APRIL 2023
networkingplus.co.uk

NETWORKING+

## Shadow IT challenges

Monitoring UC for employee engagement

***Jason Barker, IR, p5***

## MFA fatigue

AI, ML and adaptive authentication

***Stuart Wells, CTO, Jumio, p6***

## Questions and answers

My favourite will always be Batman

***Richard Massey, Arcserve, p16***

# The Wireless Infrastructure Strategy – a drop in the ocean?

**Technology secretary Michelle Donelan has unveiled the government's new Wireless Infrastructure Strategy, which promises to unlock growth and innovation across the country.**

The government has set out its ambitions to blanket the country with the fastest, most reliable wireless coverage available – with an ambition for all populated areas to be covered by standalone 5G by 2030. 77% of the population already has access to basic 5G from one provider.

Within the strategy, £8 million has been committed to delivering high-speed broadband for up to 35,000 of the UK's most remote properties – an important aim given the rise in working from home - and an additional £40 million 5G innovation fund will promote investment and adoption of 5G by businesses and public services, helping them unlock opportunities to use advanced wireless connectivity, generating value, innovation, and growth at a local level. A further sum of up to £100 million has been pledged to shape and drive early-stage research into 6G and influence global standards-setting.

The news has been met by widespread approval from the enterprise world.

"The announcement highlights the government's recognition of the huge economic opportunities offered by advancing mobile connectivity across the country," shares Ericsson's Katherine Ainley, CEO, Ericsson UK & Ireland. "We can unlock truly ground-breaking innovation through connectivity that will transform industries and create a more connected, safer, and sustainable world."

Telecommunications technologies are continually reshaping our lives, rendering the new connectivity strategy a significant step in the right direction for businesses and consumers alike. Jo Bertram, managing director, Business and Wholesale at Virgin Media O2 Business, says that the benefits for organisations will be immense: "the world of business is becoming increasingly connected – whether you're a global enterprise or a smaller business focused on conquering a local market, access to 5G and broadband networks are now vital for success. 5G has much to offer on an individual business level and to the UK economy, providing better conditions for organisations of every size and sector to adopt or scale their use."

"Today's 5G technology is now more affordable and deployment-friendly than ever, and the government's framework will begin to help businesses understand how to benefit from it," says Tony Eigen, VP Marketing, Baicells, identifying the need for enterprises of all sizes to expand their awareness of new paradigm-changing applications. "This will underpin new initiatives and stimulate growth across many industry sectors such as manufacturing, logistics, and healthcare."

Tom Bennett, CTO of Freshwave, meanwhile, believes that the strategy will help meet demand for greater mobile site density, and promote the evolution of smart cities. "It's good to see mobile private networks featuring in the government's strategy, as they will provide huge benefits to both private and public sector organisations. They not only improve productivity and safety in environments like ports and factories, but they open up exciting new use cases in health and social care settings."

Baicells' Eigen, however, highlighted that despite the good intentions, "the level of funding is something that is likely to be questioned. £40 million is a relatively small fund to support these broad ambitions. The US government, in comparison, is investing US$9 billion to deliver and improve 5G-based connectivity in suburban and rural communities. Setting positive targets for the nation is a step forward, but the government must continue to invest if it wants the UK to build a 'prosperous' digital future for all."

Is the government's new Wireless Infrastructure Strategy a fantastic initiative, or just a drop in the ocean at only £40 million? We'd love to hear our readers' views… ■

# Birmingham to gain small cells on lampposts in six weeks

Birmingham City Council has agreed the first Open Access agreements with Telecoms infrastructure providers to use council lampposts to host small cells to enhance network coverage and device connection capacity for mobile networks where large masts alone cannot meet user needs.

Typically, such agreements take more than 12 months to put in place but, thanks to support from WM5G, this has been reduced to just six working weeks. The open licensing agreement has been led by the Digital City and Highways teams in the Council and will speed up access to the city assets, resulting in faster deployment of 5G across the city.

"As we head into the Internet of Things age, the need for fast, reliable internet connections and increased capacity has never been greater. If we're to realise the full benefits of the digital age, small cells - which can be hosted on publicly-owned assets such as street lamps, buildings and street furniture - have a key role to play providing secure, reliable mobile networks," said Rhys Enfield, director of infrastructure acceleration at WM5G. "The administrative process involved in identifying suitable locations and getting the right legal agreements and contracts in place typically takes more than 12 months to complete - adding cost and delay to the process. However, thanks to support from the Department for Culture, Media and Sport (DCMS)'s Digital Connectivity Infrastructure Accelerator (DCIA), we have been able to work more closely to reduce this timescale to less than two months."

The DCIA was created by DCMS to help smooth the roll out of wireless networks, including 5G, across the country and ensure UK PLC is well placed to take advantage of opportunities arising from the digital age.

"We're proud to be among the leading Councils in the country to agree Open Access Agreements that will enable the roll out of crucial telecoms infrastructure across Birmingham much more quickly," said Peter Bishop, director for digital and customer services at Birmingham City Council. "As well as improving coverage and bandwidth, it will also improve service continuity, which will be crucial to supporting digital innovations, such as the safe operation of autonomous vehicles, as well as buildings, infrastructure monitoring and remote healthcare. It will also play a key role improving digital inclusion across the city."

As part of the DCIA programme, WM5G is working with a new platform provided by Sitenna that maps the location of publicly-owned assets capable of housing mobile infrastructure, together with their associated legal agreements and agreed market rates for use across the West Midlands Combined Authority region. The expedited signing of the Open Access Agreements between Birmingham City Council, Freshwave and Ontix has demonstrated how such initiatives will be key to speeding up the role out of upgraded network infrastructure across the country over coming years.

Virgin Media O2 (VMO2) is supplying the small cells used by both Freshwave and Ontix. "Pioneering trials like this are helping to boost connectivity in urban centres, meaning more people than ever before can benefit. Hosting small cells on existing kit means faster rollouts and less disruption – a win-win for consumers and local authorities with ambitious digital agendas," said Jeanie York, chief technology officer at Virgin Media O2. ■

# ManageEngine opens first UK data centres brings total to 16

ManageEngine has announced that it is opening two ISO/IEC-27001-certified data centre facilities in London and Manchester, its first data centres in the UK.

This announcement brings the total number of data centre sites to 16 for ManageEngine globally and represents a US$1 million investment.

The two new data centres will support UK customers who have a growing need for data sovereignty and data residency. The data centres will offer enhanced data security and will carry all the necessary SOC, ISO, and PCI DSS certifications, ensuring that data is stored securely and in compliance with local regulations and industry-specific standards.

The new sites will be hosted by Equinix, which was selected by ManageEngine for its state-of-the-art, global, secure, sustainable data centre platform that is renowned for its expansive reach. The data centres will host a few prominent ManageEngine products, including ServiceDesk Plus Cloud (for IT and enterprise service management) and Endpoint Central Cloud (for unified endpoint management and security). The long-term plan is to offer ManageEngine's entire portfolio from the UK data centres.

"Cloud adoption has been rapid in the UK, far outstripping other markets," said Rajesh Ganesan, president of ManageEngine. "We have seen 70% growth in cloud adoption YOY since 2018, versus 50% globally. Post-Brexit, we also saw increased demand from customers for data centres to be located in the UK to ensure data sovereignty and comply with local regulations."

The UK market is the second largest for ManageEngine, representing 25% of its global turnover. There has been an acceleration in cloud adoption amongst UK customers, which in turn has created more demand for local data storage. This announcement will help IT teams move operations to the cloud seamlessly while adhering to the data privacy and security standards of the UK. ManageEngine is also establishing one of the two UK data centres as a disaster recovery site.

ManageEngine's new data centres will be fully secured, employing security processes like full-disk encryption to protect data and prevent unauthorised access at the hardware level. Additional controls, like anti-DDoS strategies, will also mitigate cyberattacks. ■

# CIF: 14% of businesses are using cloud to develop AI strategy

New research from the Cloud Industry Forum (CIF) has found that while 62% of organisations are still in the process of migrating applications to the cloud, 14% have now completed this process and are using cloud to help develop their AI strategy.

This provides evidence that cloud is now helping businesses break new ground in technology projects, pushing beyond its traditionally recognised benefits such as agility and scalability, and helping companies continue to innovate in the face of a challenging economic climate.

The data also examined the importance of ESG and sustainability credentials when organisations choose a cloud provider.

Key findings from the research included that 90% of survey respondents consider machine learning either very important or critical to their business, while 86% say the same about AI; 82% consider ESG and sustainability credentials as important when choosing a cloud provider, and 85% would reject a provider if these credentials weren't in good order; 67% say current economic challenges are affecting IT spend at their company; 96% say their cloud strategy has delivered against expectations, although only 43% say it has delivered totally against these expectations so far; complexity of migration is the leading cause of cloud projects falling short of expectations, cited by 65%.

Despite the enduring promise of cloud and its role in the AI/ML revolution, there are still hurdles in place that need to be overcome. Current macroeconomic challenges are impacting most businesses in some way, so cloud providers have a role to play in helping their customers remain agile and resilient from a technological standpoint.

"Perhaps even more pertinent for cloud providers are the customer challenges that are more within their control, such as budget constraints (cited by 41% of respondents) complex migrations (38%), skills shortages (34%) and poor legacy integration (34%). Organisations are ready and willing to leverage cloud to help them fulfil their most aspirational technological goals, so cloud providers must continue to up their game to keep pace with their customers," said David Terrar, CEO of the Cloud Industry Forum. "It's a challenging time for businesses, but we believe this is also the start of an exciting period of evolution for the cloud. Technologies including AI and machine learning – alongside others such as IoT, edge computing and blockchain – are now hugely prominent in the minds of IT and business leaders. Cloud computing is the enabler for all of these, showing its ability to evolve with the times, while at the same time staying true to what made it so successful in the first place. The most agile cloud providers are the ones that will prosper in this period." ■

EDITORIAL:

**Editor:** Amy Saunders
amys@kadiumpublishing.com

**Designer:** Ian Curtis

**Sub-editor:** Gerry Moynihan

**Contributors:** Jason Barker, Justin Day, Stuart Wells, Manzoor Mohammed, Ricardo Diaz, Richard Massey

ADVERTISING & PRODUCTION:

**Sales:** Kathy Moynihan
kathym@kadiumpublishing.com

**Production:** Karen Bailey
karenb@kadiumpublishing.com

**Publishing director:**
Kathy Moynihan
kathym@kadiumpublishing.com

Networking+ is published monthly by:
Kadium Ltd, Image Court, IC113, 328/334 Molesey Road, Hersham, Surrey, KT12 3LT
Tel: +44 (0) 1932 886 537



ISSN: 2052–7373

# 50% of organisations struck by ransomware in 2022

Fortinet has unveiled its 2023 Global Ransomware Report, which revealed there was a large disconnect between respondents' level of preparedness with existing strategies and their ability to stop a ransomware attack.

Although 78% of organisations stated they were "very" or "extremely" prepared to mitigate an attack, the survey found 50% fell victim to ransomware in the last year, and almost half were targeted two or more times. Four out of the five top challenges to stopping ransomware were people or process related. The second largest challenge was a lack of clarity on how to secure against the threat because of a lack of user awareness and training, and no clear chain-of-command strategy to deal with attacks.

The survey also found that despite most (72%) detecting an incident within hours, and sometimes minutes, the percentage of organisations paying ransoms remains high, with almost three-quarters of respondents making some form of ransom payment. When comparing across industries, organisations in the manufacturing sector received higher ransoms and were more likely to pay the fee. Specifically, one quarter of attacks among manufacturing organisations received a ransom of US$1 million or higher. Finally, while almost all organisations (88%) reported having cyber insurance, almost 40% didn't receive as much coverage as expected and, in some cases, didn't receive any because of an exception from the insurer.

With concerns about ransomware still high and despite a challenging global economic environment, nearly all organisations (91%) expect increased security budgets in the next year. Based on the technologies viewed as most essential to secure against ransomware, organisations were most concerned with IoT Security, SASE, Cloud Workload Protection, NGFW, EDR, ZTNA, and Security Email Gateway.

In the future, top priorities will be investing in advanced technology powered by AI and ML to enable faster threat detection and central monitoring tools to speed response. These investments will help organisations combat a rapidly evolving threat landscape as cyber attackers become more aggressive and deploy new elements into attacks. ■


# IX Birmingham: first internet exchange in the West Midlands courtesy of Proximity Data Centres

In further exciting news for Birmingham, Proximity Data Centres has announced IX Birmingham, the first regional internet exchange in the heart of the West Midlands.

Located at Proximity's Birmingham Edge 8 tier 3 data centre, IX Birmingham will allow businesses across the city and local region to have access to higher-speed, lower latency connectivity options by eliminating the need to route all their data via exchanges in London and Manchester - local data stays local while other data can be accessed through traditional centralised internet exchanges.

"I have long pushed for the establishment of an Internet Exchange in Birmingham, recognising that it is a key component of the digital infrastructure that our businesses need to create and accelerate new products and services," said Raj Mack, Birmingham City Council's head of digital city and innovation. "The IX Birmingham will greatly enhance the capability of the city as a leading international digital city and its reputation as Digital Birmingham."

"The Council welcomes this exciting initiative which is line with our vision for creating new innovative opportunities that maximise the use of digital technologies and the skills and capabilities of our citizens and local businesses," said Peter Bishop, director for digital and customer services at Birmingham City Council. "Working closely with Proximity's Edge IX division we aim to ensure digital businesses including those in the creative, healthcare and manufacturing industries are no longer disadvantaged by the absence of an internet exchange on their doorstep."

"We selected Birmingham as our first Edge IX location as the region's digital community has remained underserved when it comes to the lowest latency solutions possible for sending or receiving data. We are looking forward to delivering similar benefits to other regions of the UK and Europe during this year and in 2024," said Commented John Hall, managing director-colocation, Proximity Data Centres. ■

# Asda adopts RCS for business messaging

Infobip has partnered with Asda to support its customer communications for grocery and online orders teams by launching the largest Rich Communication Services (RCS) business messaging traffic in the UK.

The new initiative will help to support messaging across the full online customer journey, including order confirmation, delivery times and substitutions. The roll-out has made Asda the first major UK grocer to launch RCS business messaging in the UK.

Heralded as the next generation of SMS, RCS business messaging brings a mobile app's rich functionality into the messaging platform. This will enable Asda to provide rich media experiences to its customers via a channel they trust – the native messages app – with no additional installation or downloading. The messages showcase Asda's logo, brand name, and links, giving customers peace of mind knowing they can trust the sender.

The collaboration between Infobip and Asda increases brand awareness through logos and promotion for Asda Rewards App; and increases security as the sender is verified by operators.

"Ensuring our customers receive exceptional customer service is a key focus for us and we're excited to be the first retailer to offer this innovation to customers," said Martin Coates, comms product manager from Asda. "The idea is that by providing customers with that additional peace of mind, we'll boost customer engagement and reduce the number of failed deliveries. Infobip's CX workshop helped us identify how to improve Asda's entire customer journey through automation, AI, rich conversational communication, and a customer-first approach, which has led to this first step into RCS business messaging." ■

# Digital Sandwich revolutionises digital agri-food supply chain with IoT

A consortium of food manufacturers, technology specialists and academics - IMS Evolve, Raynor Foods, University of Lincoln, University of Exeter, Digital Catapult, Sweetbridge, Crosspay, NetFoundry, INDUSTRIA Technology, and R3 - supported by the government, have launched Digital Sandwich after a two-year development project.

The platform was developed to connect primary production and supply chains to retail to provide traceability and provenance of ingredients whilst increasing manufacturing productivity, improving processes, and reducing waste across the supply chain. The project is as a national demonstrator of a digital agri-food supply chain, using sandwich manufacturing as the use case.

The open platform digital supply chain paves the way for a wider ecosystem network and offers a low barrier approach so that supply chain organisations of all sizes and technological maturity can participate. The project extends the use of IoT, blockchain and AI technologies to the ready-made food supply to ensure the traceability of every component ingredient in the supply chain.

Following the project's completion, the consortium will look to introduce and expand the solution across the food supply chain, whilst establishing new use cases that leverage the technology's flexibility to allow it to be used across other chains, with new possible sectors including the NHS or pharmaceuticals. ■

# Currys picks LTIMindtree for digital transformation

LTIMindtree has been selected by Currys for a five-year digital transformation project utilising LTIMindtree's extensive retail business consulting and technology capabilities to deliver the next phase of omnichannel transformation to its consumers and employees.

The multi-million-dollar collaboration aims to enhance Currys' omnichannel revenue stream and drive cost transformation. Consequently, it will also enable Currys to strengthen its market position.

"Our journey with Currys is a testament to LTIMindtree's capabilities in the retail space. We have successfully delivered the best-in-class omnichannel shopping experience for their consumers. In this next phase, we remain committed to leveraging our digital expertise to drive their overall transformation goals," said Debashis Chatterjee, CEO and MD, LTIMindtree. "At LTIMindtree, we understand the importance of having the right partner to drive strategic transformation initiatives, and we are honoured to be that partner for Currys."

LTIMindtree will help Currys modernise its systems by consolidating and simplifying consumer and employee-facing applications, leading to accelerated innovation, increased efficiency, and an overall improved end-user experience. ■

# Keysight achieves first 6G speeds >100Gbps in the UK

Keysight Technologies, Inc. in collaboration with National Physical Laboratory (NPL) and the University of Surrey, has made the first 6G connection at speeds greater than 100Gbps over sub-terahertz (THz) frequencies in the UK.

Future 6G use cases like augmented reality and autonomous vehicles will require data throughput speeds from 100Gbps to 1Tbps. To achieve the extreme data speeds and low latencies required by these revolutionary use cases, the use of sub-THz frequencies is being explored. However, operations in sub-THz frequency bands introduce signal integrity and path loss challenges that can negatively impact performance.

Keysight, NPL, and the University of Surrey established the first sub-THz high throughput 6G testbed in the UK to address these challenges. Funded by the UK government for 6G research, NPL and Surrey scientists are using the testbed to study and characterise sub-THz signal performance to generate new techniques for optimising data paths and calibration methodologies.

Located at NPL, this new 6G testbed achieved the UK's first high-speed sub-THz data link. The demonstration was made at a frequency of 300GHz using both 32 and 64 quadrature amplitude modulation (QAM). Built on Keysight's 6G Sub-Terahertz R&D Testbed, the testbed uses the M8194A Arbitrary Waveform Generator (AWG) combined with Virginia Diode Inc. (VDI) upconverters / downconverters to generate the signal and Keysight's UXR0704A Infiniium multichannel high-performance 70GHz oscilloscope to analyse the signal. ■

## Word on the web...

### Setting the right foundations for network management

**Justin Day, CEO and co-founder, Cloud Gateway**

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

# Growth companies need expert insight to harness the full potential of the cloud

*Dr Manzoor Mohammed, co-founder and CINO, Capacitas*

The growth that should distinguish a successful business is too often undermined by the way it uses the cloud. Growth is the prime driver for organisations migrating to the cloud, with many portfolio companies looking to achieve 30-40% each year. Yet, they quickly find costs grow faster than the business, availability becomes a problem and performance fails to deliver a great user experience.

These factors grind away at profitability and potential. Organisations end up in a running battle with Opex costs and internal tensions mount. These are serious problems that can only be overcome with a holistic approach. Discounts and cloud-monitoring tools may resolve short-term difficulties but often stack up longer-term problems. It is time to recognise that efficient use of the cloud means a company has an efficient development team that delivers on targets.

## A holistic approach

The causes of excessive cloud expenditure range from poor initial sizing to weak working practices and the inability to simplify cloud management complexity. In their early phases, companies focus on solution development and engineers spin up multiple cloud instances without coordination. Bad habits continue, with engineers using extra server capacity to compensate for badly performing software and bottlenecks.

Even with good performance across a distributed architecture, costs are very difficult to manage. Auto-scaling tools are only as effective as the applications they support, leading organisations to spend more on capacity to be certain of meeting demand.

It is possible to transform cloud efficiency and performance by addressing cost, scale, and performance holistically. Operating partners or CEOs can engage specialists to release millions of pounds in unnecessary costs, increasing the value of the platform and the equity in the company while enabling the business to scale more efficiently through incremental investment.

The holistic approach also increases development productivity significantly since poor cost-management is often a sign of more deep-seated inefficiency. The operating partners should bring engineers along with them, increasing awareness of the costs involved in proliferating cloud instances as well as their value. Development teams should become more acutely aware that software is the driver of cost.

## Other approaches fall short

There is also nothing inherently wrong with using tools and discounting mechanisms - CloudHealth, Zesty, savings plans, etc. - to address short-term budget overruns. But these will not resolve the more deep-seated structural problems such as architecture/product inefficiency. Such tactics can become counter-productive, as engineers mistakenly believe they have conquered the main challenges and continue producing inefficient software or products.

FinOps is another framework that seeks to embed shared responsibility for costs, addressing the end of the lifecycle to obtain a discount or to right-size requirements. But it does not resolve the fundamental problems and is reactive – addressing discounts once costs have already increased. To be serious about addressing the root causes requires engaging at the start of the development lifecycle. Engineers must accept that most inefficiencies are in the software created by their teams.

Therefore, it is important for engineers to view cost as another performance metric, rather than as a potential nuisance factor. There should be an expected spend and set of performance targets they are tracking against and if not, then questions should be asked. It is not necessary, for example, to fill all capacity available to meet stability challenges. This may work temporarily, but who is going back to fix this problem properly?

If organisations have access to third-party expertise in capacity management, by contrast, they can use the wealth of data the cloud generates so their developers take control and are more experimental, enjoying greater transparency. Whereas FinOps looks at cost in isolation, it is hugely more effective to look at performance and cost metrics together. With expert insight each organisation establishes what 'efficiency' means in relation to its own business objectives. It optimises cost, scalability, and performance without any of these essential attributes suffering.

The bottom-line gains for companies following this approach are eye-catchingly large, especially for tech SaaS companies where cloud is the leading cost or second only to people costs. Fix cost, scalability and performance, and an organisation has more than equity value – it has a platform and a team that will deliver real growth. It can meet its investors' ambitions, expanding from two million subscribers to 200 million without problem.

Once organisations start to address the cost drivers holistically, their value will increase dramatically, powering their bottom-line growth. ■

# Waking up from multifactor authentication fatigue

**Stuart Wells, CTO, Jumio**

Dating back to the mid-1990s with the inception of phishing, hackers have long employed the use of social engineering attacks for credential access and network breaches. Today's hackers, however, aren't hunting their next victims in AOL chat rooms. Instead, they're right beneath our fingertips, spamming users into approving push notifications and sign-in attempts that grant outsiders inside access.

The increasing use of multifactor authentication (MFA) has been a crucial step in ensuring the security of our digital lives. However, as more systems and applications require MFA, the problem of 'MFA fatigue' among users has become more prevalent. This can lead to frustration and decreased security when users are repeatedly prompted to provide additional forms of authentication.

## MFA and its drawbacks

With a tactic called 'prompt bombing,' MFA fatigue can lead to a scenario in which an attacker floods a user's device with MFA prompts to overwhelm and trick the user into providing their credentials or biometric data.

Prominent organisations such as Microsoft and Cisco have faced significant data breaches because of this tactic and in 2022, Uber faced a data breach in which hackers gained access to internal systems, including the company's Slack channel via this method. The breach is believed to have occurred after an Uber contractor's personal device was infected with malware, exposing their login credentials. The attacker repeatedly tried to access the contractor's Uber account but was initially blocked by two-factor authentication. Eventually, the contractor gave in to MFA fatigue and accepted one of the log-in approvals, allowing the attacker access.

What's more, MFA can become less effective over time as attackers become more sophisticated. Hackers can employ phishing techniques to trick users into providing their credentials, even when MFA is in place. These advances make it essential for organisations to stay up to date on the latest security threats and to continuously evaluate and update their security measures. To combat this issue, a new approach is necessary.

## Smoothing friction with passwordless authentication and facial recognition

Friction in the user experience is a significant element in cases of MFA fatigue. An effective solution that tackles this component is using passwordless authentication with facial recognition technology. This method eliminates the need for users to remember and enter complex passwords, instead relying on biometric scans or device-based authentication. This can reduce the number of steps required to log into an account, making the process faster and less frustrating for users.

Biometric technology not only improves the user experience but also makes it more difficult for attackers to gain access to accounts through stolen credentials. Facial recognition provides an additional layer of security as it is difficult for attackers to replicate a user's unique facial features, bolstering the protection provided by MFA.

## Artificial intelligence, machine learning and adaptive authentication

Facial recognition solutions that utilise artificial intelligence (AI) and machine learning (ML) can significantly improve the accuracy and speed of verification. This can help to improve productivity and reduce costs for the organisation. AI and ML can be used post-authentication to verify a user's identity by analysing their behaviour patterns. These models can detect unusual patterns in typing and mouse usage and can be used to prevent malicious activity.

Implementing adaptive authentication, which adjusts the level of security required for a given transaction based on the user's behaviour, device, location, and other factors is an additional strategy. For example, if a user is logging in from a trusted device or location, the system may only require a single factor of authentication. But if the user is logging in from an unknown device or location, the system may require multiple factors of authentication. This approach can help to balance security and convenience for the user, making it less likely for them to fall foul of MFA fatigue.

Moreover, push notifications which display varying levels of information can be used as a method of authentication. To combat fatigue and make users more aware of possible attacks, notifications can be designed to prominently display the location of the user attempting to access the account. The user is then more aware of any discrepancies and is less likely to grant access inadvertently.

## User education

In addition to the above solutions, organisations should also educate their users about the importance of strong security and the risks of MFA fatigue. The Uber incident emphasises the need for not only robust security measures, but also making sure that individuals are aware of potential vulnerabilities and avoid complacency. This can include providing training on how to recognise and avoid phishing attempts, as well as encouraging users to report suspicious activity. Ultimately, this individual training will go toward reducing the systemic risk of data breaches and other security incidents.

MFA fatigue and prompt bombing are significant issues that can have a major impact on security for individuals and organisations. However, by pursuing the aforementioned tactics explained, businesses can improve their user experience while strengthening their security posture. ■

# Shadow IT's clue to hybrid employee engagement

*Jason Barker, SVP EMEA & APAC, IR*

Shadow IT has plagued organisations for years – long before hybrid working became firmly established. With the shift to working from home (WFH), the use of personal devices and applications that fail to adhere to corporate standards has exploded – even for companies that have accelerated the deployment of unified communications (UC) solutions.

Yet, while the security and compliance risks associated with shadow IT are well known, how many companies are actively considering the implications for employee productivity, collaboration, and morale? Are employees using new corporate solutions at home or still preferring their own work around options? Are they frustrated because performance drops off every afternoon, or feeling isolated because the new corporate platform lacks features they have previously used to connect with colleagues? Without the ability to monitor the entire, end to end infrastructure, including WFH, an enterprise will be blind to the true extent of shadow IT and, critically, key indicators of employee engagement.

## Hybrid experience crisis

Elon Musk et al may be adamant that staff must return to the office, but the reality for most UK businesses is that employees now expect hybrid working. The problem for large enterprises is that hybrid working environments are still not meeting the needs of employees. For example, almost 60% of women who work in hybrid environments feel they have been excluded from important meetings; stress levels are rising, and burn out is driving high levels of attrition. Trends such as 'Acting their Wage' may be a TikTok Gen Z cliché; but lack of productivity and engagement of the younger WFH workforce is a huge issue.

Businesses have an array of cultural and operational challenges to address to create a hybrid working model that engages all employees. But too few have recognised the impact of shadow IT and a company's lack of control over the UC tools preferred by diverse individuals across the business. Over the past few years, employees have taken a proactive approach to making WFH work for them. And while companies have fast-tracked UC deployments to improve the overall employee experience, many still prefer the 'emergency' options to the new corporate standard.

The result is a not just a significant shadow IT problem - with the associated security and compliance risks - but a complete lack of corporate understanding about employee activity. Are individuals engaged with the business? Are they productive? Motivated? Or about to leave? With the UK still suffering a significant lack of skills – access to labour (75%) and skills (72%) continue to top business' labour market concerns, according to the CBI – the hybrid working experience is fast becoming a critical component in employee engagement and retention.

## Understanding hybrid performance

With employees returning to the office for a few days each week, the hybrid experience should be seamless. Individuals should feel productive, engaged, and motivated irrespective of working location but few businesses know if this is the case. While IT teams routinely monitor UC performance across the organisation, information is collected on each individual system. With 10,000s, even 100,000s of employees using multiple solutions, it is impossible to gain a complete picture of system usage or performance.

Furthermore, this monitoring rarely extends outside the core office environment, leaving the business completely blind to the WFH experience. From calls dropping out when children return from school and plug into games and streaming services, to a widespread resistance to adopting the new corporate UC standard, a lack of visibility across the entire hybrid environment is creating significant business risk.

## Monitoring UC experience

A single view of the entire UC environment is critical to both accelerate problem resolution and better understand the hybrid employee experience. Understanding how, when and where individuals are using different aspects of the UC solution set will provide companies with new insight into the way staff are adapting to the hybrid experience – and quickly flag up potential problems.

Monitoring every aspect of the infrastructure and providing a single view of performance enables IT to rapidly understand – and resolve – issues that are affecting workers in any location. From underperforming WiFi to problems with local network providers, or specific application glitches, better visibility is key to improving the timeliness of IT support.

But it also will quickly highlight issues with UC adoption and shadow IT. If employees are failing to engage with the company's preferred platform – 85% of businesses use two or more meeting platforms (according to Cisco) - questions can be raised about the education and training process. With native monitoring tools providing information limited to a single solution, it is impossible to gain a clear picture of the way individuals are interacting with different systems. Are employees able to personalise the platform to work in a way that they prefer? Is one department creating significantly fewer calls via the platform than the rest of the business – indicating a reliance on an unauthorised solution? Or is it just poor WiFi that is affecting performance, not the UC at all? Granular understanding of UC usage can help the IT operations team prioritise investment and drive strategic investment.

## Strategic hybrid planning

Monitoring the entire end to end UC environment also provides useful information for other parts of the business, including both human resources (HR) and facilities management. For HR teams, for example, early insight into IT problems that could be affecting employee morale can enable proactive intervention and support. In addition to segmenting information by geography or business group, it could be analysed by age, allowing HR to understand how different generations are experiencing and engaging with the hybrid environment.

With so many companies now offering hot desking options, this information is increasingly used by facilities management teams tasked with ensuring a building is not only safe and secure, but also as productive as possible. Infrastructure and collaboration platform management are now Key Performance Indicators, with UC usage information providing essential insight to support business decisions.

Are employees avoiding certain buildings, putting pressure on space in other locations? And, if so, is that because calls keep dropping out or the Wi-Fi is too slow? If employees must work in an office location one, two or three days each week, it is important that the office is designed to support a truly effective collaboration. Any frustration about the quality of the working environment, in any location, will rapidly affect morale. Providing facilities management teams with fast insight to usage information will give early indications of problems and allow essential infrastructure change.

## Conclusion

Hybrid working, in one form or another, is here to stay. Organisations must ensure the quality of the employee experience to safeguard productivity and collaboration and, critically, boost staff retention through enhanced morale. Proactively monitoring the entire corporate environment provides not only insight into immediate UC performance issues that need to be urgently addressed; but also, vital understanding of how, where and when different groups and individuals are engaging with the business. ■


# ChatGPT – friend or foe?

## The launch of ChatGPT signals the dawn of a new era for cybersecurity – but will that era be good or bad? The verdict is out, reports Amy Saunders

**It's broadly agreed that AI and ML presents a double-edged sword, with many organisations reporting mixed feelings about the technology.**

For cybersecurity professionals, AI is a powerful instrument that expedites and improves processes like automated security processing and threat detection, reports Matt Aldridge, principal solutions consultant, OpenText Cybersecurity. "However, we must remember that bad actors have the very same toolsets available for their criminal activity. It is proving to be a constant cat-and-mouse game between these two parties."

Bad actors have always moved with the times, if not ahead of them - and AI is no exception. From AI-generated phishing emails to pattern detection and malware, AI threats are becoming increasingly sophisticated; however, AI is also a handy tool incorporated into many modern cybersecurity solutions. "On balance, it is currently perceived as more of a threat until it is fully leveraged by all organisations," says Alan Hayward, sales & marketing manager at SEH Technology.

"As these tools become more advanced, and we as defenders learn to use them in new and innovative ways, so too will attackers. Nearly all innovation is dual-use technology," explains Jonathan Hencinski, VP, security operations, Expel.

"The key question is where the balance of advantage will ultimately lie. AI is already being deployed by both network defenders and those attacking them. The strategic issue for the community is where that advantage will fall in the long term," asserts Will Dixon, global head of the academy and community, ISTARI.

### Enter ChatGPT

The launch of ChatGPT in November 2022 made huge waves. An advanced form of AI developed by OpenAI, ChatGPT is a language model that can understand natural language and generate text that is indistinguishable from human writing.

Significant concerns have been raised, including potential malicious use by hackers or authoritarian governments. Bad actors can use ChatGPT and other AI writing tools to make phishing scams more effective. Traditional phishing messages are often easily recognisable because they are written in clumsy English, but ChatGPT can fix this, explains Florian Malecki, executive

vice president of marketing, Arcserve. "Mashable tested ChatGPT's ability by asking it to edit a phishing email. Not only did it quickly improve and refine the language, but it also went a step further and blackmailed the hypothetical recipient without being prompted to do so."

Threat actors can use technology like ChatGPT to automate convincing spear phishing emails, reports Corey Nachreiner, CSO at WatchGuard. Singapore's Government Technology Agency demonstrated this a few years ago, and recently we've seen members of a popular underground forum use ChatGPT to write data-stealing malware. "In the future, we also expect to see threat actors leverage adversarial ML to combat the ML algorithms used in security services and controls."

"AI bots like ChatGPT pose cybersecurity threats for several reasons; not only can they aid in social engineering attacks but can also help develop code that can be used to inform cyberattacks," says Michael Lakhal, director of product management, product strategy, OneSpan. "Take the ability for an AI bot to replicate written prose. Being able to parse through countless examples of an individual's writing style online means a sophisticated AI system could convincingly replicate how a specific person writes. This opens up huge potential for phishing attacks, with emails pretending to be from certain people or businesses becoming almost imperceptible to the average person."

With AI making it easier to create malicious code at scale, exposure to cybercrime has significantly increased. Malecki says that, while the number of security tools available to protect the enterprise may be increasing, these tools may not be able to keep pace with emerging AI technologies that could increase your vulnerability to security threats.

"The constantly evolving cybersecurity industry can be compared to the Lernaean Hydra, one threat is mitigated to have three newer ones emerge!" agrees Lakhal. "And the easily accessible AI systems won't help in containing this aspect, allowing hackers to keep finding new ways of developing their attacks."

Check Point Research reported that, within weeks of ChatGPT's release, individuals in cybercrime forums, including those with limited coding skills, utilised it to create software and emails for espionage, ransomware attack, and malicious spamming. "Check Point said it's still too early to tell if ChatGPT will become the go-to tool among Dark Web dwellers," reports Malecki. "Still, the cybercriminal community has demonstrated a strong interest in ChatGPT and is already using it to develop malicious code."

British security agency GCHQ has also recently identified ChatGPT and other AI chatbots as an emerging security threat to sensitive information. "Enterprises can protect against ill-intended actors by implementing clear information security policies and rules on the use of AI-powered chatbots, especially where sensitive data is involved and, in some cases, an outright ban might be the most sensible option to safeguard data until the threat is better understood," asserts Hayward.

Indeed, at the end of March, Elon Musk and 1,000 AI experts prepared an open letter calling for a six month pause in developing systems more powerful than ChatGPT-4, OpenAI's latest iteration, citing potential risks to society.

"Should we let machines flood our information channels with propaganda and untruth?... Should we develop non-human minds that might eventually outnumber, outsmart, obsolete, and replace us?... Such decisions must not be delegated to unelected tech leaders," reads the letter.

It's not all doom and gloom for the role of AI bots in cybersecurity, however, and enterprises can stand to benefit greatly from incorporating it into their networks.

"Firstly, it can help to improve threat detection capabilities by spotting threat patterns that human analysts often miss," says Hayward. "Secondly, it improves efficiency by analysing data patterns faster than humans, allowing for faster breach detection. Finally, AI bots can monitor networks at all times, even when humans are unable to, providing a more comprehensive level of security continuously."

**"Not only did it quickly improve and refine the language, but it also went a step further and blackmailed the hypothetical recipient without being prompted to do so"**

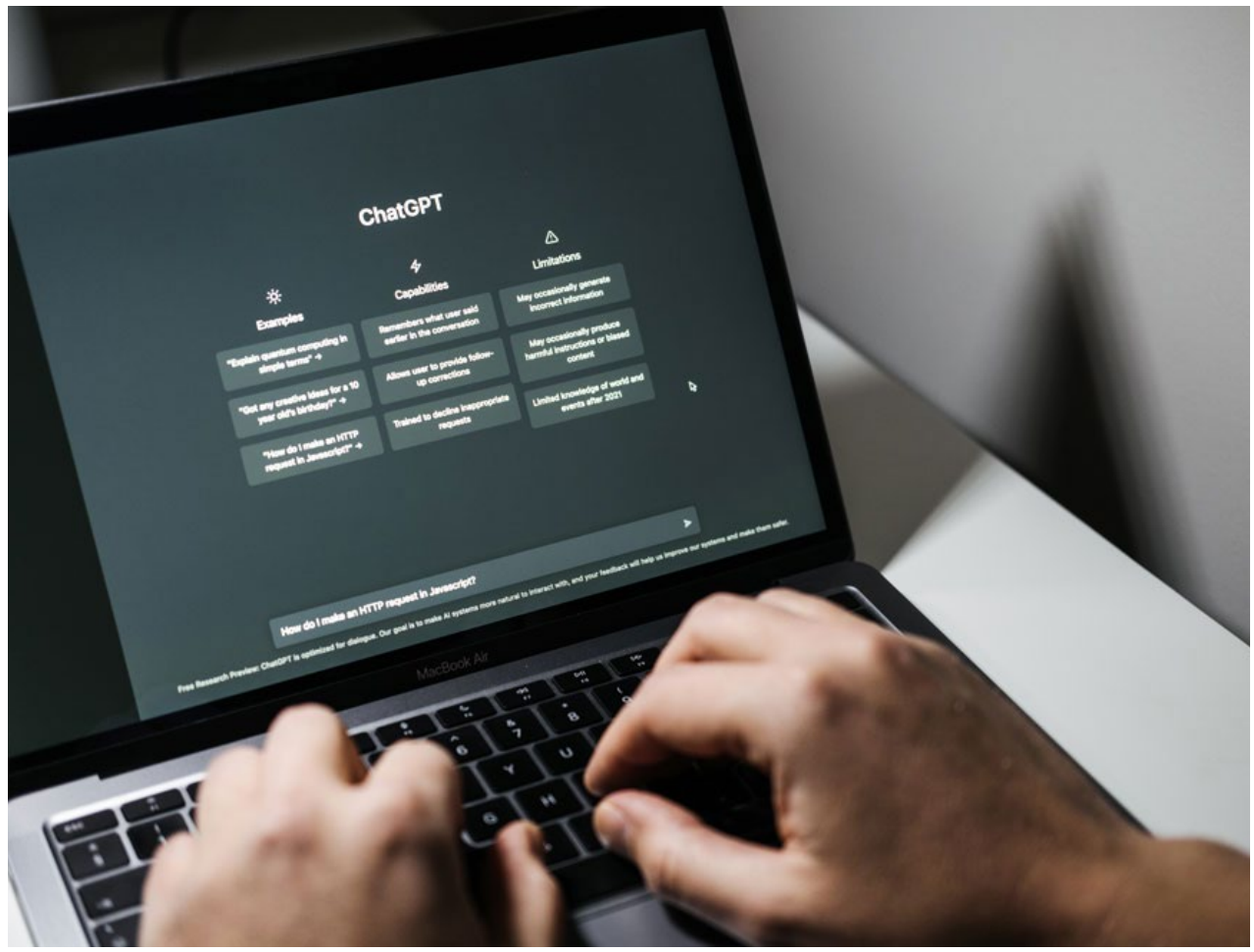
Indeed, AI has real potential to enhance the speed, precision, and impact of operational defence, and support organisational resilience.

"AI is already being used to support the security community by enhancing and scaling process-heavy tasks typically performed by analysts, such as first-response incident triage," says Dixon. "AI defence is becoming deeply integrated into defensive responses within the cybersecurity ecosystem. Ultimately, how these technologies are adopted is a question of maturity and resource. There are levels of sophistication for defenders using AI - improving security posture, dynamic threat detection, proactive defence, response, and recovery and ultimately, attribution."

"Imagine a security chatbot that inspects your security controls and

configurations and points out gaps recommending policies or defenses," explains Nachreiner. "In the future, AI systems will help audit, assess, and validate our security controls. ChatGPT's natural language processing means that we may have security chat bots advising security professionals in the future."

"For cybersecurity organisations, using AI is no longer an optional improvement, but an absolute necessity," explains Aldridge. "Considering the rise of AI-enhanced cyberattacks, the only way to maintain enterprise security is by incorporating AI into threat recognition systems to cope with the increasing sophistication and intelligence of cybercriminal techniques. You must fight fire with fire – or risk being left behind."




## An answer to the skills shortage? In a word, no…

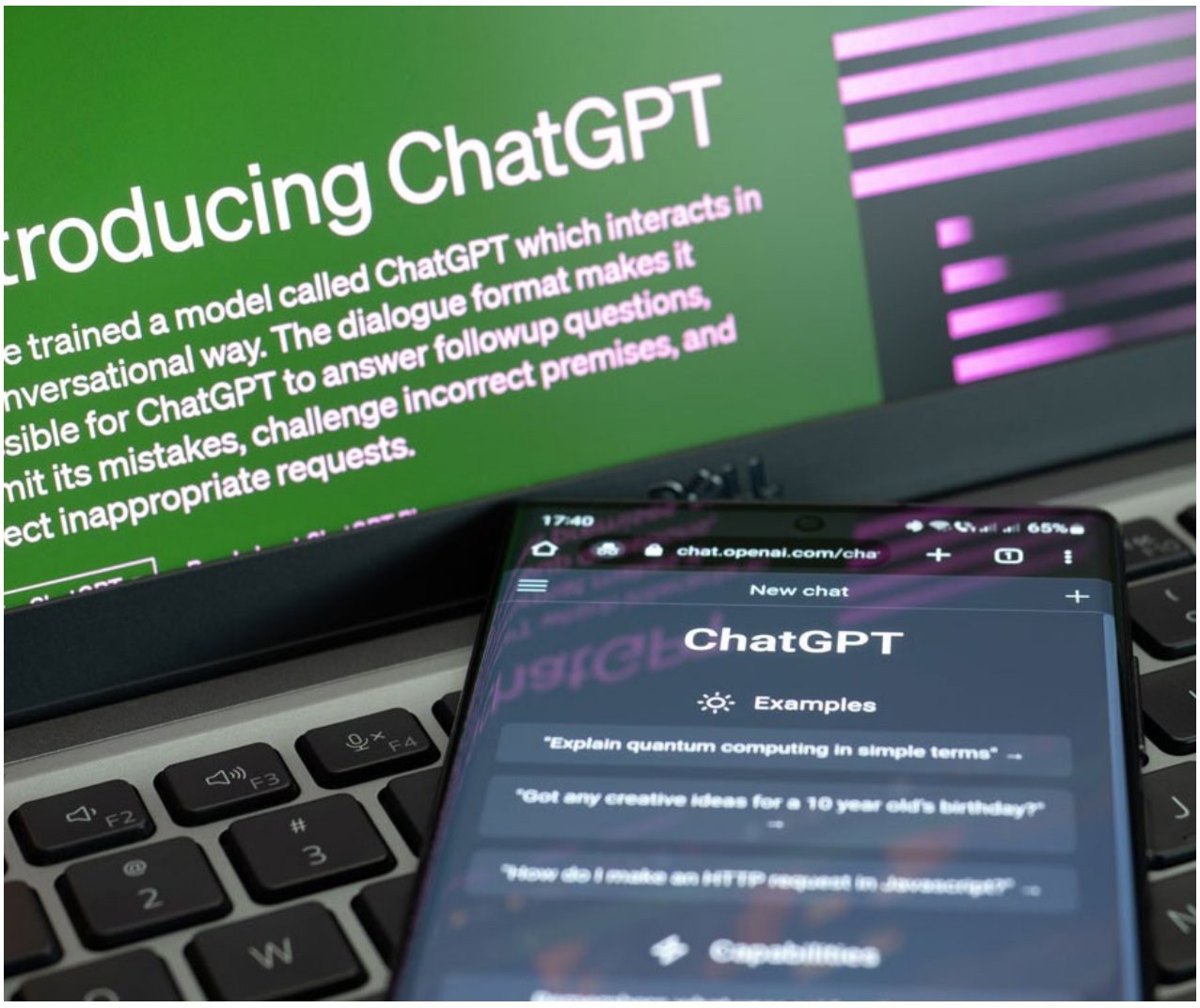
The impact of AI bots on IT employees is yet to be fully understood, but we should expect significant changes in roles and staffing levels, says Hayward: "repetitive tasks will be less of a priority for employees in the future and roles will change to have a great understanding of AI technologies and leverage human skillsets to drive forward future creativity and innovation."

Aldridge agrees that AI-enabled cyber tools are already reducing the burden of repetitive workload. "SOC teams will be increasingly enabled to focus on the most highly threatening, targeted events while AI-enabled solutions attend to the daily grind of repeated, unremarkable breach attempts and internal user errors."

"Eventually, AI may get good enough that we see staffing reductions everywhere, including security," says Nachreiner. "These AI/ML systems are good at separating the wheat from the chaff for security indicators and alerts, but you still need human incident responders to investigate the remaining highlights. However, as AI improves, even that may not be the case for long."

The skills profile for IT talent is evolving in the wake of these new AI/ML developments, and potentially not for the better. "We will have an increasingly sophisticated profile for cyber talent, with a focus not just on the technical but a strategic leader who can orchestrate complex technology and business processes that can match the cyber arms race with AI-enabled attackers," says Dixon.

Aldridge agrees: "organisations now need professionals who are proficient in, and knowledgeable about, these new tools on top of the usually required cybersecurity skills. This trend is also revealing the unsustainability of mainstream hiring practices and the impossibly high demands most companies have. LinkedIn job descriptions and company announcements are now requiring that professionals have up to two years of ChatGPT experience, when the tool has only been available for a few months!"




Tools such as ChatGPT have brought about a monumental paradigm shift - however, it is unlikely that this technology could ever fully replace humans. Cybersecurity employees bring with them empathy and emotional intelligence, allowing them to understand psychology and the human errors that often lead to cybersecurity incidents.

"Humans can also contextualise and see the bigger picture around an event, something that is not easy for a machine to do, however smart it might be," says Hayward. "Furthermore, humans can make more ethical decisions by prioritising morality and human values over pure data and logic."

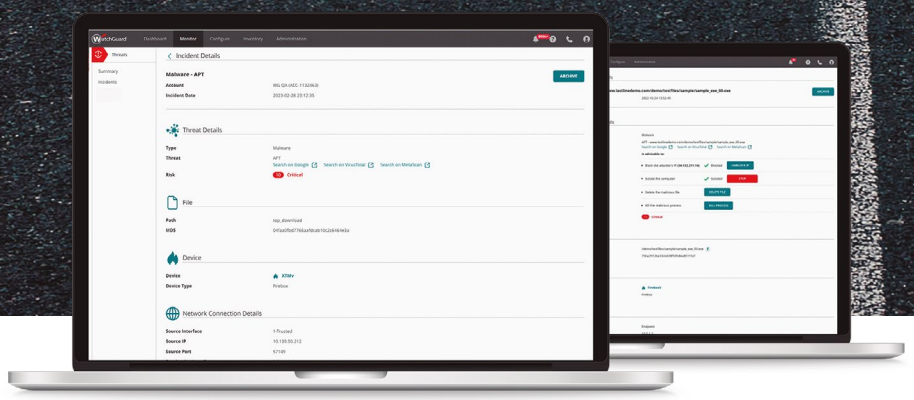
"Despite the rapid advances in AI technology, it will never replace the critical and creative thinking that human analysts bring to the cybersecurity sector," reports Hencinski. "We will see both attackers and defenders leverage these technologies, and it will up the tempo and scale of the attacks we see. But in the end, humans will be in the loop on both sides, just leveraging different aspects of the new tools at their disposal."

"ChatGPT and AI tools work based on deep neural networks, and can only respond on a predictive, not a proactive basis: without the initial human input, they would not be able to function on their own," explains Aldridge. "Crucially, they also lack the critical thinking and creativity that human brains have, the innovative power that drives novelty and growth in every sector, including cybersecurity." ■

# Access the XDR realm and unleash the power of unified security with WatchGuard ThreatSync®

XDR

WATCHGUARD THREATSYNC®




Streamline security operations and reduce the time and resources required to manage multiple security tools with our XDR-based, unified security approach.

Extend visibility, detect earlier, and respond faster with WatchGuard ThreatSync.

## Smart Security, Simply Done.

Email: uksales@watchguard.com Tel: +44 (0)20 3608 9070 www.watchguard.com/uk

# AI/ML cools Telehouse North DC

**Telehouse is a leading global data centre service provider, bringing together more than 3,000 business partners including carriers, mobile and content providers, enterprises, and financial services companies. The company provides reliable, secure, and flexible colocation, enabling organisations to accelerate speed to market and create business opportunities through fast, efficient, and secure interconnections.**

Telehouse puts sustainability at the heart of its data centres. The company strives to enable best practice operational performance across its data centre estate, concentrating resources where the most significant environmental improvements can be achieved. In addition to taking advantage of 100% renewable energy and complying with ISO standards for environment and energy management, Telehouse already takes full advantage of cloud, virtualisation, and innovative cooling to contribute towards efficiency. The company recognises that improving cooling efficiency is one of the most effective ways to optimise performance and secure environmental improvements.

## Expanding insightful data

Telehouse needed an environmental strategy to deliver against two challenges – enabling improved data centre performance while securing carbon reductions.

Accordingly, Telehouse engaged its services partner CBRE to identify next steps for its data centre performance optimisation programme. CBRE advised that Telehouse engage EkkoSense to deploy the EkkoSoft Critical AI-powered monitoring software. Backed by EkkoSense's specialist cooling optimisation skills, EkkoSoft Critical was considered an excellent solution to help Telehouse accelerate cooling and airflow optimisation across its UK data centres.

The goal was to secure continuous performance improvements around visibility, efficiency, and resilience, with the initial phase at Telehouse North – the company's oldest facility that opened in 1990. Target project outcomes included optimising cooling performance, removing potential thermal risk, and unlocking quantifiable carbon savings to support Telehouse's carbon reduction goals for 2022 and beyond.

The ML and AI-powered EkkoSense optimisation software works by monitoring, visualising, and analysing the performance of data centre facilities. It analyses thousands of temperatures and cooling points across the site in real-time to identify where levels of cooling can be tweaked, and dramatically increases the level of insightful data available to the operations team to remove risk and improve resilience.

Sensor deployment across the data halls provided Telehouse with the ability to monitor and identify performance improvements. If the temperature in a section of the data centre is outside the normal range, the sensors will flag this. The EkkoSoft Critical 3D visualisation and analytics platform continuously provides advice to the Telehouse team about adjusting cooling settings such as fan speed adjustments, cooling set points, floor grille placements etc. – resulting in quantifiable cooling energy savings and a reduction in carbon emissions.

Presenting all this ML data in a comprehensive 3D view makes it much easier to visualise the complex thermal performance of the thousands of racks deployed. With the EkkoSense software now collecting 3,000 data points every five minutes, the millions of data points already collected contribute directly to the effectiveness of ML algorithms to support continuous improvement in cooling energy usage and overall energy savings.

## Addressing corporate sustainability requirements

Deploying EkkoSoft Critical at Telehouse North has performed ahead of target and succeeded in improving quantifiable energy savings and carbon emission reductions.

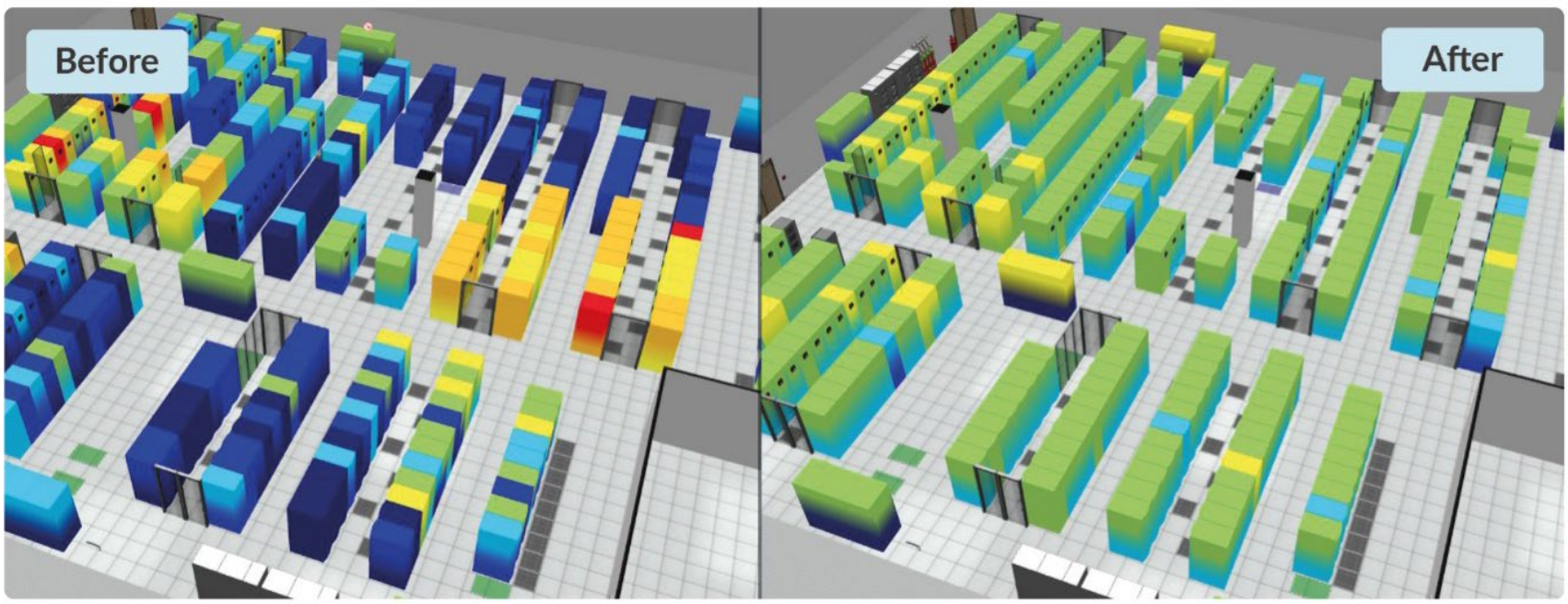
"It's very difficult to manually inspect every element of a data centre to identify inefficiencies and make improvements," said Telehouse's senior operations director, Paul Lewis. "EkkoSoft Critical provides us with a highly granular level of data and visualisation to help support our green agenda - and ensure our customers meet their sustainability targets. We've already made significant carbon emission reductions from our initial rollout of EkkoSoft Critical at Telehouse North, and we're eager to implement the software around our wider campus to extend these capabilities."

On first engagement, EkkoSense identified that a potential 10% saving against cooling load saving was achievable from optimising data centre cooling at Telehouse North. This cooling energy saving will enable Telehouse to achieve an anticipated 461 tonnes reduction in CO2 emissions.

The success of the trial forms a new chapter in a long line of sustainability wins for Telehouse. The organisation powered the world's very first multi-storey adiabatic cooling system in 2016, its North Two data centre is certified to the BREEAM excellent standard, and all its sites are supplied with 100% renewable energy. Rolling out EkkoSense to Telehouse's other London sites will help extend the company's focus and commitment to ongoing sustainability.

EkkoSoft Critical also proved to be especially valuable for Telehouse at a time of record-breaking temperatures in the UK. During July and August 2022, the software helped Telehouse's data centre team to monitor and protect equipment and maintain uptime. The 3D visualisation enabled Telehouse to identify potential thermal hotspots before they became an issue during the 2022 heatwave. EkkoSoft Critical was also able to highlight areas that were being over-cooled, presenting further opportunities for energy saving and carbon reduction.

Telehouse is now exploring how the solution can be used to improve capacity management processes, identify any capacity constraints, and better quantify available capacity. ■



# CFD enables smarter DC cooling

Iomart are a world-leading cloud computing, managed services, and co-location provider with 13 data centres in the UK, all connected to their own high speed dark fibre network.

As a publicly listed company with over £100 million+ in annual revenue and growing, the business demands that its supporting infrastructure is of the highest resiliency while also supporting its ambitious sustainability and environmental goals.

## Upgrading facilities

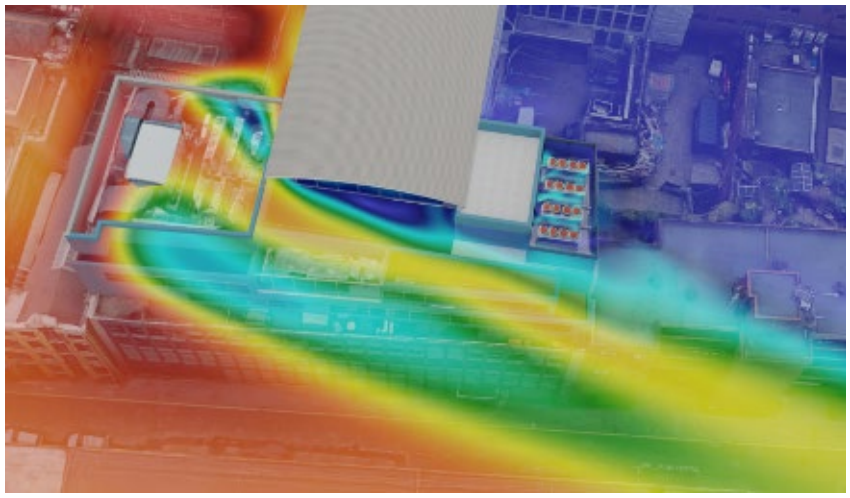
A planned lifecycle upgrade for one of their existing facilities was due and initial design works had been completed to provide the facility with new cooling infrastructure, offering higher efficiencies and a greater level of resiliency for the facility.

Sudlows was appointed to deliver the upgrade. Its data centre design, engineering and construction teams worked closely with iomart, their designers, and their site operations team to ensure the project was completed smoothly with minimal impact to the operations of the live facility and critically, with no downtime.

The project centred around the replacement of 4 No. existing water-cooled chillers, located internally within the building, with 2 No. new central chiller plant systems consisting of a total of 7 No. new Mitsubishi Electric inverter scroll and modular air-cooled water chillers.

Each plant area was to be contained within an acoustic enclosure to ensure that the planning conditions were met, however the design of these within the limited plant space required critical attention to the air flow characteristics to ensure that full capacity operation was always maintained.

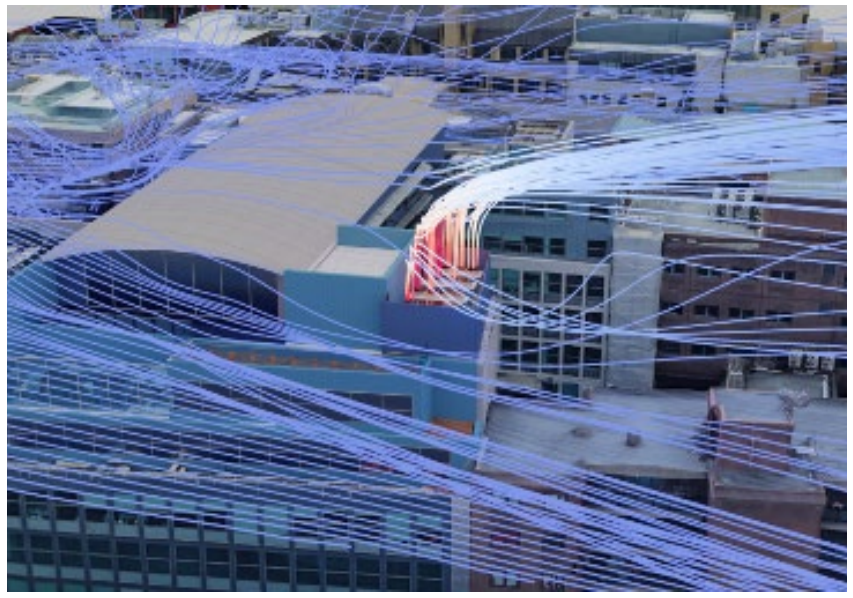
A model for simulation was produced from the design stage BIM model, with critical features affecting air flow being a focal point for detailed modelling. The surrounding buildings and urban environment were also to be considered from a combination of airborne laser scanned surface data and onsite point clouds to allow for a detailed model to be generated and for assessment of both the local and larger scale air dynamics which may affect the plant operation.



## Designed for heat

A key driver for the project was to ensure that full consideration had been given to the air flow required for the proposed chiller plant at peak ambient temperatures. Doing this during the design stage ensures that any necessary improvements can be implemented with minimal cost.

The site's location in central London means that there are many surrounding buildings which affect the air flow, and the density of development is known to result in an elevated temperature within the local micro-climate due to heat output from neighbouring buildings and the increased surface area absorbing solar energy. The requirement for an enclosed acoustic enclosure introduces further challenges as it can present a barrier to the fresh air flow required for the heat rejection to operate with stability.



Because of these risks and challenges, computational fluid dynamics (CFD) offered the best tool to be able to model the plant, proposed installation, and extreme design conditions to ensure that the equipment remained able to operate without compromise during peak ambient conditions, considerate of the local environment and potential wind and building eddy interactions. The simulations and the subsequent investigations, analysis and optimisation were a critical part of the design stage and supported the ultimate successful delivery of the project.

Initial results from the first design iteration were found to be unfavourable in a small number of conditions, with recirculation possible between the intake and exhaust sections of the acoustic enclosure. In response to the simulation outcomes, changes were made to the proposed design to mitigate these issues and a subsequent simulation was produced which demonstrated an improved air flow pattern which improved the fresh air supply substantially.

The final model was comprehensive and ensured a high degree of accuracy from the output simulations. Without such design optimisation, the heat rejection systems would not only have potentially struggled at high temperatures but would also have operated at a lower overall efficiency during lower temperature days.

Thanks to this technique, the final solution is not only a highly resilient installation but also a highly efficient solution too, resulting in a tangible ROI on the CFD exercise over and above the additional confidence gained from it. The facility now benefits from an enhanced cooling infrastructure, and the benefit of knowing that adverse ambient conditions and wind velocities have been considered as part of the design process, and potential issues mitigated wherever possible.

"This project is a great example of using CFD to ensure that not only is an installation able to perform at peak ambient conditions, but that efficiency in operation has been maximised throughout the year by mitigating the risk of recirculation. The quality of the analysis undertaken by the Simulation and Modelling Team was critical to the overall success of the project," said Zac Potts, head of sustainability at Sudlows. ■

# ‘Unbreakable connectivity’ pilots begin

The East of England Ambulance Service NHS Trust will become the first ambulance service to pilot a new technology that provides robust connectivity for ambulance crews and vehicles, including in areas where traditional cellular connectivity is impossible.

The Hybrid Connex Digital Ambulance of the Future Project is working with the NHS to provide the UK ambulance sector with a resilient connectivity solution which combines 4G, 5G and satellite so the crew onboard the vehicle will never be offline. 5G will be the primary connection, falling back to 4G when 5G is not available and then onto satellite connectivity in deep rural locations and areas with no coverage at all. The Hybrid Connex technology amalgamates software, cutting-edge hardware, and cellular and satellite services into one package that effectively creates unbreakable, permanent connectivity.

Complementing the next phase of the Ambulance Radio Programme (ARP) rollout (part of the Emergency Services Network) this advanced level of connectivity for ambulance services will:

- Open the door to new patient care pathways, taking advantage of digital advances.
- Increase the range of point-of-contact diagnostic services and tests that ambulance crews can carry out on-the-spot, without taking patients to hospital.
- Be better prepared and able to take advantage of developments in telemedicine and video technology.
- Ensure that crews can quickly and easily access immediate clinical information through electronic patient records.
- Enable crews to remain in constant contact with specialists about patients and their conditions en-route to receiving hospitals.
- Enable crews to locate patients faster in areas where connectivity is compromised.
- Help crews find key information about local health and social care services at their fingertips, enabling them to signpost patients to more appropriate, alternative sources of health and care.
- Help fleet managers and financial managers within ambulance services handle the often-complex commercial aspects of connectivity - such as billing - in a much more efficient way.

“Thetford Forest is renowned among our crews as a complete dead spot for cellular connection so if I end up responding to a call in Thetford, without good knowledge of local services and no connectivity to access that information, I may end up transporting that patient to hospital because I was unaware a more suitable pathway was available,” said Philip Elvidge, electronic patient record clinical lead and paramedic at East of England Ambulance Service. “Another issue we face is how poor connectivity affects the telemetry on our cardiac monitors. For example, if you were diagnosing an myocardial infarction (MI) in a connectivity black spot you couldn’t then send the ECG off to a specialist consultant for review of the ECG changes prior to our arrival. I’ve had this exact issue in the past in areas where there has been very limited cellular connection. You find yourself having to drive up the road and around the corner to find a location where you’re able to send the ECG successfully. It wastes valuable time which is vital to the patient.”

Stroke is another key pathway where permanent connectivity could significantly improve patient outcomes. “With a solid connection we can have a genuinely effective video triage meaning the consultant can better assess the patient to rule in or out a stroke mimic. Those assessments are supposed to be rapid - less than ten minutes - there isn’t time to waste trying to get connected as the patient could deteriorate quickly – and if the specialist decides it is a stroke and not a mimic, we need to be on the road to a stroke unit and getting them treatment as soon as possible,” said Elvidge.

Another positive of having permanent connectivity within the ambulance vehicle is that it enables staff to catch up on their continued professional development (CPD) during times when they would otherwise simply be waiting, for example during extended hospital handover delays.

The pilot will involve six East of England ambulance vehicles and will be operational between August and October 2023, after which it will be fully evaluated and if successful, offered as a service to ambulance trusts. Other UK ambulance services are also currently being encouraged to pilot test the new technology completely free of charge.

“We are delighted to be working with East of England Ambulance Service and we hope to prove how this superior level of connectivity will enable all regional ambulance services to achieve so much more with technology, whether that is for the improvement of patient care or to achieve greater efficiency in their performance,” said Bethan Evans, chief operating officer at Excelerate Technology. “The resilience of the connection that we can now achieve is leading edge technology that is being adopted in the most advanced parts of the world and we can now deliver that capability to our emergency services customers in the UK, the ambulance sector and its patients being the primary beneficiary.” ■

# How to pick the best LAN cabling for your enterprise

*Ricardo Diaz, EMEA market development, CommScope*

Choosing the right LAN cabling for your enterprise can seem like a mine field. As network convergence, IT/OT, power/data – is ramping up, enterprise network infrastructures are under increasing pressure from external stakeholders to expand their networks. It's more crucial than ever to have a future-proof infrastructure platform to cope with expanding business needs.

## How to choose a structured cabling system?

When it comes to buying new products online, many consumers, me included, like to research to compare offers and look for recommendations. It's easy to find plenty of guidance online. However, when it comes to choosing a structured cabling system (SCS), detailed information on the subject is few and far between.

When choosing the best LAN cabling for your enterprise, the best place to start is by thinking 'what does my customer need?' – this should always drive the outline of the conversation.

## What will be the forecasted lifespan of the installation?

For a temporary site, it wouldn't be advisable to go for a high-end solution, however reliability is an imperative, so the recommendation would be to choose a Cat 5e copper cabling from a reputable vendor. For an installation where lifespan isn't foreseeable, Cat 6A would be the most sensible choice.

## What's the size of the building?

In a small building, one or a few telecom rooms (TRs) may be enough to service all areas. Usually, fibre optic is used to link each TR to the main telecom room (MTR), but this is not a firm rule.

However, it's a different case in a multistorey building or a multi-building campus, where it is imperative for a 'campus backbone' to communicate buildings (usually with outdoor plant fibre cabling) and building backbones to link TRs to the MTR. It's recommended to use Class OM3 or above (OM4, OM5) to provide support for longer distances and future readiness. Single mode fibre is becoming trendy, but inside buildings it's rarely worth the extra investment on the associated electronics.

## What's the type of industry the building belongs to?

Some industry-specific standards include stricter performance specifications. For instance, to support distributed building services ISO/IEC11801.6 calls for Cat 6A performance. Equally, healthcare or education installations may also have their own requirements, depending on the country or region.

## Will you need to support advanced wireless access points (such as 5G DAS or WiFi 6 or above)?

If yes, there are two recommendations: designing a zoned layout and choosing Cat 6A for the horizontal copper cabling. Any other solution will not be flexible or scalable enough and we get short on bandwidth.

## Are you planning to converge your IT and OT networks? Do you need your cabling to transmit power as well (PoE)?

Zoned service areas are a necessity. When it comes to basic IoT devices on the ceiling (sensors, lighting fixtures) these may not need the top-performing solutions, but others, such as 4K PTZ surveillance cameras or wireless APs will. In any case, it's desirable for the system to last for as long as possible, serving multiple generations of equipment, therefore it's important not to underestimate future needs.

PoE is one other aspect to factor in, the higher the category, the more power it can provide to the end devices with less heating. If the answer to the above two questions is 'yes,' Cat 6A is the best choice.

## What support network do you need?

When you buy any new product, you'll want to get first-class post-sales support. The choice of vendor and installation partner will certainly have an impact on that consideration.

Similarly, the performance of your system should be guaranteed and backed up by a thorough documentation that details how each application will operate along the system's life. If any incident happens, it would be good that the labour to fix the issue is included in the warranty.

## Can sustainability be a factor when choosing LAN cabling?

Regardless of the chosen system, the cabling elements will all be made from copper or other metals, plastic, or glass (fibre optic), but best practice is to ensure that your new system can last for decades. Preventing the need to replace or expand – making the solution more sustainable. ■

***PRODUCTS***

The **Cable Matters** Cat6 Snagless Network Patch Cable delivers connectivity to computers and network components, such as routers, switch boxes, network printers, network-attached storage (NAS) devices, VoIP phones, and PoE devices.

This cable supports up to 550MHz and is suitable for Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet. All Cable Matters Cat6 cables are made of 24AWG bare copper wire as opposed to copper clad aluminium (CCA) wire, therefore fully compliant with UL Code 444, which requires pure bare copper wire in communications cables.

The cable meets or exceeds Category 6 performance in compliance with the TIA/EIA 568-C.2 standard. The connectors feature gold-plated contacts and strain-relief boots to provide durability and ensure a secure connection.

**JuicEBitz** CAT6 Shielded RJ45 Network LAN SFTP Patch Cable LSZH provides a fast and reliable wired internet or network connection between hundreds of LAN devices including computers, laptops, games consoles, routers, switches and more. With backward compliance to CAT5 / CAT5e, the cables are perfect for office installation and come with a lifetime warranty.

Each cable is fully shielded to effectively reduce the potential for cross-talk and interference including electronic (EMI) and radio (RMI). Double shielding is used for the high-performance cables, as well as Low Smoke Zero Halogen (LSZH / LS0H) instead of PVC for the outer sheath, which means that it has enhanced fire protection performance. Low-smoke zero-halogen material is becoming very popular and can be required when the safety of people and equipment is critical. The cable also features a shielded, gold-plated modular connector for extra protection.

The heavy duty, fully shielded CAT6 Cables are made from 26AWG 100% pure copper and a custom moulded design. A high density 6.5mm diameter Low Smoke Zero Halogen (LSZH) cable keeps everything in place and ensures practical installations to all environments.

The CAT6 (Category 6) specification means the cables can perform with speeds of at least 1000Mbps which makes them well-suited for demanding high-speed local area networks in an office or industrial environment. At 250MHz, these cables are suitable for 10BASE-T, 100BASE-TX (Fast Ethernet), 1000BASE-T/1000BASE-TX (Gigabit Ethernet), and 10GBASE-T (10-Gigabit Ethernet).

The **Jadaol** Cat6 Snagless Network Patch Cable offers universal connectivity to computers and network components, such as routers, switch boxes, network printers, network attached storage (NAS) devices, VoIP phones.

Jadaol Cat 6 patch cables are available in 10 different colours and in various lengths ranging from 1-150ft, enabling enterprises to colour-code, customise, and organise their network.

This cable supports up to 250MHz and is suitable for Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet. All Jadaol Cat6 cables are made of 100% bare copper wire as opposed to copper clad aluminium (CCA) wire and are therefore fully compliant with UL Code 444.

The CAT6 4-Pair UTP type cable features an outside diameter 5.8 ± 0.3 mm (0.23 ± 0.01 inch), a connector type RJ45, 50 micron gold plated contact plating, and a conductor gauge 32AWG. Further specifications include a stranded cable structure, Power over Ethernet and VoIP Compliance, and UL Listed, TIA/EIA 568-C.2 verified, RoHS compliant.

The **PatchSee** Cat6 RJ45 Ethernet Cable comes with optical fibre identification. Available in six lengths from 0.6m to 4.9m, the cable conforms to EIA/TIA 568-B2.2-1 category 6 and comes with a 25-year guarantee for use in category 6 channels inter-operable with any cabling system.

PatchSee Cat6 RJ45 Ethernet Cable features a black sheath and grey boot to distinguish it from black booted category 5e patch cords and is compatible with colour coded PatchClips for the first level of identification. All PatchSee cables are 100% tested for electrical and optical properties, with each cable identified by a unique serial number. The PatchSee Cat6 RJ45 Ethernet Cable comes with plastic cross-web unshielded (UTP) and individually foil shielded pairs (FTP), as well as a PVC sheath for UTP cables and zero halogens (LSOH) sheath for FTP cables.

Ultra Clarity Cables cat6 ethernet patch cables are used for wired home and office networks, data transfer and phone lines and have been designed specifically for Gigabit ethernet applications.

They perform at high-data transfer rates, provide exceptional transmission performance with low signal losses, support frequencies of up to 500MHz, and are suitable for high-speed 10GBASE-T internet connection for LAN network applications such as PCs, servers, printers, routers, switch boxes, and more, while remaining fully backward compatible with the existing network.

The cat6 ethernet cable features eight stranded bare copper conductors 24AWG. Each of the four unshielded twisted pairs (UTP) are separated by a PE cross insulation to isolate pairs and prevent crosstalk and covered by a 5.8mm PVC jacket with RJ45 connectors and gold-plated contacts. It is UL listed, complies with TIA/EIA 568-B.2, is ETL verified and RoHS compliant.

Ultra Clarity Cables with CM grade PVC jacket is UL listed, complies with TIA/EIA 568-C.2, is ETL verified and RoHS compliant.

# Please meet...

*Richard Massey, vice president sales EMEA, Arcserve*

## Which law would you most like to change?

In my work, I am very closely associated with the threat and effects of cybercrime and often see the devastation this can bring to businesses and people. I suppose it isn't a law, but I would love to see a situation where everyone must train to protect themselves from cyber-attacks. Most breaches occur when cyber-criminals trick users, and there are some simple techniques that everyone should know to make it harder for criminals to win.

## Who was your hero when you were growing up?

Am I allowed two? I am a comic-book superhero fan, but my favourite will always be Batman. He had no super-human powers, but he always found a way of helping people. It always made him more special to me. He didn't fly or have super strength – he had to use his wits and the skills he developed. Like the rest of us do, I guess!

My real-life hero is my dad. He was a farmer, and he never took a holiday. He worked hard day and night, looking after the land and the animals, and he instilled in me a fantastic work ethic that has served me well throughout my education, career, and life.

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

A former manager whom I had much time for said don't stress over the things you can't control. When he put me in a senior position, he said, "I know you can do the job, but I am worried about the stress it could cause you. Work out what you can control, and don't stress about what you can't."

It is so true. You can lose a sale, or even a long-term account, for all sorts of reasons that are out of your control. Of course, you still must make targets, but there is no sense in expending energy on something unachievable, whatever you do. Hard work will always pay off in the long-term, if you work with a strong team who can support you.

Making mistakes is part of life. Once something is done – it's done. You can't change it; you can only learn from it and move on.

## If you had to work in a different industry, which would you choose?

I would go into the film industry as a writer or director. I love the idea of being in control of telling a great story.

## What did you want to be when you were growing up?

Of course, when I was very young, I wanted to be a farmer like my dad. But as I grew older, I developed a passion for film-making and wanted to be a writer/director. I even wrote an entire script

## What was your big career break?

Another thing I learned from my father was that to get on, there is no such thing as luck. You get what you want through hard work and practice. Even in college, when I was working three jobs simultaneously, I was always looking for opportunities to learn and take on more responsibilities.

A massive break for me was working as a sales development trainer for Epson. I would visit retailers like PC World and Currys to train staff on how to sell the products. One of the account management team salespeople went on maternity leave, and I offered to step in and cover her role, without extra pay, just for the experience. It worked! When she returned from maternity leave, I was offered a full-time position in the account management team, and this was the start of my exciting and fulfilling journey in corporate sales.

## If you could dine with any famous person, past or present, who would you choose?

Quentin Tarantino! I love his films so much. What he has produced is not just about what you see in front of you on the screen. I would love to talk to him about how he gets his ideas and brings them to life on the big screen. His imagination is incredible, and I would love to know more about where this comes from and how he can tell his stories in such a vivid and entertaining way.

I suggest showing him a script developed by a young me to see what he thinks!

If there is an extra place at the table, I would love to invite the inimitable Brian Clough. I grew up in Derby, and Brian Clough is part of the DNA of anyone growing up there in the 1970s. I even met him on the bus! He was an interesting character who loved people but had no time for fools. I would enjoy asking for tips on management from the master.

## What's the greatest technological advancement in your lifetime?

The way communication has improved in my life is incredible. But the one moment of technological advancement heralding this is the first text sent from one network to another. It has driven how we all work and play today and allows us to do much more as a society. ■