optical Communications*

end-face contamination NTT state in excess of 80% therefore this is the number one problem within DC connectivity and one I have experienced on numerous occasions,” he says. “The main recommendation I give anyone handling fibre within a DC is to get the best fibre inspection they can afford and then learn how to clean fibre correctly.”

If there’s one thing to remember from this, it’s to keep it clean, guys. ■

HellermannTyton

RapidNet Data Centre Solutions




RapidNet is the world-leading pre-terminated, pre-tested cabling infrastructure solution from HellermannTyton. By choosing a pre-terminated RapidNet system it is possible to reduce installation times by up to 85% when using copper or 95% with fibre.


HellermannTyton's RapidNet pre-terminated copper systems offer options and flexibility to any network cabling infrastructure project. Available in Cat6A, Cat6 and Cat5e, HellermannTyton are able to supply pre-terminated copper RapidNet in 12-port, 6-port and 4-port cassettes.

The extensive RapidNet fibre range from HellermannTyton has developed with the increasing demands of high performance, high speed networks and data centres. Available in OM5, OM4 and OM3, RapidNet fibre provides a number of connectivity options, including MTP, LC and SC cassettes.

Visit us online at
htdata.co.uk



Stay in touch with us!



CORNING



Connect to maximum density
with faster installations.

As the popularity of cloud computing and big data grows, the demands for high-speed transmission and data capacity are greater than ever before. Address your most challenging data centre concerns with our high-fiber-count MTP® trunks, a preterminated solution offering increased density, easier cable management, and enabling reduced installation time.

Visit corning.com/emea/en/dc-solutions to learn more about how to overcome cabling challenges in larger networks operating at higher speeds.

DCW London 2020

Visit us at stand: D960

© 2020 Corning Optical Communications. LAN-2472-A4-BEN / January 2020



connectivity
consultancy
engineering



CONNECTING THE PUBLIC SECTOR

- **Carrier Class:** Cost-effective, resilient and flexible networking solutions delivering private wide-area networks, ISP & cloud connectivity from our own national network.
- **Secured Solutions:** Hyper-scaling, market-leading security solutions to support secure digital transformation.
- **Expert Engineering:** Consultancy-led design, expert engineers backed by a 24x7 NOC/SOC.

**CALL 08456 800 659
OR VISIT WWW.TNP.NET.UK**

KVM CHOICE
Total Control in Computing



**Specialist suppliers
of Datacentre
equipment
call for a quote today!**

**DCW
Stand D50**

HASSLE FREE PROCUREMENT OF: IT / NETWORK / POWER / INFRASTRUCTURE EQUIPMENT



**sales@kvmchoice.com | sales@pduchoice.com
www.kvmchoice.com | 0845 899 5010**

IT upgrades for the blues and twos

All three emergency services get help to continue saving lives



Radiocoms assists Derbyshire Fire & Rescue with digital transformation

Derbyshire Fire & Rescue Service (DFRS) covers a service area of 1,000 square miles, which includes a variety of urban and rural communities, with a population of around one million people. Its operational area includes the Peak District National Park, underground caverns and historical sites such as Chatsworth House and Bolsover Castle. The service operates and maintains 31 fire stations, four area offices and has a joint police and fire headquarters in Ripley, Derbyshire.

DFRS pushed forward with a digital radio communications upgrade in 2019 as part of its commitment to digital transformation within the firefighting industry.

After DFRS reviewed a number of radio technologies, it chose Radiocoms to supply the upgrade to a Motorola Solutions MOTOTRBO radio system to replace the existing analogue radio network. The technology is designed to cope effectively within the harshest of environments.

"Clear, concise communication is essential in the effective delivery of a modern fire and rescue service, working to make Derbyshire safer together," says Derbyshire Fire & Rescue Service Response Area Manager Phillip Mitchell. "It is critical that we have a reliable and robust communications system that provides uninterrupted service for every situation that our Firefighters encounter."

The aim of the new system was to create robust and clear communications with functions which address the specialised needs of firefighters. Radios selected by Derbyshire Fire & Rescue Service were the rugged, easily operated MOTOTRBO DP4601e and MOTOTRBO DP4401Ex ATEX GPS-enabled hand portables which in addition to all the expected basic functions have a number of features ideally suited for FRS purposes.

Other pre-requisites were a prominent orange emergency button to summon help with one touch, location and telemetry sensors, design for easy operation when wearing gloves and the latest energy technology also delivers up to 28 hours of battery life for 3-shift working, plus an improved receiver boosts range by up to 8% compared to previous models.

Programmed and aligned to work within NOG (National Operating Guidelines) the new radios have provided the fire service with a resilient, operational ready communications device that they can rely on during unpredictable situations.

Now, even when in the depths of a building staff will hear every broadcast which is imperative should an emergency evacuation be initiated.



Ambulance services enhances IT security

The North East Ambulance Service NHS Foundation Trust (NEAS) operates across Northumberland, Tyne and Wear, County Durham, Darlington and Teesside. It provides emergency care services to respond to 999 calls and a Patient Transport Service (PTS) for pre-planned non-emergency transport to help patients in the region.

A team of five IT systems senior analysts at NEAS manage 900 endpoints at multiple sites across the northeast of the UK, from the Scottish borders to North Yorkshire. However, they were facing a number of challenges, including complex security requirements as a mobile ambulance trust, issues around visibility of threats and consolidation of IT security to a single synchronised platform.

Sophos EndPoint Protection was due for renewal, so the NEAS IT team decided to explore wider propositions from Sophos with the support of its Sophos partner, Trustmarque. After a number of meetings in which it discussed several Sophos offerings – including next-generation firewalls, Sophos Synchronized Security, Sophos UTM and Endpoint Protection – the team decided to move forward with a complete solution from Sophos to improve its IT security and upgrade the traditional on-premises line-up. NEAS has now implemented the following products:

- Sophos Central with Server Protection Advanced – a unified console for managing Sophos products
- Sophos EndPoint Protection (five-year renewal) – prevention, detection, and response technology
- Sophos UTM – a unified network security package in a single modular appliance
- Sophos RED – which makes extending a secure network to other locations easy. In this case, it was used to access patient data. RED was tested with the air ambulance service, allowing first responders to securely access patient files while mobile.

NEAS placed the order through Sophos partner Trustmarque. NEAS reduced its IT security risks through increased visibility of threats using one synchronised platform. "Our key objectives in the procurement of this security software were to reduce management time and ensure a seamless migration from the existing software," says NEAS IT technical engineer Daniel Malone. "Many of our challenges were overcome with the procurement, ensuring that our information is now secure."

Among its future plans, NEAS intends to further upgrade its existing Wi-Fi solution and implement Intercept X, a next-gen anti-ransomware, anti-exploit solution, and will work closely with both Sophos and Trustmarque to implement these additional improvements.



Falck Fire Services gets VoIP assistance

Falck is a deliverer of emergency services and has a long, proud history of saving and improving lives across the globe.

Since the company was founded in 1906, a core business has been fire fighting for public authorities and industrial clients. Falck Fire Services UK delivers a range of services to customers in a variety of industrial manufacturing sectors. Falck's industrial emergency response team prides itself on the high standards of services it delivers to companies at the heart of chemical, petrochemical, oil and gas, energy, biofuel, and biotechnology production in the UK.

When you are in the business of saving lives and helping people, you rely on the very best technologies to ensure employees are ready to help those in need.

In order to react immediately to a reported incident, Falck operates in a state of permanent readiness and therefore requires a robust, simple to use communication platform with constant availability, 24/7, without fail.

The company required expert assistance with the design and installation of a sophisticated Voice Over Internet Protocol (VoIP) and call recording solution for its new operations centre at Wilton Teesside.

PowerDial, a specialised division of Prodec Networks, worked in close collaboration with communications specialist Avaya to deliver the ideal solution and meet Falck's high demands.

Avaya's communication's manager solution is used by 60% of the UK's emergency services, making it an ideal choice. It provides two-way communication to response vehicles and with no single point of failure, it is specifically designed to be always available.

As part of the systems failsafe design, critical components were duplicated to prevent any single problem causing a system failure and ensure maximum reliability uptime. This has resulted in zero breaches in PowerDial's service level agreement and a lasting, stable relationship between client and provider.

What's more, the client feedback couldn't have been more positive. "The service standards we set correspond with the high expectations of our customers – and from the outset of this project, PowerDial's technical knowledge and service quality more than lived up to the testing criteria that we set," says project manager Jakob Thinggaard. "PowerDial designed and implemented the project very professionally, providing real insight into how we might deliver our services with maximum efficiency and showed a real empathy with our business needs." He added that "it's been a true joy" working with the vendor and he "can highly recommend choosing" the firm for any kind of communications project.



Met invests in Sepura TETRA terminals

The Metropolitan Police Service selected Sepura's SC2 Series of TETRA terminals to replace their existing fleet in an agreement forming one of the largest single orders ever received by the UK-based TETRA specialist manufacturer.

This decision was taken after an extensive trial with the devices across numerous sites with varied teams within the force. Trial users reported back their strong preference for Sepura SC2 terminals over other suppliers, with positive feedback based around improved performance where coverage was poor and the ease of access to emergency call buttons. The large screen on both devices also proved popular, with its intuitive user interface offering quick access to essential functions.

The force fleet will comprise of both Sepura's flagship SC20 terminal alongside its more compact but equally powerful stablemate the SC21. A choice of terminal is available to officers dependent on their operational requirement. This operational flexibility will be supported by a common user interface across devices ensuring that users will be familiar immediately with their allocated terminal.

Indeed, the overall solution delivered was as important to the force as the choice of terminal. Sepura's "efficient battery management", combined with streamlined accessories across the Sepura SC2 Series range, will allow the force to save costs and reduce deployment time on a day to day basis.

In addition, a bespoke software release has been developed to deliver specific functionality, supporting the operational performance of the Metropolitan Police. With future innovation possible through the AppSPACE software environment, the new terminals will help to drive operational efficiencies.

"The outstanding feedback from the Metropolitan Police trial users was that the SC20 and SC21 devices were significant upgrades on their existing terminals, with improved audio and an intuitive user interface allowing officers to use the terminal quickly with minimum expense on training," says Gary Maughan, regional director for UK and Ireland, Sepura. "By taking the time to understand the force requirements, we were able to deploy innovative solutions that will enhance force-wide operations and TETRA fleet maintenance. We look forward to working closely with the MPS to deploy the devices and further support their communication requirements."

The fleet will number over 32,000 terminals from the SC2 Series and SRG3900 mobile series, supplemented by Sepura's extensive range of audio accessories. They were deployed throughout 2019, with the first devices going live in May and all devices operational by December.

"This order from the largest police force in the UK is a considerable endorsement of both Sepura's products and our customer-led approach," adds Steve Barber, chief executive officer (CEO), Sepura.

Trash talking

How smart city specialist Connexin is helping a northern city clean up its act

A partnership between Hull City Council and smart city specialist Connexin has optimised waste collection from Public Waste Bins across the city.

The city of Hull, also known as the slightly more grandiose Kingston upon Hull, is a port city located in the heart of England's Northern Powerhouse. The city attracted the title of UK city of culture 2017 and was assigned £32.8m for cultural events and to improve the city's public spaces. In 2017 tourism was worth more than £300m to Hull for the first time.

With the influx of visitors, the city found itself processing more rubbish than ever before. However, the council also recorded that, up to 75% of Hull's 4000 waste bins were empty when they were collected. With the council facing continued year on year budget cuts, to prevent further reductions in the services provided to the city's 284,321 residents, the authority looked to optimise its services for maximum efficiency.

The council looked to source an infrastructure provider to design and build a network which could support Smart Waste Management sensors but also easily be scaled if required to support additional services such as Smart Lighting, Air Quality Monitoring or Parking.

Once the network was available the sensors would then need to be installed into the top of public waste bins and integrated onto the network and the information relayed on a dashboard where data can be tracked and monitored.

Connected via LoRaWAN connectivity, Connexin installed waste sensors into specified waste bins. These sensors were then configured to feed information back into the Connexin City OS. Following this, Full training on the usage of Connexin City OS was provided to senior users.

Connexin was able to utilize its existing

carrier-grade citywide LoRaWAN network in Hull to provide backhaul connectivity to the sensors at a highly competitive cost. With gateways located across Hull already providing connectivity readiness, Connexin was also able to reduce the overall time frame of the project.

The council could improve the management of their waste collection service using real-time data, with an alert configured to automatically notify council staff upon the fill level within the bin reaching 80%.

Notifications were also forwarded to the council dashboard in the event of an incident such as overflow, fire or vandalism enabling the council to respond more quickly.

The intelligent Connexin City OS also helps the council use information to predict future trends and fill levels.



Furqan Alamgir, chief executive & founder of Connexin shows Networking+ one of the sensors that will be installed in Hull's new smart bins

Use of waste sensors to rocket by 2023

The number of installed smart waste management sensors is set to rise from 379,000 worldwide in 2018 to 1.5 million in 2023.

That is according to new research from M2M/IoT market research company Berg Insight, which also said that figure represents a compound annual growth rate (CAGR) of over 30%.

These wirelessly connected sensors can either be pre-integrated into waste bins and containers or retrofitted into existing ones.

At present, Europe accounts for more than 50% of the installed base. The UK, as well as markets such as the Benelux, France, Spain and the Nordics have witnessed particularly positive market developments.

The world's leading smart waste sensor technology vendor in Q3-2019 was the US-based smart bin provider Bigbelly, which had a global market share of 13.3 percent. Finnish Enevo and Chinese Dingtek Technology shared second place. Enevo is a leading player in Europe and North America while Dingtek has a strong position on its domestic market.

Other important vendors include UK vendor FarSite Communications.

The top 10 vendors accounted for more than 60% of the global installed base of smart waste sensors. Many of them have

chosen to focus on specific customer segments such as public litter bins, commercial waste containers or textile recycling banks.

"The interest in smart waste sensor technology has increased significantly over the past 18 months and is now increasingly seen as an integral part of any smart city strategy", said Levi Ostling, IoT Analyst, Berg Insight.

Cellular 2G/3G/4G technology has prevailed as the dominant connectivity option for smart waste sensor installations, accounting for around three quarters of the global installed base in 2018. LPWA technologies such as NB-IoT, LTE-M, LoRaWAN and Sigfox are however establishing themselves as attractive alternatives due to their lower power consumption – a feature that is essential for the performance of smart waste sensors as they are mainly battery powered.

In fact, LPWA communications technologies accounted for around 20% of the global installed base of smart waste sensors in 2018. The share is expected to increase to more than 50% by 2023.

"The transition to LPWA will significantly improve the overall feasibility of smart waste sensor investments and prompt a growing number of large-scale initiatives in the near future," added Ostling.

BAPCO 2020

The Annual Event

10 - 11 MARCH 2020

RICOH ARENA, COVENTRY

REGISTER NOW

THE UK'S LEADING
PUBLIC SAFETY
TECHNOLOGY
EVENT

WWW.BAPCO-SHOW.CO.UK

SAVE THE DATE



DATA CENTRE WORLD

11-12 March 2020 ExCeL, London
www.datacentreworld.com

Register at

www.datacentreworld.com/networkingplus

ORGANISED BY CloserStill

LONDON
TECH SHOW

CLOUD EXPO
EUROPE

DEVOPS
LIVE

CLOUD & CYBER
SECURITY EXPO

SMART IOT

BIG DATA
& AI WORLD

BLOCKCHAIN
TECH WORLD

DATA CENTRE
WORLD



Managing rapid IoT adoption

Martin Hodgson, head of UK & Ireland, Paessler

The explosion of IoT uptake is one of the greatest technological trends since the birth of the World Wide Web. By 2025 there will be over 38 billion connected devices on the network and as many as 50 billion by 2030.

IoT devices are everywhere; everything from phones, watches, toys and even cars offer consumers and businesses unparalleled degrees of connectivity. As all forecasts point towards this trend continuing into the foreseeable future, businesses are facing the growing challenge of implementing, maintaining and securing IoT networks in order to uphold the needs of customers and meet IoT driven business outcomes.

Assessment of IoT maturity

According to Gartner, there are five levels of IoT maturity to assess how far businesses have come in their journey – and how far they are yet to go. CIOs can use this model to understand, track and maximise the business impact of IoT investments across their organisations. The five stages are: Initiating, exploratory, defined, integrated and optimising.

At the moment, most businesses sit anywhere between stage one and three. Many companies have only just started connecting everything to one central system. This means processes are no longer operating in siloed conditions, but businesses are focused on learning about how to create a connected enterprise so that they can progress to eventually working in a more data-driven environment.

As things start to evolve, companies naturally navigate their way into stage four, as integration is a crucial step to achieving IoT maturity. Companies across the globe are realising that they need to completely integrate their IoT projects into the organisation's overarching strategies and long-term goals. This is crucial in ensuring IoT infrastructure creates truly seamless, connected experiences at every level of the business.

Network reliability is key

Modern IT systems are often chaotic. It has become incredibly easy to spin up a virtual machine, download and run cloud software, or now, connect a device. As business IoT networks grow and become more complex, they risk becoming unstable if they aren't continually monitored for infrastructure or virtual machine issues. Network failure can have a disastrous effect on productivity and can significantly damage the overall customer experience as well as a business's bottom line.

When it comes to ensuring reliability, visibility and understanding are key. There are three main protocols that are used to connect the Internet of Things: Simple Network Management Protocol (SNMP), REST APIs, and XML. By gaining a stronger understanding of how devices interact, you'll be able to design more sophisticated network architectures. Likewise, mapping and tracking every "thing" that is added to the network as well as a robust monitoring system that empowers network managers to anticipate, diagnose and solve issues, often before the problem even has an impact on the end user, will save plenty of headaches in the long run.

Ensuring endpoint security

An IoT network is only as strong and secure as its weakest endpoint, so before you connect the refrigerator to central IT, be sure to have a security plan in place. Each connected device is a potential

gateway into the network, so it is integral that network managers can monitor every device (new and old) to detect rogue devices that may pose a risk. Security is a key concern of IT teams because of the importance of the data at stake and the technical complexity existing in the communication network and cloud infrastructure. There are three main targets for hackers to access the functionalities and data of a connected device: devices and hardware, cloud infrastructure that includes conceptually IoT supervisors via servers and the network of communications.

While some connected devices will be

productised and designed to fit securely into networks, others will rely heavily on customisation. With all these different device types, integration becomes a challenge. Therefore, it is critical for security reasons that all connected devices be brought under one roof so they can be accurately monitored and quarantined if need be.

Customise for the most benefit

One of the most exciting aspects of the IoT is that there is seemingly no limit to what can be connected. In terms of monitoring, this creates challenges that can be solved by creating new sensors and custom reports. This is especially

exciting in industrial settings, where data extracted from devices can be used to make business processes smarter and more efficient. This allows creative network administrators to take advantage of this opportunity to think outside the box and build custom solutions that not only solve monitoring problems but boost productivity and business outcomes.

As IoT systems continue to be adopted by consumers and businesses of all sizes, the ways we monitor our network infrastructure are being disrupted. For companies who are planning to upgrade or implement IoT systems, this begs the question; is your IT department ready?

Data Centre World

11-12 March 2020 ExCeL, London

Meet us at Booth D640



CLIMATE. CUSTOMIZED.



ONE STULZ. ONE SOURCE.

STULZ stands for precision air-conditioning of the highest level.

Whether customized or standardized, data center or industrial application, chiller or software; rely on STULZ for your mission critical cooling.

STULZ – your One Stop Shop.

www.stulz.com



Check and go: choosing a network tester plus LAN testing top tips

Dan Barrera, global product manager, Ideal Networks

LAN cable certifiers are the go-to method to test twisted pair cabling. But what is the difference between a certifier and other types of testers? And which to choose?

Put simply, the first two elements of a LAN cabling system are the cable and the connectors. Third is their installation and this is what LAN cable certifiers test.

When to choose a certifier. Quality connectors and cable will perform as advertised when properly installed in laboratory environments. In the field it's very different so your system has to be tested once installed.

Cabling standards are critical for engineers. The main standardisation bodies are ISO/IEC with the 11801 series standards and ANSI/TIA with the 568 series of standards. These define performance require-

ments for components, cable and cabling.

What is a cable qualifier? Unlike certifiers, cable qualification has no defined tests, performance or accuracy specifications in the standards organisations. Qualification is up to the manufacturer of the LAN qualifier to decide what to test, accuracy of the instrument and how to report results.

The problem is that the results from one brand of qualifier cannot be compared to another. Plus, without a definition for pass/fail limits, what does it mean when a qualifier "fails" a cable? For these reasons, no major cable or connector manufacturer will accept results from a qualifier.

Qualifier or certifier? It is not always easy to tell whether a tester is a qualifier or a certifier. However, a certifier must:

- Meet ISO/IEC 61935 and TIA 1152-A accuracy requirements, find faulty components, installation mistakes and help ensure materials are genuine.
- Have ETL Level III/IV for up to 500MHz or Level V for up to 3000 MHz for verified accuracy
- Measure NEXT, ACR-N and DC Resistance, Return Loss, Insertion Loss and ACR-F
- Specify a frequency range of at least 500MHz

Where do cable verifiers come in? Different testing equipment is used to test the different layers of an Ethernet/IP network. For Layer 1, the physical electrical/optical signalling and cabling components, a verifier is often used to check cable and terminations. They test electrical continuity for shorts, opens, crossed and split pairs. They are inexpensive and

invaluable since more than 80 per cent of problems are due to cabling faults.

However, remember! Where a warranty is required, a cable certifier is necessary as it uses radio frequencies on the cabling to measure pass/fail to ISO and TIA standards.

Layer 2 testers check cabling and Ethernet switches by counting network data frame loss (data transmission test). Unlike a Layer 1 qualifier, a Layer 2 tester does not measure electrical parameters; it measures the successful transmission of data across a cable or a network.

Layer 3 testers are similar but check performance between different networks through routers and Layer 3 switches by counting packet loss of actual network data.

In new features have been added by SolarWinds to its remote monitoring and management product which is available under licence on-premise or hosted.

N-central 12.2 now includes network topology mapping so that technicians can view and troubleshoot connectivity issues from their desks, saving time and frustration.

Another feature, disk

encryption manager, is designed to make disk drives unreadable to unauthorised users if a device is lost or stolen.

Automation manager is a feature that can now talk to and act on VMware environments, making it possible to automate VMware software-related workflows and activities.

Patch manager allows faster response to patches. SolarWinds says that the separation of patch manager from the main N-central engine better supports the rapid changes typically associated with third-party applications, enabling more timely patching.

In faster installation and troubleshooting of Power over Ethernet (PoE) devices are promised by Fluke Networks with the introduction of its MicroScanner PoE tester.

It displays the class of power available as reported by the switch in to indicate if sufficient power is available for the device in question. It uses the Ethernet Alliance certification for PoE of 0-8.



Fluke says MicroScanner PoE also provides a complete set of tools for installing PoE and non-PoE devices. They include cable wire-mapping, a built-in toner and distance-to-fault indicators to quickly track down cabling problems. When connected to a live switch port, the unit displays the speed of the port up to 10Gbps, said to be especially useful for troubleshooting slow access points. Cable identifiers can be used to track which cable goes where.

IDEAL NETWORKS

Proof of performance

Frustrated your certifier is no longer supported?



NEW

LanTEK IV

Trade-in your DTX today for a new LanTEK IV and save up to £3,000

Cable Certifier	RRP	1-4 units	Saving	5-9 units	Saving	10+ units	Saving
LanTEK IV 500MHz with PL adapters (Part No: TRADE163000 Promo code: T163000DTX)	£7,395	£5,395	£2,000	£4,895	£2,500	£4,395	£3,000
LanTEK IV 3000MHz with PL adapters (Part No: TRADE163001 Promo code: T163001DTX)	£8,995	£6,995	£2,000	£6,495	£2,500	£5,995	£3,000

This promotion cannot be used in conjunction with other offers. Terms and conditions apply.

For a 20 minute online demo please call (0)1925 428 380 or visit www.idealnetworks.net

© 2020 IDEAL INDUSTRIES NETWORKS LIMITED. All Rights Reserved.

In field technicians, even those with no DWDM experience, will benefit from the two-in-one features of the Optical Wave Expert, says EXFO.

It is said to save time and money for multiple service operators as the first device to integrate DWDM channel power validation and intelligent OTDR fault-locating capabilities on a single port. Users, says EXFO, can auto-



matically measure, diagnose and troubleshoot optical fibre links. Technicians can perform real-time channel power readings through an intuitive GUI and benefit from tuneable OTDR capabilities. Bar graph and table views are available on a touchscreen display.

EXFO says the device ensures faster service and repair compared with the "trial and error" process that previously relied on separate, less proficient devices which increased the chance of disabling nodes.

It is said to fill a gap in the market by eliminating the need for multiple instruments and seamlessly isolating problems for quick resolution.

In under a minute a new tester, the NSC-100 can identify network performance problems, says Viavi. And fixes can be made on the first visit.

NSC-100 (Network and Service Companion), a rugged handheld device, integrates passive optical network (PON), Ethernet and Wi-Fi testing.

It features an automated test process called VIAVI OneCheck, to ensure that a technician carries out all necessary tests while on site.

A hosted, cloud-based service, StrataSync, is designed to ensure that all of the company's devices have the latest software and options installed.

Viavi says NSC-100 can be used by those of any skill level and is designed to troubleshoot current and future networks and services. And it can be paired with other Viavi devices to expand their capabilities.



In big businesses are the target customers for PRTG Plus, where 50,000-plus sensors can be deployed across as many servers as required.

It is the latest version of PRTG, which was first launched by Paessler in 2003. Paessler says that, with more than 200,000 users of PRTG monitors in 170 countries, the new version is a natural progression.



PRTG Plus is available on a licensing basis, with flat rate pricing per sensor per year, billed annually. Paessler says it enables companies to monitor all their systems, devices, traffic and applications.

It runs alongside existing PRTGs which now have enhanced performance and new features for large infrastructures as well as small to medium sized businesses.



How secure SD-WAN can underpin tomorrow's agile networks

Martin Bosshardt, founding partner, Open Systems

Technology is going through an era of unprecedented change. Connectivity, globalisation, and increased competition for talent, services and customers is driving a fourth industrial revolution, in which organisations have been forced to rethink the way they use tech to underpin their growth. Emerging breakthrough technologies such as artificial intelligence (AI), the Internet of Things (IoT) and autonomous vehicles have been the flagbearers of this change – celebrated for their potential to transform the way we interact with the world.

Yet, for organisations to realise such opportunities, they need the right infrastructure in place. This requires an agile and secure network – in which aspects such as bandwidth control, app visibility and traffic routing are simplified and accessible through a single 'pane of glass'.

This is often a challenge for enterprises. Delivering that level of agility, moving away from traditional networks such as MPLS, often invokes concerns around security. With regulators already handing out significant fines following the introduction of legislation such as the GDPR, this is completely understandable.

Typically, as organisations have attempted to respond to continually shifting market demands, they have deployed a steady stream of new technologies across the enterprise spectrum. The result of this is an ever-more complex technology ecosystem. This, in turn, has an inverse negative impact on an organisation's security posture – with every degree of amplified complexity increasing its exposure. Attempts to then secure that environment further prevent future agility. And so the cycle goes on.

But with rivals waiting in the wings to capitalise on any business performance issues a competitor may experience – from a poor customer interaction to 'black-outs' – businesses can ill-afford a lack of flexibility if they want to survive, let alone thrive, in today's marketplace.

So what if delivering agility didn't mean a trade-off against security? What if

organisations could strike a careful balance between the two – delivering for the business, while safeguarding its data and end-points?

Technology such as SD-WAN creates an abstraction layer that both consolidates and simplifies the complexity and explosion of exposed capabilities at an organisation's edge.

While SD-WAN can deliver a more flexible network – in which data and bandwidth can be seamlessly shared across locations and territories – it does often result in questions

being asked around security. These concerns are typically intensified when the notion of connected devices are brought into the equation.

However, by bringing all potential contact points into one place – and by taking a software-defined approach to managing the various technical and business services that an organisation may require at its newly complex edge – they can strike that much-needed balance between agility and security. With SD-WAN now available as a managed service,

organisations need not be concerned about a lack of internal skills or expertise in running the network – the process can be easily outsourced.

In today's hyper-competitive landscape, organisations cannot afford to take their foot off the gas when it comes to deploying new technology to improve the customer experience, solidify relationships and unlock new revenue opportunities. A secure, flexible network is critical to underpin such sustained development.

TSB creates 100 tech jobs in £120m investment

TSB has pumped £120m into a new IT centre in Edinburgh, to drive forward digital banking and creating 100 new tech jobs in the process.

This move forms part of a three-year plan announced in the wake of the bank's 2018 IT disaster and will serve its five million customers. The centre will open in April and will be home to IT specialists, data engineers and analysts. TSB has also announced a partnership with computing giant IBM, to run its key banking platforms, including ATMs, digital banking and high street branch systems.

The bank was rocked by a dreadful upgrade in 2018 that left nearly two million customers without access to their accounts for several days and made some basic services unavailable for months. The fiasco, which marked what analysts described as "the most ambitious IT upgrade attempted in the country", cost TSB north of £350m and led to the departure of a host of senior executives, including chief executive Paul Pester.

TSB's board and then executives placed much of the blame on Sabis, the in-house IT provider of its Spanish owner Banco Sabadell that managed most of the bank's systems. It said in 2019 that it would take more control of its infrastructure in response to the crisis.

Whether it's V2V, V2X, tolling, parking, V2I or specialized vehicles, wireless coverage must reach seamlessly into hard-to-cover crossroads and expanses of motorway - DSRC system designers need a complete palate of options to construct a network offering continuous, balanced coverage. Mobile Mark's antennas can help make that possible.

**Antennas for Intelligent Systems...
Connections for seamless communications**

www.mobilemark.com | Email: enquiries@mobilemarkeurope.co.uk | Tel: (+44) 1543 459 555

PLUS
Fully qualified
NIC/EIC electrical
engineers and
in-house F-GAS
certified engineers
available

ONE SUPPLIER...

Providing turnkey critical power solutions,
including design, installation, maintenance & support

- Electrical installation & consulting services
- New thermal imaging capabilities
- Power ■ Cooling ■ IT infrastructure
- 3-Year warranty
- World class impartial advice saving you time & money
- Call now for a FREE site survey & health check
- Nationwide sales & engineering team, on hand 24/7
- **DAIKIN** Installer



Design & Build



Cooling



Batteries & Accessories



Generators



Onsite 24/7 Services



UPS



Data Centres



Voltage Optimisation



PDU



Racks & Enclosures

Critical POWER : When it matters most

www.criticalpowersupplies.co.uk | 0808 196 0370