APRIL 2020
networkingplus.co.uk

NETWORKING+

Predicting the future

Three tech trends with disruptive potential

Scott Dodds, Ultima, p7

Delivering business value

Here's what can help network teams achieve that goal

Mark Fieldhouse, NS1, p11

Meet Eran Brown...

Find out which other industry he'd like to work in

Eran Brown, Infindat, p15

'Remote working gives hackers new opportunities'

The mass move to work from home during the coronavirus crisis has created openings for hackers, according to global cyber security experts.

Employees have been told to stay at home to work and study because of the coronavirus pandemic, but using their laptops and accessing company data will only encourage hackers to exploit sensitive information belonging to the likes of the NHS and giant corporations.

Government officials around the world have issued warnings about the dangers of a newly remote workforce, with Britain's National Cyber Security Centre having issued a six-page leaflet for businesses managing remote employees who regularly access confidential data.

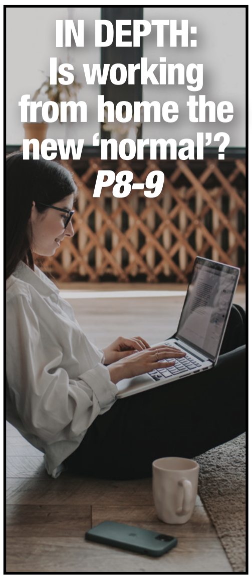
Kurt Glazemakers, CTO software defined perimeter at secure access specialist AppGate, told *Networking+* that "hackers will certainly have more opportunities" because typically, remote access to the network creates more vulnerability. "While all workers should be mindful of security issues, remote workers need to be extra vigilant," he said. "Hackers will be looking for weak links and ways into a business's network. It's important then to reduce the attack surface as much as possible so it is harder and less appealing for an attacker. Workers too need to be extra careful when they receive emails with IT-issued instructions and password resets as these are a simple way for attackers to gain access."

An annual survey commissioned by Apricorn, the manufacturer of USB drives, found that more than half (57%) of UK IT professionals believe that remote workers will expose their organisation to the risk of a data breach. It also found that apathy is still a major problem, with 34% of IT leaders saying their remote workers simply do not care about security – exactly the same as last year – which suggests enterprises are struggling to get staff to acknowledge the importance of data security.

"This year, the need for organisations to facilitate effective and secure remote working has been cast into the spotlight to an extent no-one could have anticipated," said Jon Fielding, managing director EMEA, Apricorn. "Our survey shows that while progress has been made in some key areas since 2019, some of the same risks – such as employee apathy or error – remain a problem. In these currently challenging times, when UK workers are being urged to work from home, it's all the more important that security is a priority for everyone."

As far as implementing security is concerned, Cisco Systems said the number of requests for security support to support remote workforces have jumped 10-fold in the last few weeks.

continued on page 2



IN DEPTH: Is working from home the new 'normal'? *P8-9*

Workers at risk when working from home

Continued from page 1

"People who have never worked from home before are trying to do it and they are trying to do it at scale," said Wendy Nather, a senior advisor with Cisco's Duo Security who has spent the past decade working from home in different roles.

She said the sudden transition from office to home would create more scope for errors, more strain on information technology staff and new opportunities for cyber criminals hoping to trick employees into revealing their passwords.

It has been claimed that criminals are dressing up password-stealing messages and malicious software as coronavirus-themed alerts, warnings or apps.

Many workers are moving their employers' data from professionally managed corporate networks to home Wi-Fi setups protected with basic passwords. Some firms are loosening restrictions to allow employees to access work-critical information from their bedrooms or home offices.

Fielding said that while remote working is not a new concept, the change in the work\life balance currently experienced by employees is something businesses must start to accept.

"With so many employees now having a taste for home working, it might be hard for businesses to put that particular lid back on – so they need to figure out where their vulnerabilities lie now and address them he said. ■

Smaller businesses braced for 'working from home indefinitely'

Small businesses are more likely to consider the prospect of working from home indefinitely a major challenge than larger businesses (21% vs 15%), according to a survey Hitachi Capital Business Finance.

When asked to what extent the level of technology in their business was affecting their day-to-day operations during this period of coronavirus outbreak, 30% of small businesses said they would be held back, with almost half of these businesses suggesting they may be forced to close temporarily until the virus was under control.

More broadly, the research found that small businesses were twice as likely to have concerns about their business's survival as larger ones during this period of coronavirus lockdown. The results showed that a third of small business respondents (31%) said they had concerns, compared with 19% of larger businesses.

"Uncertainty is the biggest threat to business," said Gavin Wraith-Carter, managing director at Hitachi Capital Business Finance. "Without warning, businesses have been thrust into a situation that few would ever have imagined. Businesses are now being forced to tread water as events unfold, and should be aware of the government incentives to help ease the burden in the form of grants or the CBILS. For business owners, the key is in focussing on the aftermath of events, to ensure operations can resume to normal as quickly as possible once the green light is given, and capitalise on the opportunities at hand."

The research, carried out by Hitachi Capital Business Finance, found that small businesses were twice as likely to have concerns about their business's survival as larger ones during this period of coronavirus lockdown

Wraith-Carter added that extreme situations will stretch businesses to limits and expose areas that require attention. He also said that smaller businesses, without the same resources and facilities as their larger counterparts, "will have felt this bump" the hardest. "However, many of these issues can be fixed, and these improvements will offer significant competitive advantage over the years," he continued. "Where small businesses have an advantage over their larger counterparts is the speed at which these changes can be implemented and incorporated into the core business practice." ■

Cohesity launches 'industry's first' enterprise data management app

Microsoft partner and hyper-converged secondary storage business Cohesity has introduced a new mobile application to enable access to its enterprise data management platform through a smartphone.

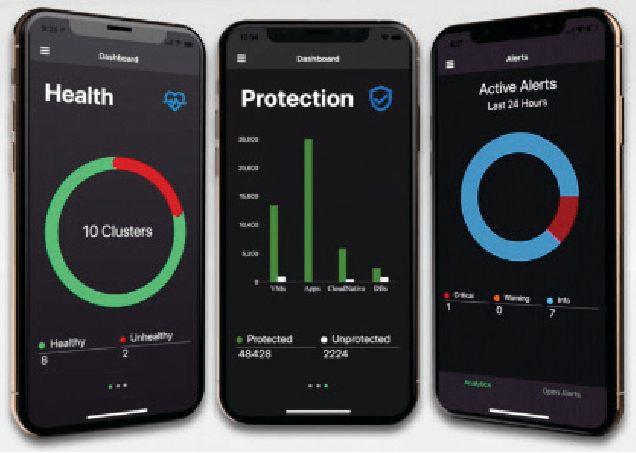
Known as called Cohesity Helios, the new service allows IT professionals to monitor the health and performance of their Cohesity infrastructure. They can also get alerts about any anomalies in the system, such as ransomware attacks.

Furthermore, the software-as-a-service (SaaS) data management offering enables users to see, manage and take action on their data whether it is located in data centres, in the cloud or at the edge. For example, the app's dashboard provides a way to see available storage capacity and view data sources. It also uses machine learning to detect anomalies and repel or mitigate ransomware attacks.

"In today's always-on business environment, companies need the ability to respond quickly to critical data issues at any time, from any location," said Vineet Abraham, senior vice president of products and engineering at Cohesity. "Cybercriminals don't just work during office hours and having a way to monitor the health of your data clusters from a mobile device 24 hours a day, seven days a week, and receive notifications that could uncover a ransomware attack in action, could save your organisation millions of dollars and keep brand reputations intact."

The Cohesity Helios mobile app is now available for download via the Android Play Store and the Apple App Store.

In 2018, the company announced integrations with Microsoft that enable customers to deploy multiple secondary apps and data on a hybrid cloud architecture. ■



Known as Cohesity Helios, the new service allows IT professionals to monitor the health and performance of their Cohesity infrastructure. They can also get alerts about any anomalies in the system, such as ransomware attacks

'Three quarters of equipment not being recycled, enterprises aren't paying due attention' – report

Only 24% of end-of-life IT equipment is being sanitised and reused, despite 83% of enterprises having a corporate social responsibility (CSR) policy in place, according to a provider of mobile device diagnostics and secure data erasure solutions.

Blancco Technology Group's Poor sustainability practices – enterprises are overlooking the e-waste problem report, produced in partnership with Coleman Parkes, also revealed that nearly 40% of organisations physically destroy end-of-life IT equipment. In addition, most businesses are keeping unnecessary data in active corporate environments that consume significant energy resources.

The findings of the research underline the role global organizations play in damaging the natural environment.

"Dealing with end-of-life equipment is part of the majority of organizations' CSR policy (91%) but this isn't being communicated or properly enacted across the business," the research report noted.

Nearly a quarter of government organisations do not have a policy in place that has been both implemented and communicated across the business. The same is true for the transport and advisory sectors, at 25% each.

"Despite the media conversation around climate change ramping up following global fires and record-high temperatures in Antarctica – and the topic taking centre stage at events like Davos – enterprises are not paying due attention to their contribution to this urgent, global issue," the report said.

It added that despite the existence of the EU's WEEE Directive and WEEE Regulations (2013), the UK missed its targets in 2018 and is one of the worst offenders for exporting waste to developing countries.

"In today's global climate, sustainability should be at the heart of every business' strategy," added Fredrik Forslund, vice president enterprise and cloud erasure solutions at Blancco.

The World Economic Forum (WEF) and the UN E-waste Coalition says approximately 50 million metric tons of e-waste are produced each year—the equivalent in weight to the total number of commercial aircraft ever built. ■

EDITORIAL:

Editor: Robert Shepherd
roberts@kadiumpublishing.com

Designer: Sean McNamara
seanm@kadiumpublishing.com

Contributors: Gerry Moynihan, Paul Liptrot, Scott Dodds, Peter Clarke, Eran Brown

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

ISSN: 2052–7373

Property debt fund backs Proximity Data Centres

Proximity Data Centres has received a £25m shot in the arm from a fund managed by Intermediate Capital Group's real estate asset management division.

ICG-Longbow has provided the capital to the UK regional edge colocation provider to help its strategic £80m rollout of 18 internet data centres.

The funding will also enable Proximity to continue its expansion, offering national capability and helping customers keep pace with their increasing data needs, according to ICG-Longbow.

"We are delighted to partner with Proximity and further our track-record of investing in the data centre sector," said Kevin Crowley, managing director at ICG-Longbow. "The company has a clear vision for the future of data in the UK and an experienced management team; providing a cycle-independent, long-term business with robust fundamentals - a key attraction to ICG," he said.

Crowley said the deal was signed before the outbreak of Covid-19 and in light of the fast-evolving situation across the globe there is even more need for Proximity's business model.

John Hall, managing director, Proximity Data Centres added: "By investing in a network of new internet edge data centres we will empower our customers to keep up with these rising demands, enabling them to succeed in today's digital-first era. Our partnership with ICG provides us with the financial firepower to rapidly develop our data centre portfolio." ■

The funding will also enable Proximity to continue its expansion, offering national capability and helping customers keep pace with their increasing data needs, according to ICG-Longbow

KOHLER-SDMO's 'most powerful' diesel gen set

KOHLER-SDMO has expanded the KD series with the rollout of four new models ranging up to 4500kVA (@50Hz)/ 4000kWe (@60Hz).

Building on the KD Series product line these generators are "designed to deliver extreme durability and ultimate reliability" in a variety of emergency and prime applications.

The modular design of the KD103V20 powered generator, the manufacturer has claimed, sets deliver unprecedented power density and unrivalled performance. Matched turbochargers are engineered for maximum power and response.

Furthermore, high ambient cooling systems ensure performance is maintained in the most extreme environments.

Fuel mapping options for either optimised consumption or emissions compliance enable the generators to be deployed globally without worry, the firm said. It has also claimed that users of the KD Series generators will find cost savings because "the line delivers the best fuel consumption" at more nodes than any other competitor. ■

Glide connects key workers

Glide Group, UK provider of ultrafast broadband connectivity and fibre infrastructure, is supporting key workers at the new NHS Nightingale hospital in Bristol.

It is providing Wi-Fi connectivity to staff accommodation, for no additional cost, as part of its existing contract with the University of the West of England (UWE). The hospital is being built on the university's Frenchay campus. Glide will provide wired and wireless broadband for the 300-800 key workers due to move in shortly.

"These key workers go above and beyond, fighting on the front line against COVID-19, so we are proud to be able to support the NHS in this critical operation, by providing seamless connectivity to key workers at the new NHS Nightingale Hospital Bristol," said Richard Jeffares, CTO, Glide Group. "We have invested heavily in our core network capacity in the last 12 months and are confident in our ability to cope with any increase in network traffic. We are pleased to play our small part in supporting the NHS and other critical workers around the country." ■

FROM THE COVER

Moving wireless forward

Mobile Mark is a leading supplier of innovative, high performance antennas to wireless companies across the globe. We've been in the wireless industry for over 30 years and have our roots in the early Cellular trials. We have grown and evolved over the years, along with the industry. Today, we benefit from enhanced design capabilities and expanded production capacity – along with a greater understanding of new and emerging markets – all of which have allowed us to become one of the best antenna developers in our field. Our customers have been our partners throughout the years. We believe in taking the time to understand our customers' individual needs. Through close consultation with clients, we are able to deliver innovative, tailored solutions that meet specific antenna requirements. Rapid prototyping capabilities allow us to take our designs from concept to reality in an extremely short time span, and to verify the performance of the antenna. A variety of network analyzers and an anechoic chamber enable us to conduct measurements up to 13 GHz, and ensure that the antennas designed meet or exceed customer requirements. We have onsite injection molding equipment and a fully equipped modeling shop staffed with skilled model makers to assist in the design phase and help us come up with a superior product – an antenna that not only meets the customer's electrical specifications, but is also very attractively packaged. Mobile Mark antennas are used in many sectors of the wireless industry. Here are just a few examples:

- Emergency services
- Commercial fleet management
- Public transport & bus management
- Smart cities & smart highways
- Remote monitoring & surveillance
- Mining & exploration
- Asset tracking & RFID

Let us know how we can help.

We understand the RF wireless world and are ready to help you evaluate your options. Contact us by email, phone or fax and let us know how we can help.

Mobile Mark Europe Ltd
8 Miras Business Park, Keys Park Rd.
Hednesford, Staffs.
WS12 2FS, United Kingdom
enquiries@mobilemarkeurope.co.uk
www.mobilemark.com
Tel: (+44) 1543 459 555
Fax: (+44) 1543 459 545

MobileMark
antenna solutions

Cisco integrates SD-WAN with Google Cloud

Cisco and Google have tightened their relationship by rolling out a turnkey package that lets customers tightly mesh SD-WAN connectivity with applications running in a private data centre, Google Cloud or another cloud or SaaS application. Cisco SD-WAN Cloud Hub with Google Cloud is a joint platform that combines Cisco's SD-WAN policy-, telemetry- and security-setting capabilities with Google's software-defined backbone to ensure that application service-level agreement, security and compliance policies are extended across the network. "For customers looking to support multiple clouds while preserving on-prem data centres, this is how they can effectively connect all their sites," said Sachin Gupta, senior vice president of product management with Cisco's Intent Based Networking Group.

TeamViewer offers 'Blizz' free of charge

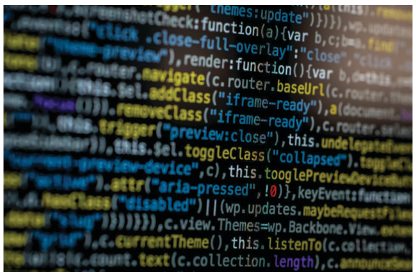
TeamViewer, the secure remote connectivity vendor, is offering its online collaboration solution Blizz to all schools and universities free of charge. The free Blizz licences can enable teachers and professors to hold interactive lessons in a virtual classroom environment for up to 50 participants via video and telephone connections to help schools manage the transition to remote learning. Blizz is based on TeamViewer's global connectivity platform and runs all major computers, laptops, tablets and smartphones. We hope that with this offer we can help simplify teaching during the coronavirus crisis," said Oliver Steil, CEO, TeamViewer.

Spy drafted in to advise NHS on app

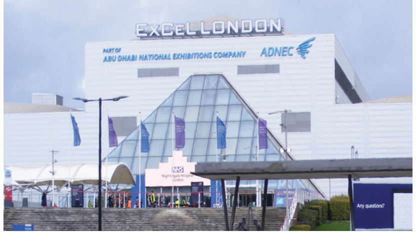
One of country's most senior spies has been drafted in to advise the government on how to secure the NHS's contact tracing app, which is a vital part of the UK's plan to lift lockdown restrictions in the coming weeks. Ian Levy, technical director of the National Cyber Security Centre, is currently advising the UK's health service on how it can encrypt data and ensure privacy. The cryptography and cyber-security expert was instrumental in the UK's decision to allow the Chinese telecoms company Huawei to participate in developing the country's future 5G telecoms network.

UK government offers free cybersecurity and coding courses

The department of education has launched the Skills Toolkit, a free online learning platform to help people pick up digital skills while in lockdown. It offers digital and numerical courses to boost skillsets, progress in work and boost job prospects, according to the government. "The high-quality and free to access courses on offer on our new online learning platform, the Skills Toolkit will help those whose jobs have been affected by the outbreak, and people looking to boost their skills while they are staying at home, protecting the NHS and saving lives," said education secretary Gavin Williamson.



Mobile Mark's LTM302 transmits at temporary hospital facilities



When NHS Nightingale Hospital's temporary 4,000 bed facilities in ExCel Centre London were set-up to fight Covid-19, Adey Electronics chose a Mobile Mark antenna to "ensure reliable and easy-to-install wireless connectivity" so that essential medical data compiled by Vision's Mobile CT Scanner Unit could be sent seamlessly to medical personnel. The company said it was able to offer a bespoke version of the LTM-302 antenna design to meet the technical and aesthetic needs of the end user and very importantly, within tight project deadlines." Mobile Mark's LTM302 multiband antenna employs MIMO (multiple-input-multiple-output) technology using two 4G LTE Cellular antenna elements for faster and more reliable data through-put.

INCA praises independent network sector

The UK's independent network sector has been praised by the Independent Networks Cooperative Association (INCA) for its significant contribution, as the country was revealed as one of the fastest growers in Europe for delivering fibre networks to businesses. It was revealed as one of five of the fastest growing markets in Europe for making new connections in the FTTH Council Europe's annual FTTH/B Panorama report. The UK also jumped two places in FTTH Council Europe's annual FTTH/B Panorama table.

NCSC launches new 'Cyber Aware' campaign for reporting suspicious emails

The NCSC has launched a Cyber Aware campaign and also urged businesses and the general public to be more vigilant online. Numerous scams have emerged as criminals seek to take advantage of concerns ranging from how to reclaim money lost on holidays to financial support when schools closed. Jeremy Fleming, director of government communications headquarters which oversees the NCSC, said the current "crisis is changing the world very fast ... the scale of activity among opportunistic cybercriminals seeking to profit from the virus should concern us all".

More police forces choose SC20 Radio

A further three UK police forces have jointly upgraded to Sepura SC20 TETRA radios, significantly improving their front line officers' ability to communicate with colleagues. Bedfordshire Police, Cambridgeshire Constabulary and Hertfordshire Constabulary made use of their joint purchasing power to equip officers from across all three forces with the new SC20 TETRA radios. In all over 1,900 radios were purchased across the three forces, to work alongside their existing fleet of Sepura radios. By using the SC20 TETRA radios, officers will benefit from powerful, robust radios with loud, clear audio, ensuring that critical voice communications can be clearly heard and understood, even in noisy environments.

Interxion and Amito in new partnership

Enterprises can now access a data centre campus located on the most connected site in central London, following a reseller partnership between Interxion and Amito.The campus, owned by the former and located between the Square Mile and Tech City, counts more than 250 capital markets participants including investment firms, financial exchanges, high-frequency trading firms, hedge funds, brokers and banks. Opening up access, UK-based Amito will now provide flexible colocation services – including quarter and half rack solutions – to enable organisations to "realise the benefits the central London campus community has to offer via tailored physical space".

Word on the web...

Whether it's the security concerns relating to Huawei or it being a cause of coronavirus, talk of 5G continues unabated. Per Lindberg, CEO at Ranplan Wireless, explains why we need to wake up to the indoor challenge synonymous with this new technology...

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

Legal eagles must keep an eye on security threats

John Higginson explains why law firms are targets for cyber criminals and what they can do to strengthen their cyber security posture

While cyber-attacks are a consistently growing threat to all businesses, law firms in particular are in the crosshairs of many cyber criminals. This is not really surprising as law firms by default hold a lot of sensitive and therefore valuable information, do a lot of time critical work and also process a lot of money, from probate settlements and conveyancing to lucrative business transactions.

This makes law firms a profitable target for cyber criminals, whether it is simply to steal the data to sell on or exploit themselves, to intercept monies and divert them to their own accounts or hold the company to ransom. According to the UK's National Cyber Security Centre, £11 million of client money was stolen from UK law firms due to cyber-crime between 2017 and 2018. Although law firms present higher value targets, they don't really need to do anything different to businesses in other sectors; they just need to set the bar higher.

A popular scam used against legal firms is Business Email Compromise (BEC), where an attacker will gain access to a network – usually through social engineering or phishing emails – and then monitor the email traffic to gain knowledge of the business relationships between law firms and their clients or suppliers. The attacker will then intercept emails, waiting for the right moment to hijack an existing conversation about upcoming payments, in order to divert funds to their accounts.

Another common attack against legal firms is ransomware, which is a fast-spreading malware that encrypts computer files. By locking these files, attackers prevent or limit lawyers from accessing their systems and typically demand payment, usually in the form of Bitcoins, in exchange for a key to unlock the files. In recent months, a new variant of ransomware has emerged, called Maze, which places a ransom note on the infected system and the company name onto a website. If a payment is not forthcoming within the timeframe demanded, the attacker then posts a small amount of the stolen data as proof. The consequences of such an attack can be severe. In addition to the business disruption it can cause, there is also likely to be a financial consequence, not to mention the huge reputational damage to the law firm and their clients, whose data may have been leaked.

Like any business, law firms need a cyber security strategy that involves stakeholders from across the business and not just IT. However, this is just the first step and a cyber security strategy comprises different strands. These should include:

Ongoing network monitoring to be able to detect any suspicious activity

Regular incident response exercises to better prepare for and mitigate / reduce impact of any incident

Ongoing risk and threat assessments which identify projects or clients likely to raise the risk of attacks and protecting that data appropriately from the outset

Incorporating network hardening measures with increased visibility of evidence sources along the 'Kill Chain' – a set of steps an attacker must work through, from network reconnaissance to the exfiltration of data – for aiding investigations when breaches occur

Engagement with clients, across the legal sector and government to share issues

Working with HR to increase staff education and awareness

A capability to deal with cyber attacks in a 'Business as Usual' fashion; this will include as a minimum an Incident Response Plan

Law firms, with access to sensitive data are rich targets and will likely sooner or later be successfully attacked, unless they identify and mitigate cyber risks. Reputational damage in the aftermath of an attack will be a key aspect, as any current or potential future clients will be seeking assurances that their data is safe while in the hands of their lawyers. Furthermore, financial penalties for any data loss may also have a serious impact as regulators seek to punish this type of breach, where the organisation hadn't suitably prepared and secured their data appropriately.

Cyber security is akin to an arms race, with businesses needing to stay at least one step ahead of the attackers. Law firms being such lucrative targets should aim to be at least two steps ahead. A good benchmark to aim for as a minimum should be Cyber Essentials Plus, which will highlight areas of vulnerability and where the most cost-effective investments should be made.

The Cyber Essentials Scheme is a cyber-security standard governed by the UK National Cyber Security Standard (NCSC) to ensure that organisations adhere to a baseline of good practice in information security and protect themselves against common internet threats. According to research carried out by Lancaster University, with Cyber Essentials controls implemented, 99% of vulnerabilities in the SMEs interviewed were mitigated showing how beneficial it can be to organisations. Cyber Essentials Plus certification offers an even higher level of assurance as it entails both an onsite and remote verification that controls have been met and is an important step toward establishing good information security practices that meet business needs. For more information go to: *https://www.contextis.com/en/blog/cyber-essentials-what-is-changing*

John Higginson, head of incident preparedness, Context Information Security

Three top technology trends that have significant disruptive potential

Scott Dodds, CEO, Ultima

Some of the more sensational, yet commonly spouted technology predictions for the next decade include the rise of the fully autonomous vehicle, a robot of some form in every household and electric cars being ubiquitous (although the latter has the greatest degree of potential). With that being said, there are certain areas that are expected to see substantial changes over the next decade within the enterprise IT space. These are; the increasing generalisation of AI, the move from application centric to data centric infrastructure, and the transition towards edge-based intelligence.

1. AI generalisation a possibility

AI generalisation, or general-purpose AI is something that scientists and mathematicians have been striving for since the 60's. Every year we get closer to this being a reality, humanity has now created AI which can beat humans and incredibly complex games with millions, if not billions of permutations. Comparatively, these models are simplistic as they only have a single goal, when you look at generalising it there are multiple goals and as humans, we must balance these. There is a mathematical breakthrough that is needed, whilst it can't be guaranteed that this will happen in the next 10 years it will be an area that has much greater focus due to the availability of computational power.

2. Data centric infrastructure

With the significant rise in virtualisation over the last decade, there has been a big change in the IT industry from being system centric to application centric. The physical platform that a specific piece of software runs is becoming less important. Virtually all businesses are nearly fully virtualised at this point with quite a few now moving onto containerisation. Micro-services use containerisation to deliver smaller, single-function modules, which work in tandem. Due to this approach, there is no need to build and deploy an entirely new software version every time you change or scale a specific function. This makes building agile, scalable applications far more feasible. The application centric system often stores data within a single application rather than having it in a single centralised location. Over the next 10 years there will need to be a greater level of interoperability between applications, giving a much better view into data, company-wide.

3. Edge based intelligence

As more of our lives become IT-enabled, there has been a proliferation of data that has been created away from the data centre. Accessing, processing and understanding this data will be one of the largest challenges for businesses over the next decade. The ability to process all of this data centrally is going to be impossible, therefore new models of data processing are going to be required. As these systems become able to adapt to change by leveraging AI, there is likely to be a substantial rise in swarm reinforcement learning; a distributed AI system. Each system will have their own environmental factors but will share knowledge between edge points allowing for a subset of data to be further processed centrally for deeper insight.

AI sentience still a long way off

According to Gartner, through to the end of 2022, data management manual tasks will be reduced by 45 percent through the addition of machine learning and automated service-level management. But that doesn't necessarily mean that AI sentience is going to be here anytime soon. We're a long way off autonomous systems that can think for themselves in a primitive way and make decisions independently of humans. It does mean, however, that humans instead will be here to manage the unexpected and the exceptions, rather than do the repetitive and mundane. AI is automating many of the manual tasks and allowing less technically skilled users to be more autonomous using data.

Driving the change

Whilst all of these trends will be influenced by a number of different factors which have a huge influence on timescales, some of them can already be seen in prototype today. However, over the next decade, there will be vast leaps forward in computational power which will most certainly help to enable these.

One thing is for sure, a growing ability to manipulate data is set to propel business operations forward. Whether its productivity and efficiency savings or greater innovation opportunities, data is advancing organisations in a tremendous amount of ways and helping to solve a large variety of problems. The effects of this will only become more pronounced as these trends gain maturity and adoption gains critical mass. Organisations that are able to harness these capabilities effectively will be able to differentiate themselves and drive significant value.

Will working from home become the new 'normal'?

The arrival of Covid-19 has meant we have no idea when – indeed, if – we will go back to the once familiar office life. Robert Shepherd investigates

The opportunity to work from home is one we all grasp when it arises. Imagine: more enjoyable down time, a 5km run instead of a commute, drinking decent coffee and the dulcet tones of BBC Radio 4 keeping the world up to date with what really matters in life. Alternatively, there's the option to find a smug people-watching area of that village coffee shop or gastro pub and work there for an hour or two. Added up, it makes for better mental health. Anyway, that's enough about me.

However, we tend to work from home/ remotely because we are afforded that luxury from time to time – very different to the enforced remote working we are currently experiencing, courtesy of Covid-19. Now, most us couldn't go to the office, even if we wanted to.

Businesses – those lucky enough to have remained solvent during the ongoing pandemic – have had to suddenly embrace this change. That means anything from a handful to tens of thousands of people all logging in to the same network at different times of day and in different countries.

Apart from a decent broadband connection and network access, employees are now having to adopt technology they possibly may never have heard of before. One area that has seen exponential growth and uptake is video conferencing with Zoom Video Services evolving from a relatively niche app as recently as early March to one that has added billions of dollars to its market capitalisation. Zoom has seen its market value increase exponentially, reaching $42bn (£34.2bn) by the end of the month. Between the beginning of February, when the virus was only beginning to go global, and 23 March, Zoom's share price more than doubled from $76.30 to a peak of $159.56.

One company that claims to have seen a surge in demand for its services is remote connectivity platform TeamViewer. "So much so, that the spike in demand has mirrored the geographical line of the spread of Covid-19," says CEO, Oliver Steil. "Companies across the globe are taking a crash course on home working at the moment."

Of course, most companies today are set up for remote working and Richard Fogg, chief executive officer at technology PR agency CCGroup, says his company was ready for the challenge.

"Our business has always been set up to enable people to work from home – and most of us do, at least one day a week," says Fogg. "While we miss all being together under one roof, we have been able to adapt to rules around social distancing relatively quickly. Over the past few weeks, we have done what we can to maximise face time with each other – through collaboration tools like Microsoft Teams and Zoom. We have tried to remain as positive and as inclusive as possible to support each other through such anxious times."

Fogg adds that many 'normal' working practices as possible is also important in reducing this anxiety and the company has continued with its regular 'Lunch & Learn' training sessions and weekly team meetings as virtual meetings".

"Perhaps more importantly, we have also looked for fun ways to enjoy our collaboration tools, so we can continue to laugh and joke together," he continues. "We have a range of virtual social activities like team lunches, an Easter party, games nights, quiz nights and even a virtual game of 'Through the Keyhole.' Like any business, we have always relied on strong connectivity to function. The global pandemic has made this connectivity even more critical as we look to offset the impact of social distancing, maintain efficiency, promote inclusion and preserve mental wellness."

While many employees will have access to the luxury of video-calling, numerous things need addressing first, such as cybersecurity.

According to the 2020 Zero Trust Progress Report published by Cybersecurity Insiders and Pulse Secure, the software-defined secure access vendor, 72% of organizations plan to implement Zero Trust capabilities in 2020 to mitigate growing cyber risk, but nearly half (47%) of cyber security professionals lack confidence applying a Zero Trust model to their secure success architecture.

Add to that a report from Kapersky Lab, the Moscow-based cybersecurity and anti-virus provider, which found that 90% of corporate data breaches in the cloud happen due to hacker attacks that target employees. Is that because humans, by their very nature, will tend to be more relaxed and browse personal sites at home, which might not be secure? Yes, according to new research conducted by NordVPN Teams, which revealed that 62% of people are using personal computers (or other personal devices) to work from home.

"It is concerning because most private laptops are not equipped with proper security software," says Daniel

Markuson, the delivery expert at NordVPN. "Therefore, more and more companies turn to VPNs (virtual private networks). For example, recently, our business solution NordVPN Teams saw a 165% usage spike and almost a 600% increase in sales overall. It can be related to companies encouraging their employees to work from home in the safest manner possible."

Markuson says employees forced to work remotely during the quarantine means companies are now more vulnerable than ever. "When in the office, everyone uses the same Wi-Fi connection, so it's easier to ensure secure communication," says Markuson. "To have a safe connection when working remotely, a VPN is needed. It encrypts users' internet traffic and protects their online identity. A VPN effectively grants employees working from home secure access to servers, systems and databases that otherwise only could be accessed at an office. With a VPN turned on, no malicious actors can snoop on what people do online."

The VPN field is a crowded one "but don't take short cuts" and seek advice from security experts," warns Jonathan Whitley, director of northern Europe at WatchGuard Technologies.

"It is too important a decision to get wrong," he adds. "Ensure that users are not just dropped on the corporate network; using VLANS (virtual LANs) will help mitigate against a potential breach.
Also don't allow RDP (remote desktop) functionality to run natively on the internet and ensure you control access with a VPN and MFA (multi-factor authentication)."

However, there are skeptics, even detractors, when it comes to VPNs and Kurt Glazemakers, chief technology officer (CTO) software defined perimeter at secure access IT vendor AppGate says that lots of questions still need to be asked. "From a cybersecurity standpoint, there is much to consider about when implementing a work from home policy, including: can the company's network handle a large increase of workers who must access resources remotely?" he says. "If all remote workers are trying to access the network through a single VPN ingress point, how will that impact network bandwidth and latency? Once workers connect to the network, what checks are in place to make sure only those resources needed are accessible?

In fact, Glazemakers isn't convinced that VPNs are the answer because "the technology is rapidly showing its age and lack of agility" at the most critical period in recent memory.

"It simply isn't fit for purpose for the ways in which workers need to access network resources today," he continues. "This is especially true in a time of crisis when the number of users may increase significantly in a short period of time. VPN solutions are hardware-based and have limited bandwidth, making it difficult to scale based on demand. Also, it takes a lot of time and money to implement expansion of VPN systems. We're seeing many organisations now looking at software-defined perimeter (SDP) technology to provide agile and highly elastic capabilities enabling secure remote access while reducing their costs. SDPs are much better for network administrators too as they can quickly and easily manage user access. This helps to maintain security while enabling productivity."

Another vendor with a focus on keeping us all safe is Storage Craft, which provides data management, protection and recovery solutions, "with the mission to protect all data and ensure its constant availability".

Florian Malecki, the company's international product marketing senior director, says the current situation has not only forced businesses to build remote working environments, they've had to do it in a very short space of time.

"Moving millions of employees, their computers (corporate or personally-owned) and their data from a secure office environment to their homes with such short notice presents enormous data security risks for businesses," he says. "From technical glitches and accidental human error, to malicious and damaging ransomware attacks, caution must be taken when transitioning such large volumes of data."

While security is – quite rightly – a core consideration when kitting out staff at home, how does it impact performance?

"Along with increased security risks, performance could also be impacted due to employee devices not being able to cope with the various inhouse security applications they're expected to run," says Whitley. "Business must provide centrally managed lightweight client applications which deliver enterprise grade security, while also allowing employee productivity to remain high. Cloud-hosted firewalls can also help to load-balance VPN traffic destined for your HQ and scale to accommodate the connections your company requires. Deploying these solutions will provide Management teams with the confidence their corporate assets are safe and thus focus their time of proactively driving business."

Simon Kelf, co-founder and chief executive officer (CEO) of full-service managed IT support firm BCN Group says the amount of pressure is "entirely dependent" on how well equipped they are for staff to work remotely. "Questions business leaders need to ask themselves now is if the government did order everyone to work from home, could they facilitate it?" he adds. "It is the time to review and assess your requirements quickly and if you have gaps in your business contingency planning and infrastructure, they must be filled without delay."

Indeed, it hasn't been seamless for all concerned. Aryaka's 2020 State of the WAN survey has found that the biggest challenges to voice and video performances are set up and management of underlying network infrastructure (48% of those questioned), while 43% complained of a lag in communication. Poor voice quality was reported by 39%.

Vannina Kellershohn, vice president of enriched interactions and collaboration business unit, Orange Business Services, says one sector that has seen a significant impact is customer support. "Many call centres have been closed and staff is now working remotely, which could therefore be difficult for them to access their environment to offer customer support functions," says Kellershohn. "However, Orange Business Services has been helping customers to migrate their contact centres to the cloud, enabling them to continue business as usual."

Kellershohn says moving forward we will see a wider acceptance of remote working across the board and increasingly flexible working policies where they are appropriate. "The current pandemic has illustrated that with the correct technology and infrastructure in place, remote working can be highly successful and in fact, has not come with the downsides that more established and traditional companies may have feared."

Swedish video and audio specialist Konftel has been rewarded with favourable column inches during the pandemic as social media and news channels showed its kit being used in 10 Downing Street by the prime minister Boris Johnson and his colleagues, as they keep in daily contact with world leaders via video link. "We supplied the C50 800, which all the pictures are showing - and our huddle room solutions were supplied for smaller room use," says Jeff May, regional sales director at Konftel.

"It's '100% proof' that remote working is the future. "Many organisations will adopt this more and more as the norm – this period will convince the most sceptical of employers that home working is a productive, trustworthy and reliable option," he continues. "Expensive real estate and office space might well be (probably will be) downsized as more staff are encouraged to work from home and then realigned to have more meeting spaces, allowing for social distancing, with their remote working colleagues, customers and suppliers. Staff will want it, having experienced it and seen the work life balance it offers. Travel and meetings will be less desirable for everyone for a while yet, perhaps a long time for some."

Hira Ali, chief executive officer of Advancing Your Potential and author of Her Way to the Top, says "there is a prevalent organisational culture that values presenteeism highly" without realising that an employee physically working within an office doesn't improve results or productivity. "The use of Zoom, Skype and Microsoft Teams provides more flexibility, convenience and safety than physical spaces, since interactions can be planned on your schedule," she says.

Where employees are based is one thing, but businesses around the world will need to make some other big decisions, too. Robert Staines, a data centre management specialist, questions what companies will do going forward with regards to renting office space now that it's become harder to justify.

"So, at present a lot of companies have had to make the adjustment to allow most staff to work from home," he says. "Any of those companies noticed any real difference in productivity (something I know a few old school managers always feared)? Could this be the beginning of the decline for office buildings? Imagine the potential savings and reduced overheads, the terror threats instantly reduced for commuters no longer needing to travel so much, the reliance on the transport infrastructure virtually gone, the list goes on. So, who's really happy with all of this, apart from missing physical people? Count me in."

NHS staff and other key workers have – quite rightly – made 8pm on Thursday nights their own, as we all stand outside our properties and applaud their life-saving work and general hard graft. However, Fogg says it's right that we acknowledge the people who make working from home possible.

"There is little wonder therefore, that telecoms network engineers and their partners are currently regarded as keyworkers, alongside doctors and nurses, in helping us overcome Covid-19," he says. "While their efforts are not as immediately visible as our incredibly brave and unconquerable healthcare workers, they still deserve our thanks and adulation all the same. The task that we collectively face would be all the more daunting without them – both socially and economically."

We're all still in the dark as to what the 'new normal' will be once things even begin to resemble what they were just a few months ago. However, we can all agree that the work/life balance we see in the likes of Sweden and Australia – and have long been envious of - is coming to our shores, thanks to a nasty pandemic. Bosses will be taking note. ■

"A VPN effectively grants employees working from home secure access to servers, systems and databases that otherwise only could be accessed at an office."

Daniel Markuson,
delivery expert,
NordVPN

Low-power WAN network enables logistics solution

Peter Clarke, sales and marketing director at WND UK, explains how we can connect 20 million devices by the end of the year

PIN IoT is just one of new breed of logistics businesses finding innovative ways to tap into the potential of the internet of things (IoT) for enterprise. It offers a simple yet powerful logistics tool for businesses that rent out containers for waste management services. By combining real-time container tracking with a purpose-built app, it gives its clients a live view of their entire fleet of containers. This delivers multiple benefits, including minimising losses, maximising availability, and improving operational efficiency – ultimately saving both time and money.

The PIN IoT solution works by fitting waste containers with discreet, low-powered tracking devices that can send location data to the cloud – where it can be accessed via the app. One key challenge they faced was that, to make the project viable, they needed a low-cost and low-power network to send the data.

Assessing the network needs for IoT applications

When it comes to the networking requirements for IoT applications, it is not a case of one size fits all. Some applications, such as smart security cameras, need to send a lot of information and therefore require high data rates. Increasingly, however, companies like PIN IoT are developing solutions that deliver value by collecting and sending lots of small bits of information. Other examples include smart meters, e-health sensors, and temperature sensors – all of which require just a few bits of data (not megabits or megabytes) to do their job effectively.

Applications which can function with low data rates do not need the same high-speed networks that are designed for speech and video. Using cellular networks like 4G and 5G would only add unnecessary cost and complexity. Other solutions might require a combination of different data speeds. With smart security, for example, motion sensors (running on a low bandwidth network) could send a signal to the cloud, prompting the cameras to transmit video footage (on a high bandwidth network) when required.

The viability of a large scale IoT solution like PIN IoT depends largely the cost of delivering the service, which comes down to two factors: the cost of the devices, and the cost of sending the data they collect to the cloud. Therefore, matching the right networking solution to an IoT application is crucial to determining its success.

The role of low power wide area networks

The solution to PIN IoT's connectivity challenge came from Sigfox, a low power, wide area network (LPWAN) technology specifically designed to provide connectivity to devices that require only intermittent connectivity and to transmit small amounts of data. A major benefit (alongside cost saving) is that Sigfox is much less power hungry than other cellular technologies. This leads to a significant increase in battery life and means that the devices can be smaller and more discreet. This gives Sigfox a clear role to play in the increasing number of IoT applications where battery life, price, security and ease of deployment are key factors.

Sigfox in the UK

The UK Sigfox Network Operator, WND UK, has implemented a fully operational network achieving over 90% population coverage in just 18 months. It is already establishing a firm foothold in the low power, wide area network space. WND UK now has over 130 channel partners and the list is growing by the day. These companies are using the network for real-world commercial applications – from metering to flood detection to legionella monitoring.

PassivSystems is just one of many companies putting the WND UK network to good use. A supplier of smart hybrid heating systems, it has already connected 3,000 meter readers using the Sigfox network, enabling accurate billing for residents. This leverages another major benefit of the Sigfox network. LPWAN offers much greater penetration than other cellular networks, so is better suited to applications where the device (such as a gas meter) is tucked away in a hard-to-reach location.

The future of the global IoT market

While there are tens of billions of IoT connected devices operating around the world today, the market is still in its infancy. Market analyst firm Statista has forecast the global market for IoT end-user solutions will reach $1.6 trillion by 2025 (from just over $200 billion in 2019).

Having access to a cost-effective low-power sensor data network is sure to open up opportunities for more companies like PIN IoT to bring innovative solutions to market, especially as more high-volume, low bandwidth IoT applications begin to emerge in different sectors. As well as transforming logistics and transportation, likely areas of development include consumer electronics, manufacturing, healthcare, and retail. PIN IoT and WND UK are among the innovative, tech-savvy companies leading the charge.

WND UK has implemented a fully operational network achieving over 90% population coverage in just 18 months

Working from home: Cybersecurity tips for remote workers during COVID-19

Alan Hayward, sales & marketing manager at SEH Technology UK

With most of us wondering how long it will be until lockdown measures are relieved and we can return to work, it's apparent that enforced social distancing measures may need to be practiced intermittently through to 2022, to stop a resurgence of the virus. Fortunately, digital technologies have ensured that most people can complete their regular duties from home, during this difficult time and beyond. That being said, remote working comes with its risks, mainly in the form of cybersecurity threats. Cyber hackers are on the hunt for network vulnerabilities and opportunities to exploit valuable data, which not only puts employees' own privacy at risk, but could result in company security breaches too.

Most employees will continue working from their home, where they can secure their Wi-Fi, but others may use unsecured public Wi-Fi networks. This will open up opportunities for cybercriminals to breach the network, track internet traffic and potentially collect confidential data. It's also important to consider the personal devices that employees may be using at home. These will often lack the same level of security tools built into corporate devices, such as antivirus software, customised firewalls or automatic online backup tools. As a result, this can increase the risk of malware finding its way onto devices, leading to information or data leaks.

Coronavirus-themed phishing scams and hacking campaigns are also on the rise, leveraging fear and taking advantage of workplace disruptions. With social distancing set to become a semi-permanent fixture in our daily lives, organisations and employees need to continue pursuing factors that will help reduce the number of threats and allow them to remain productive when working from home.

Setting up firewalls and antivirus software

Firewalls are a strong defense to prevent threats entering the network, by creating a barrier between employees devices and the internet with closed ports of communication. The device will usually have a built-in firewall and employees need to ensure that it is enabled on the device they are using at home. For added protection, there are plenty of other third-party firewalls available too. It is also important to consider antivirus software as the next line of defense, as it detects and removes any known malware from the employee's computer system. Not only does this software eliminate the virus, but it also prevents any potential threats from infecting the device in the future.

Updating devices and data back-ups

Updates to device software can often be time consuming or tiresome, but they are really important when employees are working remotely. These updates will often include patches for security vulnerabilities that have been discovered since the last version of the software was released. During this time, employees should also ensure their data is backed up. Data can easily be lost due to a number of reasons, such as human error, hardware failure or cyberattack, but ensuring that their data is backed up either in the cloud or external device will ensure peace of mind for both them and their organisation.

Controlling access to corporate systems

Virtual Private Networks (VPNs) allow remote employees to access the organisation's IT resources securely, including email or file services. VPNs create an encrypted network connection that authenticates the user or devices, and secures data in transit between the employee at home and the organisation's services. Not only do VPNs enhance security, but it also allows for better performance and efficiency of the network. If the organisation is already using a VPN, it needs to ensure that it is fully patched. It may also require additional licenses or bandwidth due to the increased number of employees working from home.

Securing removable media

USB dongles can contain huge amounts of valuable or sensitive data. They can also easily be misplaced and when inserted into an organisation's IT systems, malware can be introduced. These dongles may be openly shared amongst remote workers, making it more difficult to track what they contain, where they've been, and who has used them. Dongle servers are a popular choice as they allow USB dongles to become available over a network. This means copy-protected software can be used as normal, but users don't need to connect the license dongles directly to their client, minimising the risk of data breaches and attacks on the organisation's network.

Managing these risks

For most people, remote working is the 'new normal' which exposes fresh cybersecurity risks that need to be managed. It's important for organisations to access the risks associated with their employees working from home and remotely accessing the network. The resulting cybersecurity policies should determine the processes that need to be put in place to minimise the risk of attacks or data breaches. In addition to the precautionary security measures, employees should be trained regarding the use of their devices when working remotely. This will include secure storage and management of user credentials or passwords and how to report a cybersecurity incident, as well as building an awareness of the risks and the ways that they can be prevented.

www.seh-technology.com

Why APIs help network teams to deliver business value

Mark Fieldhouse, general manager EMEA, NS1

The desire to be agile and respond quickly to changes, drives enterprises to use APIs that allow disparate teams to communicate efficiently. The objective is to create open channels that are accessible to internal, and external audiences, and deliver interoperability at such a level that it automatically creates a competitive edge.

The network engineering department spends too long deploying, configuring and managing network services, all too often using manual processes. This is increasingly at odds with the demands being made of network management, particularly when it comes to IP Addresses, DNS and DHCP, or enabling the development of new architectures for modern apps.

Automation can help keep network teams ahead of the game so they can embrace APIs and fuel their own agile initiatives.

We regularly work with enterprises that benefit from modern deployment models, using APIs that not only drive network automation but empower multiple groups to rapidly obtain appropriate changes to core network services (i.e. DNS, DHCP, IPAM). Network engineers working with gaming companies or retail organisations, for example, need tools that are designed to suit their skill sets, and these enterprises, keen to avoid spinning up infrastructure unnecessarily, are embracing 'lite tech' products and containers.

So, what can engineers gain from catalogues of API's available from companies like ours? Create networks, configure IP ranges, and manage IP allocations. Create and manage DNS zones and records, including large zone imports, record QPS reporting, and configuring DNS record metadata to incorporate traffic steering policies, global load-balancing requirements, and real-time infrastructure conditions.

Single source of truth

Automate service discovery by ingesting data from microservices and/or cloud environments (e.g. Consul DNS, Kubernetes, etc.) to maintain a single source of truth about IP allocations and DNS records.

Automatically assign IPs to new devices by managing DHCP scopes, scope groups, leases and IP reservations for new devices (e.g. printers, VoIP phones, etc.) as part of the provisioning template for new branch locations.

Automate deployment of lightweight, local DHCP and DNS server containers at branch or remote locations for on-going IP assignments for employee laptops and mobile devices.

Better security

API's are increasingly used to gain visibility of the multiple threats facing every enterprise. APIs extract data from on-premises security, logging products, or data from infrastructure to highlight vulnerabilities. Using this information, action can be taken to protect the enterprise, whether it's to defend against malware or divert an attack on the DNS.

Some APIs, including our own, can update DNS metadata with information about the back-end infrastructure that results in superior reliability and resilience. Without APIs it's very difficult to bring together the DNS/IP administration and change management tasks with the global traffic load balancing tasks to improve end-to-end application performance.

API performance

The shift to using APIs to automate deployment, manage changes, and improve application performance means that API performance becomes an increasingly important criteria for success. APIs exposed to large numbers of requests will have the same requirements for scalability and performance as any web applications. Therefore, simply bolting on a set of RESTful APIs to legacy DNS-DHCP-IPAM appliances (or their virtualised equivalents) won't guarantee a positive automation experience.

Another significant benefit of having a high-performance API is that DNS, DHCP, and IPAM capabilities can become infrastructure-aware. For example, metadata updates (such as latency, up/down status of load-balancing) can be made in real-time, thereby dramatically reducing the time it takes for DNS responses to reflect real-time conditions.

Enterprises must start thinking about their own development processes with an 'API-first' mentality. APIs underpin the development, deployment and updating of applications much more quickly than previously and have the potential to revolutionise network operations. Without automating the network DNS, DHCP, and IPAM changes cannot be made rapidly and in a repeatable fashion, so the network has to become part of the software delivery process.

If we consider the many different customers that are using our own APIs and integrations, we can see that bank employees now get access to accurate IP address information without manual intervention from a network engineer. That DevOps teams in large technology firms can deploy application changes into production without errors introduced by the manual update of DNS records. In fact, across oil and gas, retail, technology and multiple other industries, APIs are enabling network engineers to collaborate with colleagues to create applications and deliver services that are setting their organisations apart and providing business value.

From Wuhan to Weybridge and Woking

The current global health crisis has provided the British education sector with the biggest challenge it has ever faced. Robert Shepherd asks how well-equipped Surrey institutions are for home learning

A Twitter poll recently conducted by consumer champion Martin Lewis found that 60% of respondents were the same or better off financially as a result of the coronavirus pandemic. Had Amazon CEO Jeff Bezos taken part, he would have been in that 60%, too. To rub it in, the American entrepreneur added a mere $24bn (£19bn) to his fortune as the demand for online shopping sent Amazon's stock price to an all-time high, propping up the retail sector in the process.

At the other end of the spectrum, a number of sectors face challenges they've never seen before. Take the domino effect in education: schools closing, working parents having to balance doing their jobs with home-schooling, schools having to resort to emergency teaching, furloughing 'non-essential' staff. You get the picture.

While the closure of schools and when they should re-open are moot points at many a 10 Downing Street press briefing, one thing less talked about is just how schools, colleges, universities and any other academic institution you care to mention are progressing with what's been the most debilitating 'attack' on our freedoms since World War II. Even from 1939-1945, most schools were moved to country hotels, homes and estates in that very British manner of keeping a stiff upper lip, keeping calm and carrying on. With that in mind, you could argue that the true litmus test of how prepared schools are for 'war' is now.

The good news is august tech firms have done their bit by offering up key services for free. TeamViewer, the secure remote connectivity vendor, is providing schools its Blizz solution at no cost. It allows teachers and professors to conduct interactive lessons in a virtual classroom environment with up to 50 participants, either via video or telephone.

However, it's one thing having all this at your disposal, but you also need to be experienced and skilled in using it.

Sarah Evans (pictured above), head teacher at Weston Green School (WGS) in Thames Ditton, says a sound remote/distance learning strategy was already in place at her school, courtesy of parent company Bellevue Education.

"Due to the significant investment in computing hardware and a group wide strategy to utilise the Google toolkit, we were well prepared to extend this to remote learning at very short notice," she says. "Being a member of a national group of schools, many meetings, discussions, shared training etc. had already been achieved through the use of Google Meet and Hangouts as well as consistent use of Google Drive to share documents."

Evans adds that many staff and children were already familiar with this system and so "the extension to remote learning therefore focussed on upskilling all staff, sharing skills and techniques around live and recorded lessons" and getting the balance right for children in terms of their overall experience across the week.

"We are a school with children from three-11 and therefore the ways in which the Google toolkit has been utilised demanded a progressive and differentiated approach across the school," she continues. "We have also taken time to add in apps which will support ease of use, such as Kami and Jamboard and trained staff to use these."

Sir William Perkins's School (SWPS) in nearby Chertsey was also prepared for distance learning, says senior deputy head Sherry Husselbury. However, it wasn't without its teething problems.

"We had a system for uploading work via Firefly (a learning platform) which was in place to ensure that learning could continue on 'snow days' or other weather extremes," she adds. "This would have been successful in the short term but actually proved to be catastrophic as the system 'fell over' on the first day of the school closures because of the high volume of traffic experienced globally. They dutifully worked up their capacity in a very short time (two days) but we had to abandon that process as our #1 system."

Fortunately, just before the closure, the school's IT network support manager recommended switching over to Microsoft Teams, which was enabled across SWPS. The school then quickly wrote some protocols and had assemblies to introduce it to students. "I am staggered at the rate colleagues were able to upskill in this previously unused area and in no time, it was in wide use across the curriculum," adds Husselbury. "Other tools such as OneNote, Explain Everything and other apps have been used with great success too."

Foresight seems to have been a wonderful thing, with some schools benefitting from having put certain technologies in place much earlier than others. Karl Rivers, director of IT at Royal Grammar School (RGS) in Guildford, says his school put in plans in place for remote learning a few years ago.

"In 2016 RGS began providing all teachers with Microsoft Surface as their primary computer and removed desktop computers from all classrooms," he says. "At the same time, we moved all our data to services within the Microsoft 365 cloud. The result was that the RGS already had the technology in place to work remotely, and this provided us a smooth transition into distance learning with which has been extremely successful under such difficult circumstances."

Rivers says Microsoft Teams has been key at his school, describing it as "not only the bedrock of RGS' distance teaching and learning provision", but it also provides a platform for all school communication and technical support. "Teams has provided us a single application through which all staff and students can communicate, carry out lessons, and connect the whole school community," he adds. "From an IT perspective, teachers and students can instantly communicate with the IT team and access remote support."

Hugh Thomas, computing team lead at Cleves School in Weybridge, says staff and pupils are "well-versed" with the use of the Google Classroom platform and so "it made sense for us to use it as a teaching method. However, it's been a very different story with video technology. "We stayed away from video conferencing between staff and students as this opened up too many issues regarding safeguarding for both parties," adds Thomas. "It does also lead to issues for some pupil premium students who may not have access to the technology required." Cleves uses Securly software, designed for school platforms for its filtering of appropriate material.

The approach to video communication is mirrored at SWPS as staff members were advised against Zoom and Houseparty – both now firmly established in the lockdown lexicon - due to the inability to monitor the provision in-house, not to mention the much-publicised security concerns associated with the platforms, according to network IT manager Luke Halestrap.

"Teams allows the school to run exports of conversations centrally should any concerns be raised, along with being able to block communication with external sources," he adds.

The importance of cybersecurity cannot be emphasised enough, especially when minors are concerned and Evans says when at school, and this holds different connotations when remote learning, so amendments to policy as well as guidance for families and staff have all been issued to ensure children are protected as far as possible.

"Our safeguarding concerns were around reliance on firewalls in family homes rather than school, ensuring parents are in the room when teachers have a 1:1 live session with them," she adds. "Set ups protocols for both staff and parents."

For Rivers and RGS, the key focus has been on student safeguarding, with a view to "making sure that we provide students a safe online learning experience" which replicates the hardworking but friendly atmosphere they get on site.

"For example, the school can manage who has access to features like chat and video meetings, regardless of their location or the device they are using," says Rivers. "We can also set a range of policies to ensure that the type of content shared within the school system meets acceptable standards and that where it doesn't, we can react to it appropriately."

Foresight seems to have been a wonderful thing, with some schools benefitting from having put certain technologies in place much earlier than others

Universities up and down the country are facing similar challenges as students grapple with alternative methods of learning and the security issues synonymous with it.

Kevin Curran, senior member of the IEEE and professor of Cybersecurity at Ulster University says the "rapid move towards remote working" raises the risk of increased data breaches for institutions such as universities. "Indeed, they are very similar to other commercial enterprises," he says. "Universities will have built policies and procedures over many years which protect staff, students and the organisation's infrastructure. However, unless a significant percentage of staff and students had previous access to proper remote access technologies, there is a real risk of them making bad choices."

Curran says one of the biggest risks is an increase in ransomware attacks, which, he says "are a serious problem" right now. "Employees may be using non-standard email or messaging systems which fail to properly filter out the emails that carry the threat," he adds. "University staff could also be tempted to use public Wi-Fi without a virtual private network (VPN)."

VPNs secure data between remote workers and core systems and Curran says, "in an ideal world, organisations would have a 'zero trust' network system deployed". Notwithstanding that, he says this can be difficult to implement in response to Covid-19, "as it should ideally be rolled out in a phased manner", which entails pilot projects and tweaks in a safe environment before deployment. "However, if an institution has not yet embraced the concepts of privileged access and least privilege, or still uses shared accounts for access, then zero trust is probably not going to work," adds Curran.

When it comes to staff mobile devices, Curran points out that mobile device management (MDM) is essential to mitigate risks and some software now enables devices to connect to a cloud-based solution which bolsters the existing support.

"Users can log in to these software's with many different types of accounts, including those which allow multiple users who share a single device to have full control over the Windows Store, VPN, device-wipe capabilities and configuration of enterprise data protection policies," says Curran. "It also separates personal and corporate data, which can be a useful feature in heavy bring-your-own-device (BYOD) environments and you can choose between data mining (DM), traditional Active Directory (AD) or group policy models."

While University of Surrey has been conducting lectures, seminars and "face-to-face" appointments using video platform Zoom, technology was already a key part of its modus operandi way before Covid-19 made its way from Wuhan, China to the leafy home county.

"It certainly feels like a self-taught online degree rather than the whole university experience," says Dionysia Savvas, one of its law undergraduates. "We already have our lectures recorded so we can watch them from home using our university portal. Many materials continue to be provided online such as lecture slides or seminar worksheets. Our reading is also given online through the year anyway."

Students submit work via its portal, which is accessed by module conveners – and lecturers at the university have given students the option to set up video calls for feedback on work. However, Savvas says that has proved difficult for many students who lack the necessary resources. "The university has offered for some students to borrow laptops and other equipment if need be," she adds.

"It certainly feels like a self-taught online degree rather than the whole university experience."

Dionysia Savvas,
law undergraduate,
University of Surrey

Despite the clear disruption to her first year of university life, Savvas says the online lectures are useful because students can communicate with the lecturer and ask open questions to other online participants. "There are some technical difficulties which have delayed certain lectures but other than that it has been simple to use," she says.

Now, it's time for that inevitable question: will schools, colleges and universities embrace distance learning going forward even when there is no obvious need?

Thomas says whilst "schools are probably now in a better place than they were regarding having researched methods of engaging with students at home", he's not convinced that this will replace the personal input that the student receives in a classroom setting whether from a teacher, teaching assistant or peer.

"Many parents I'm sure will have been surprised by the level of support students need (even high achieving) to attain quality outcomes," he says.

"In unusual and special circumstances - the use of technology with distance learning can clearly have a positive impact on students who for whatever reason can't be in school however this doesn't supersede the role of the teacher in a classroom. Especially for primary school/vulnerable students, numerous safeguarding issues must be considered in the use of technology."

What about in higher education? "Personally, I think that the online lectures are useful, but they are not as engaging as actually being present in a physical lecture," adds Savvas. "I find that learning from home is not always efficient. I like to keep my learning and living spaces separate to maximise concentration and minimise distractions."

When it comes to the pros of distant/remote learning, Savvas says it's often easier for students who would ordinarily have to travel to the campus. However, "the cons are simply that the physical presence of being in a lecture or seminar is deducted - it is possible to replicate this atmosphere, but I find it difficult".

Distance isn't going to replace the classroom or lecture hall as a preferred method of teaching and learning – certainly not in our lifetime – but it's reassuring to know it's there when parents and children need it. ■

Types of data centre architectures

Marc Garner, VP, secure power division, Schneider Electric UK&I

Today Internet use is trending towards bandwidth-intensive content and an increasing number of attached "things". At the same time, telco and data networks are converging into a cloud computing architecture. To support the needs of IT today and tomorrow, computing power and storage is being inserted out on the network edge in order to lower data transport time and increase availability.

For many enterprises, there is also a need (or desire) to keep some business-critical applications on-premise. This allows for greater levels of control, meeting regulatory requirements and availability needs. Today companies can embrace a hybrid approach to IT, with some services provided via the cloud and others hosted locally in distributed IT, or edge computing solutions.

Hence the emergence of various types of data centre architectures, where localised IT systems help to increase uptime, resiliency, connectivity and application availability by using standardised, pre-configured systems, which are pre-integrated, tested at the factory level and offer an increased speed of deployment.

From the largest systems, to the smallest and most geographically dispersed distributed IT solutions, these data centres come in many shapes and sizes. Smaller systems may be required for reasons of latency—the need to ensure reliable high-speed connectivity with a low risk of delay from network congestion or distance; data sovereignty—where control of the data must remain in local hands due to security or regulation; or efficiency of operation where there are advantages to local operators retaining control of maintenance, servicing and computing capacity in response to ever-changing needs.

Distributed IT systems host far fewer applications than larger, multi-tenant colocation, or hyperscale environments. They also tend to be deployed in locations with little or no specialist IT support on-site, meaning the ability to remote monitor them from one location is essential to ensure resiliency. Fortunately, many systems are IoT-enabled as standard and have this ability built into their very fabric. Greater monitoring and management capabilities also allow unmanned data centres to be operated without the need for permanent on-site technical staff.

This higher degree of standardisation and pre-integration can allow customers to design bespoke systems comprising IT equipment from numerous vendors, including racks, servers and storage, to be assembled in factories and installed on site with the minimum of technical expertise. These systems are often built to specification, using the lessons learned from tried and tested reference designs to increase reliability. They can, in many cases, be customised to the user's exact requirements.

For security purposes, pre-integrated data centres come equipped with a variety of features such as management software, biometric access systems and cameras, alerting users to any unauthorised intrusion or tampering.

Resilient power is essential for any data centre, especially if it is being used to support mission-critical applications. Therefore pre-integrated systems include uninterruptible power supplies (UPS), which offer battery backup in the event of a disruption or outage.

IT cooling is another key aspect and one that is in constant use from the moment a system is operational. Many pre-integrated systems offer the provision of sophisticated air-cooling, but more recently, the ability to deploy liquid cooled systems has become another consideration for High Performance Computing (HPC), hyperscale and smaller on-premise data centres.

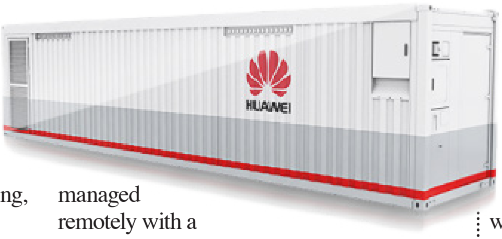
Some standardised architectures allow the user to deploy chassis-immersion liquid cooled servers as standard, whereas others may need some level of customisation.

An interesting observation is that liquid cooling can offer lower operating costs compared to air-cooled systems, as the need for electrical fans and other components is reduced or eliminated. Nonetheless, choosing a cooling solution needs careful consideration and should always be based on the needs of the applications being hosted.

Schneider Electric has a number of tools and online resources to help guide and educate IT professionals about the various types of data centre architectures available today.

PRODUCTS

German firm **Rittal**, located in picturesque Hessen, provides the RiMatrix S containerised data centre. Within the RiMatrix S, Rittal supplies 6 x server racks, 1 x networking rack, a fan-based cooling supply, an ABB UPS, a distribution board, fire suppression and 2 x free-cooling chillers. The result is a turn-key solution and complete data centre with a small site footprint and no need for any building work on-site. Here is a happy punter: "Rittal's ability to deliver a turn-key solution using a standardised product was a major consideration for us," says Andy Dixon of Envision AESC UK. "We are very impressed with the quality of the RiMatrix S product and the associated chiller units. The solution has provided us with the environment we needed to host our critical IT infrastructure." *rittal.com*

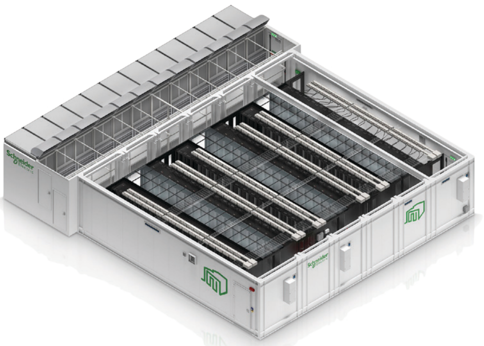


Huawei FusionModule1000A is an all-in-one, prefabricated, outdoor data centre (DC) solution, which the Chinese giant describes as "both environmentally friendly and reliable". The DC is available in 2N and N + X redundancy configurations. Integrating power, cooling, firefighting, lighting, and management systems into a single ISO dimension enclosure, FusionModule1000A, Huawei claims, can be deployed quickly, with smart managements systems ensuring reliable operations. In addition, operations and maintenance (O&M) can be managed remotely with a mobile app. FusionModule1000A can be applied to a wide range of industries, including enterprise, smart city, safe city, education, mining, oil exploration, finance, transportation and telecom carrier. *huawei.com*

Prime Wire and Cable's natural air-cooling data centre PRM-RIL-15 is a prefabricated data centre solution that integrates multiple physical infrastructure systems; all components are fully prefabricated, inspected and tested prior to the unit being shipped out to the customer. The data centre, Prime says it provides customers with the following: rapid deployment, reliability, energy efficiency, easy operation and remote digital operation, plus maintenance through intelligent software. *primewirecable.com*

The HPC Data Container by **EcoCooling** is described as a "flexible, transportable housing solution for the latest in HPC (high performance computing) equipment as well as lower density server equipment ideal for Edge Computing. EcoCooling reckons the container has been designed with rapid deployment strategies in mind and is, the firm says, easily stacked to enable quick scale ups. It also provides a low total cost of ownership solution for the low latency infrastructure critical to edge computing, which is being driven by digital innovations such as driverless cars, gaming and 5G. What's more, the container uses low energy direct fresh air cooling supported by a system of EC fans, EU4 filtration and CREC air mixing. This provides consistent temperatures to equipment which reduces failures. The filtration reduces contaminants harming the servers while the direct air cooling provides an efficient, green alternative to refrigerant based systems. Such techniques have been refined over the last 10 years working with clients such as BT, Hydro66, Talk Talk and ETIX Blockchain. *cloudcooler.co.uk*

Data Centre UK says its self-contained infrastructures contain all of the necessary power, cooling and security features that IT equipment needs. It claims its SmartShelter is the ideal solution for those looking for a larger, more robust data centre solution. This container holds a considerable amount of infrastructure, whilst providing significant levels of protection, power and cooling. Able to be deployed in remote areas with limited construction support, the SmartShelter is designed for organisations operating in unconventional locations away from typical office buildings and is the ideal solution for those looking for a larger, more robust data centre solution. Designed to meet current IT market trends and applications, ranging from high density computing and networking through to broadcast and audio/video, Data Centre UK says its modular data centre comes with full data centre infrastructure management (DCIM) functionality. *datacentre-uk.com*



The ModCel & ModCelEdge containerised data centre designed and supplied by **Secure I.T. Environments** consists of a 100% bespoke total solution "delivering an innovative effective energy efficient and re-deployable containerised data centre facility". The manufacturer says it can be used as a primary or critical data centre, secondary disaster recovery facilities or scalable and secure hubs for wider or remote data centres. They are available in single or multiple formats up to a height of 9m. ModCel & ModCelEdge may be installed as an external standalone structure or internally within an existing building or warehouse. It is manufactured in the UK and helps to resolve, space, deployment time, build complexity and cost challenges. *siteltd.co.uk*

"Please meet...

Eran Brown is the EMEA CTO at Infinidat, a provider of multi-petabyte data storage solutions. Networking+ asked him some questions of a very different kind

What is the best thing about your job?

Customer advocacy: I get to help customers solve real issues using our technologies. There is real satisfaction in enabling companies to meet their end goal for data storage and providing them with the tools to offer a better customer experience. This, we are finding, is paramount in today's instant gratification world! I'm a techie at heart but I've worked hard to simplify complex technical challenges into tangible business value, which is really useful in winning over non-techie key stakeholders!

Who has been your biggest inspiration?

I'll have to say my parents: my mum's philosophy in life can be summed in two words "so what?" – she cared very little about what other people say and think and taught us to ignore "common wisdom" and think independently. I think she probably had a lot to do with me always choosing to work for upcoming companies who were disrupting their field, instead of the entrenched incumbents. My father is more of a talker – his life philosophy requires four words: "Learn, always and everything". He always fuelled my curiosity, making me the proud tech-nerd that I am. Anyone seeing me walking my dog will see me with one earpiece in, learning something new through a podcast. It also contributed a lot to my career, where I can find myself in a conversation with a web company in the UK in the morning, a financial customer in Italy around noon and a US federal account in the evening. Having a keen interest in their area of work and being able to relate to what they are trying to achieve, is critical to building the relationship, and makes working together a lot more interesting.

What is your biggest regret?

I was supposed to relocate to another country twice in my life and both times it didn't happen (for very different reasons). As a keen traveller, the idea of living someplace completely new, with a different language and customs seems like the greatest adventure possible. Discovering the unknown and learning about yourself (and sometimes surprisingly so) is part of the journey that travel allows one to nurture! In the pre-Covid-19 days I travelled a lot and I hope to keep discovering the world, one city at a time soon.

If you had to work in a different industry, what would it be?

It may still happen! My dream, if I can afford it, is to start a non-profit organisation that will develop a critical thinking curriculum for young kids. I think it is among the most important skills of our time, especially in this fake-news era, where people are getting hurt by misinformation on the internet. Getting kids to think critically, to go beyond what information is given to them and developing their investigative skills, could be a silver bullet for several of our generation's problems. I would LOVE to be a part of the solution.

Who was your hero when you were growing up?

Angus 'Mac' MacGyver! He's a superhero in my eyes – using nothing but his intellect, engineering skills, knowledge of physics and a preference for non-lethal resolutions to solve problems. What's not to admire?

The Beatles or the Rolling Stones?

The Beatles. Don't ask me to choose a favourite song though – there are too many contenders!

What would you do with £1m?

I'd start my own non-profit company. Investment is key to getting new ideas off the ground and non-profits are no different to any entrepreneurial business in this respect. Innovation is at the heart of this and if we do not constantly do this, we won't be able to find new ways and approaches of doing things that we never thought were possible. With a non-profit, it allows one to have the gift to give back to society and create unimaginable opportunities. Reminds me of the old adage that 'the world is your oyster' and it's true. If one puts their mind to it, everything is possible – this is the philosophy I would hone with £1m.

Which rival do you most admire?

Pure Storage has always been an admirable opponent – in the early days its marketing was truly innovative. While we differ in our offering and market focus, they have always been interesting to watch (and even more interesting to beat on a deal).

What's the weirdest question you've been asked at an interview?

In an interview a few years ago a journalist (who I won't name) kept asking about a product we were secretly developing that he heard about, except the product was a figment of the imagination. I spent quite a lot of time trying to gently talk him down from writing about this. I hope in hindsight he's glad he didn't!

If you could change any UK law, what would it be?

I don't live in the UK, so I don't have 'skin in the game' here, however I would cancel Brexit. I'm sure I'm not the only one to have Brexit-fatigue! And there are more important things to focus on at this time. "

Powering The Northern Tech Revolution
DTX