NETWORK+

The hidden dangers of shadow IT

Unapproved SaaS tools upping risks

Kirk Jensen, WatchGuard, p5

DR planning is essential

The scale of cyberattacks is a major concern

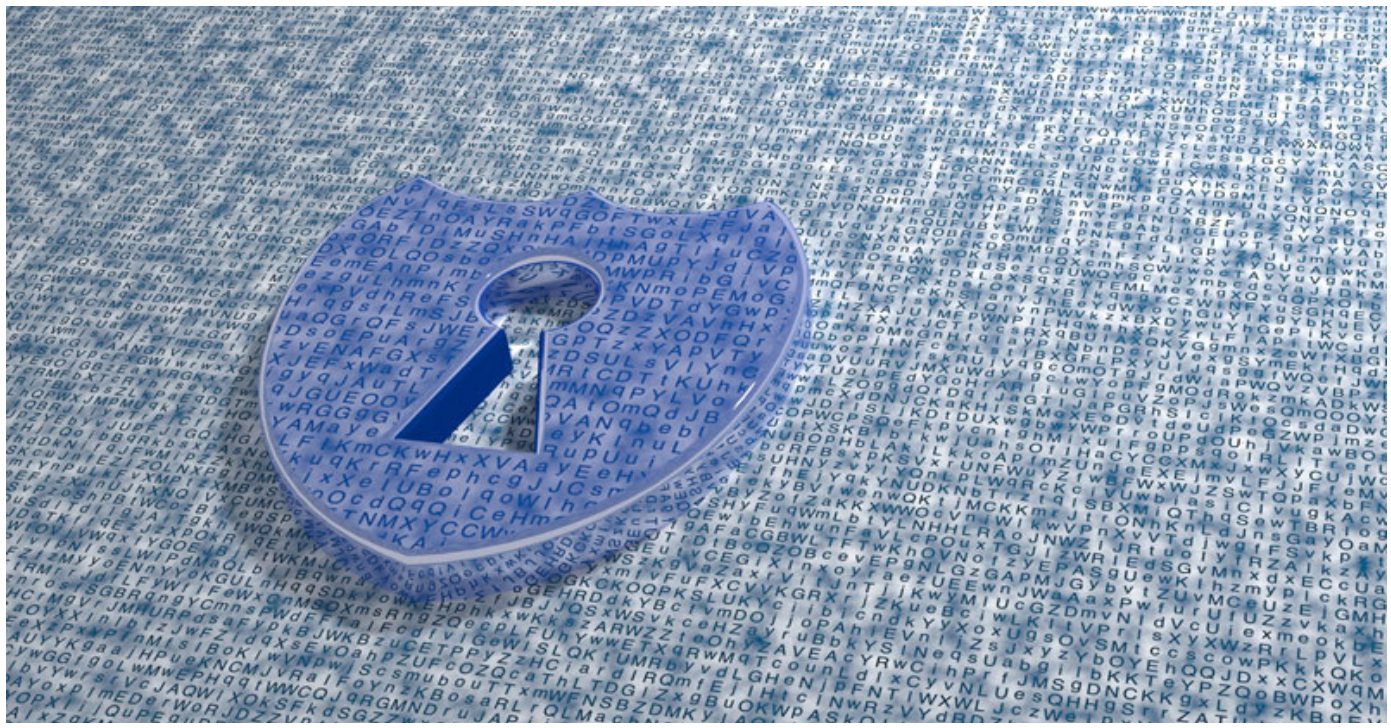
Stephen Young, Assurestor, p9

Questions and answers

Renewable energy is the place to be

John McKindland, Sona Business, p16

Why UK enterprises mustn't ignore NIS2



The EU's new Network and Information Security Directive (NIS2) came into force on 17 October – and while not directly applicable to UK enterprises, its impact will still be felt.

Building on the original 2016 directive, NIS2 expands across critical sectors including energy, healthcare, transport and digital infrastructure and introduces stricter requirements for organisations classified as either 'essential' or 'important' entities. Key provisions include mandatory risk assessments, enhanced supply chain security measures and a robust incident reporting process. With its implementation, organisations with more than 50 employees or an annual turnover exceeding €10 million are now required to improve their security measures.

This scope will require a significant number of UK organisations with EU connections to assess their compliance to avoid disruption with European partners, particularly since the EU remains the UK's most important trading partner, accounting for 42% of UK exports and 52% of imports.

"Many more UK organisations than you might expect collaborate with European partners. UK organisations must act swiftly to determine if the NIS2 Directive applies to their operations," reports Keith Poyser, Vice President for EMEA at Horizon3.ai.

Ernst & Young highlights that a key difference between NIS2 and its predecessor is the introduction of personal accountability - in the case of UK companies, this could separate them from their EU partners.

"Take a British cloud provider serving customers in France. If they do not comply with NIS2 standards and a breach occurs, the executives of the French company face significant fines. This could lead to substantial business losses for British firms that have not addressed NIS2. British executives need to improve their compliance now to avoid these serious risks," explains Poyser.

So what actions can UK IT teams take to ensure compliance and retain EU-business?

"Identity Security is going to take centre stage from a compliance point of view here, as it involves constantly checking and authorising both internal and external users, following Zero Trust principles," says David Higgins, Senior Director, Field Technology Office at CyberArk. "This is especially important since organisations have to protect a huge network of threats under NIS2, including subcontractors and service providers. Companies also need to tick off important NIS2 Article 21 requirements related to handling and reporting incidents. Having a solid Identity Security strategy is important here, to not only protect vital infrastructure against those inevitable future attacks, but also to track and manage the handling of critical information in real-time."

Meanwhile, Bart Salaets, Field CTO EMEA at F5, says that "to navigate the legislation, organisations should create centralised visibility and unified reporting across security platforms. The need for integrated solutions and sophisticated reporting tools - potentially AI-driven - will be essential in helping organisations meet their reporting obligations under NIS2."

It's not all doom and gloom though – with the stricter new regulations comes an opportunity for some of the UK's best and brightest to expand their business with European partners.

"Implementing the required changes will not only ensure organisations are attractive business partners and avoid unwelcome fines and negative publicity, but it will also bring new opportunities to enhance cyber resilience and overall security posture," says Simon Fisher, Senior Advisory Services Consultant, Orange Cyberdefense. "With finances remaining tight – especially in advance of the UK government's upcoming budget – IT and security leaders should use these regulations to reiterate the importance of cybersecurity and compliance to the board. This should help them unlock additional budget to stay ahead of the incoming regulations by investing in comprehensive cyber risk assessments, integrated incident reporting, cyber resilience testing and cross-framework governance." ■

IN DEPTH: Storage p7-8

Trinny London transforms data flow with Fivetran

Trinny London, the beauty brand founded by Trinny Woodall, has transformed its data operations using Fivetran's platform. By automating its data processes, Trinny London has gained the equivalent efficiency of an entire data engineering team, resulting in annual savings of up to £260,000.

As one of Europe's fastest-growing beauty brands, Trinny London has rapidly expanded from a thriving e-commerce platform to a global retail presence across the UK, Ireland, Australia, and the US. However, its previous data stack was overwhelmed by the company's growth, and existing data integration processes were outdated and inefficient. Trinny London also needed to migrate its database from the US to the UK to comply with GDPR regulations. Given its reliance on an online presence, these data challenges presented a significant barrier to growth. To remain at the forefront of the beauty industry, Trinny London turned to Fivetran to optimise and streamline its data movement, ensuring data accessibility across all departments.

"With Fivetran, we can finally focus on what we love – tackling new and exciting challenges," said Holly Foster, Data Lead, Trinny London. "Everything runs smoothly and just works. Whenever we reach out to the team, they're ready to assist. It's always been a collaborative effort, and that's what we appreciate most about Fivetran – it feels like a true partnership."

Within days of deploying Fivetran, Trinny London had a fully automated and reliable data movement solution in place. Over 50% of Trinny London's employees now have self-serve access to data, eliminating bottlenecks and boosting business agility. Additionally, with over twenty Fivetran connectors integrated into its data stack, the brand has gained full visibility across marketing platforms, optimising cross-channel campaign performance.

Trinny London's data culture has also undergone a major transformation. Supported by Fivetran, this proactive approach has enhanced the company's understanding of data's role in strategy building, enabling teams to make informed projections and create long-term plans. Meanwhile, the data team can focus on high-level strategic projects instead of constantly building pipelines.

"As a global online brand, it's vital that Trinny London's data operations run as smoothly and efficiently as possible," said Stephen Mulholland, Regional Vice President, EMEA, at Fivetran. "It's been great helping the data team achieve this goal to drive further business growth and democratise data access across the whole company." ■

Bedfordshire and Cleveland lead the UK on cybercrime risk

New research has revealed the UK areas most at risk of cybercrime, with Bedfordshire coming out on top.

The study by Freename analysed the latest data from the National Fraud and Cyber Crime Reporting Centre to see which UK police forces reported the highest levels of cybercrime as a percentage of all cybercrime and fraud reporting in the past 12 months.

In the areas of the UK most at risk, it found that Bedfordshire was the most at risk of cybercrime.

Of the total 6,901 cases reported to Bedfordshire Police, 2,918 or 42.28% were cybercrimes. Cleveland takes second place on the list, with Cleveland Police reporting 2,527 fraud and cybercrimes in the past 12 months, with 456 or 18.05%, being cybercrimes. Coming in third place is Staffordshire. Staffordshire Police data shows that of the 6,332 total fraud and cyber-crimes reported in the past 12 months, 1,025 or 16.19%, were cybercrimes.

"Scams in general are getting a lot more sophisticated these days, with many attempting to manipulate victims by disguising themselves as platforms we use every day," said commenting on the findings, Davide Vicini, CEO at Freename. "This, alongside some scammers even beginning to use AI to trick people, is an important reason to stay vigilant online, and this can be done by doing things like double-checking links you click, keeping strong passwords, and always attempting to find as much information as possible about who is using your data." ■

Rank	Police force	Total reports of all fraud and cyber crimes (past 12 months)	Cyber crimes reported	Percentage of cyber crime as total
1	Bedfordshire Police	6,901	2,918	42.28%
2	Cleveland Police	2,527	456	18.05%
3	Staffordshire Police	6,332	1,025	16.19%
4	Greater Manchester Police	16,916	2,675	15.81%
5	Warwickshire Police	3,197	501	15.67%
6	Hertfordshire Constabulary	8,125	1,266	15.58%
7	Merseyside Police	7,120	1,103	15.49%
8	Northumbria Police	5,995	926	15.45%
9	Lancashire Constabulary	7,950	1,214	15.27%
10	Gloucestershire Constabulary	3,283	496	15.11%

US targets UK data centre market

Four US-based companies are set to invest £6.3 billion in UK data centre infrastructure. The planned investments from Cloud HQ, CyrusOne, CoreWeave, and ServiceNow were announced as part of the UK government's investment summit.

Technology secretary Peter Kyle described the investments as "a vote of confidence in Britain."

"Data centres power our day-to-day lives and boost innovation in growing sectors like AI. This is why only last month, I took steps to class UK data centres as Critical National Infrastructure giving the industry the ultimate reassurance the UK will always be a safe home for their investment," said Kyle.

Washington DC-based CloudHQ confirmed at the summit that it is pressing ahead with a £1.9bn data centre campus at Didcot Power Station. DCD has previously reported the company is working with AWS to deliver the project, which was granted planning permission in 2021 and was set, at the time, to offer 84MW capacity.

"We are very excited to deliver a hyper-scale campus in the UK that is truly an extension of Slough due to our private diverse fibre optic route," said Hossein Fateh, CloudHQ's founder and CEO. "Our site enables us to build out our campus environment to provide scale and density to meet our customers' requirements."

CyrusOne, meanwhile, will spend an additional £2.5 billion in the UK over the coming years. It is planning a 90MW campus in Iver, Buckinghamshire, which would offer 63,000 sqm of data centre facilities in a plot of 16.59 hectares. The site will have 10 data halls across six buildings and include a new on-site substation. Plans, initially drawn up in 2022, were resubmitted earlier this year to ensure they comply with Iver's local plan.

"The UK government's recent CNI designation was a strong signal that data centres are of strategic importance to the UK economy," said Eric Schwartz, president and CEO at CyrusOne. "It has provided CyrusOne with the confidence to continue its expansion in the UK and support the government's policy ambition to become a centre of excellence for digital services, technology innovation, and AI."

ServiceNow will spend £1.15bn updating its existing UK data centres over the next five years, while AI data centre provider CoreWeave is investing another £750 million on infrastructure in Britain, on top of the £1 billion it pledged to invest in May. ■

UK's UC&C market heats up

The UK's unified collaboration and communications (UC&C) market is witnessing heightened competition, benefiting enterprise customers with a broader range of service options, according to GlobalData.

Providers are increasingly transitioning from on-premises to cloud-based solutions, enhancing flexibility and scalability. With the rise of AI-driven features, businesses are strategically selecting partners that offer both cost efficiency and innovative tools to improve collaboration and productivity in a rapidly evolving market landscape.

"The UK businesses have a wide choice of UC&C service providers as options expand to include former data network specialists adding cloud-based solutions to their offerings, and smaller niche players expanding their portfolios to gain greater share of customer wallet," said Robert Pritchard, Principal Analyst, Enterprise Technology & Services at GlobalData.

The journey from on-premises solutions to cloud-based services continues apace, with several service providers that had originally focused on providing data connectivity solutions now also targeting the cloud-based UC&C and contact centre markets.

The battle for market share is intense with a rocket boost to demand for collaboration tools during the COVID-19 pandemic. With most providers using the same base technology platforms, it has been hard for service providers to differentiate themselves, so the options have been price, customer service, and value-added features based on artificial intelligence, GenAI, and data analytics.

"Having seen market adoption accelerate during the pandemic with 'Zoom' entering the national lexicon, AI and GenAI are driving hype, change and new product development. This is also being accelerated by the January 2027 PSTN switch-off meaning that many legacy systems and services will no longer be usable," said Pritchard.

Collaboration services have proven their merit for facilitating internal and external communications across all locations, and they are increasingly being integrated with and complemented by unified contact centre services – so the choice of a reliable and trusted service provider partner is of strategic importance to businesses.

"Inevitably, UC&C services are a focus of GenAI-related speculation. Widespread fears of mass employee redundancies remain overblown. These new technologies should be seen as a complement to most existing roles, helping workers to be more productive, and to concentrate on improving the value-add they can offer to their company or organization," said Pritchard. ■

EDITORIAL:
Editor: Amy Saunders
amys@kadiumpublishing.com
Designer: Ian Curtis
Sub-editor: Gerry Moynihan
Contributors: James Moore, Kirk Jensen, Stephen Young, Fred Whipp, Duncan Swan, John McKindland

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

User behaviour named biggest cybersecurity challenge

The results of the 2024 Kaseya Security Survey are in and, overwhelmingly, IT professionals reported user behaviour as their biggest cybersecurity challenge.

Another important finding relates to the widespread adoption of AI by both threat actors and defenders. The survey found that feelings are mixed as IT professionals learn to navigate this new industry game-changer. The results of the survey are featured in the Cybersecurity Survey Report 2024: Navigating the New Frontier of Cyber Challenges.

"Cybersecurity attacks are widespread and more sophisticated, and as a result, are shaping business and IT strategies," said Chris McKie, VP, Product Marketing-Security at Kaseya. "IT professionals are navigating this new frontier as they try to find a balance between cybersecurity needs against hybrid workforces, dependency on cloud-based applications and services, and the role of artificial intelligence in cyberattacks."

89% of respondents cited a lack of training or bad user behaviour as their main cybersecurity problem. User-related security issues cause the most distress for IT professionals with poor user practices and gullibility (45%) and lack of end-user cybersecurity training (44%) as the root causes for cybersecurity problems. When asked which cybersecurity issues have impacted their business, phishing ranked first at 58%, followed by computer viruses or malware at 44% and business email compromise at 34%.

Cybercriminals are leveraging advances in AI technology to launch more sophisticated cyberattacks at a faster pace than ever before. However, its role in cybersecurity is highly debated with critics questioning its current limitations and ever-evolving cybercriminal tactics. More than half of survey participants say they believe AI will help them be more secure. But one-third of the IT professionals surveyed said they're unsure about the impact AI may have on their company's security. More research and clarity around the benefits and limitations of AI as a cybersecurity tool is needed.

According to the survey, the most widely adopted cybersecurity frameworks are NIST (40%) and Zero Trust (36%). There is a trend in rising security maturity in response to increasingly sophisticated threats. Respondents have rigorously implemented an array of security solutions with antivirus software (87%), email/spam protection (79%), and file backup (70%) topping the list. Three out of five respondents have an incident response (IR) plan in place – but follow-through is needed. Only 37% of those surveyed reported that they confirm the efficacy of their plan with periodic drills, down from 46% last year. ■

66% of malware linked to state-funded attacks

New data released by Netskope Threat Labs has found that, over the past 12 months, 66% of the attributable malware targeted at its customers was linked to state-funded attack groups.

The largest share of malware attacks came from North Korean threat groups, with Chinese and Russian groups as second and third most prevalent. A growing number of attacks use cloud applications as a point of entry and exfiltration.

The research also reveals North Korea, China, and Russia's differing strategic objectives drive very different approaches to cyber attacks, leading to their widely varying 'market share' in the threat landscape.

Currently, North Korea accounts for the largest share of malware attacks globally. Unlike Russia and China, North Korea's campaigns are primarily financially motivated, leveraging cybercrime and cryptocurrency theft to fund military programmes. As a result, it targets non-specific population groups in its quest to maximise profits.

In contrast, Russia and China use cyberattacks to target their global adversaries' critical infrastructure and high-value targets to cause targeted but high-impact disruption and damage. Examples of such targets include NHS England and the Electoral Commission, both of which have been recently targeted in cyber-attacks. This means that Russia and China's share of overall malware attacks is smaller, but the national impact of their attacks has the potential to be more disruptive.

Recent research from Netskope Threat Labs has also found that approximately 50% of all global malware downloads now originate from popular cloud apps. The average global worker regularly interacts with 24 cloud apps each month, with Microsoft tools such as OneDrive (51%), SharePoint (28%) and Teams (22%) being highly favoured. The top cloud apps abused for malware download in the last 12 months are OneDrive (26%), GitHub (13%) and SharePoint (12%). Today's data further proves that businesses will need to enhance their security measures to cloud-native security systems to help prevent such malware attacks. ■

The 40th anniversary of the APC UPS: The journey of innovation continues

It's the piece of IT equipment that most of us take for granted, and it is sometimes forgotten in implementation plans. But it's also absolutely essential to bring reliability to IT operations by protecting everything from desktop PCs to servers to entire data centers.

Of course, we're talking about the uninterruptible power supply (UPS), and this year, we celebrate the 40th anniversary of the first UPS created by APC in 1984 – the 300PC. Now ubiquitous wherever you find IT equipment, UPS technology has grown in sophistication and capabilities thanks to numerous innovations along the way. It's a fundamental component of any new IT implementation or upgrade.

Over the decades, the UPS has grown in stature as IT teams and organizations have become increasingly dependent on data. Now, as the Internet of Things, Artificial Intelligence, and other data-intensive technologies infiltrate our lives, the UPS has never been more important

AI is powering an increasing array of mission-critical applications in every industry, from healthcare to education, manufacturing, logistics, and transportation.

APC started building a market 40 years ago with the 1984 introduction of our first UPS. Then, a few years later, in 1989, we revolutionized power management with the launch of PowerChute™ software, enabling the graceful shutdown of critical hardware and protecting the data on this hardware. The same year, we entered partnerships with two major IT distributors, which proved consequential in building our partner ecosystem.

Throughout the decades, we've continued to innovate. In 1990, we introduced the Smart-UPSTM brand of UPS, now considered the industry's premier network power protection solution. In 2004, we introduced the now industry-leading InfraStruXure architecture, the first scalable modular, energy-efficient, network-critical physical infrastructure (NCPI) architecture, which is an integral part of complete power and cooling systems. For a blast from the past, hop into the Way Back Machine to check out the original InfraStruXureTM offer.

The innovation journey continues

With our industry-leading EcoStruxure™ IT portfolio, our vendor-neutral data centre infrastructure management (DCIM) solutions enable our customers to operate the most resilient, secure, and sustainable IT infrastructure anywhere. We offer business continuity with secure monitoring, management, planning, and modeling from a single IT rack to hyper-scale IT, on-premises, in the cloud, and at the edge.

Other recent innovations include introducing products with recycled and recyclable materials to support your and your customers' sustainability strategies. We've also increased the use of lithium-ion batteries in UPS models, from small home office units to industrial-grade power-protection systems. Lithium-ion enables longer lifecycles and reduces footprint and maintenance costs, all of which contribute to the goal of decarbonization.

Building a sustainable future

Digitization and electrification are central to sustainability strategies across almost every industry. To support these efforts, we are investing in technologies such as the Smart-UPS™ Modular Ultra. The most sustainable UPS of its kind, it aligns with the growing demand for sustainable solutions and recycling programs.

We will continue to innovate as we look into the next 40 years and beyond. And we will continue to rely on you as trusted advisors to our customers to help us make an impact on the market. The journey continues. As in the past, we will walk it together. Please check out our 40th Anniversary website, 40 Years On, for the full innovation journey and see how we can help you evolve your business.

Cellnex UK and Netmore amp up infra sharing across UK

Cellnex UK has announced the new phase in its partnership with network operator, Netmore, to enhance the UK's low power wide area network coverage (LoRaWAN). The collaboration will see the installation of LoRaWAN gateways on Cellnex UK's existing streetwork sites.

This forms part of Cellnex UK's sustainable asset-sharing model, which allows operators to co-locate their equipment directly on Cellnex's existing infrastructure. This ultimately allows for greater flexibility, reduced costs and an enhanced connection for customers.

This model supports Netmore's network expansion, after being chosen by Yorkshire Water to replace 1.3 million water meters in one of Europe's largest LoRaWAN projects. Earlier this year, the companies successfully installed on 20 sites and building on this success, they plan to expand to an additional 200 sites.

"By leveraging our approach to sustainable asset-sharing, we are not only facilitating the rollout of Netmore's cutting-edge technology, but we are also able to ensure efficient and targeted wireless coverage and capacity for its customers," said Paul Stonadge, Commercial Director at Cellnex UK. "Cellnex UK's extensive infrastructure portfolio means we can provide connectivity exactly where it's needed, whilst also providing a cost-effective solution that allows Netmore to connect to a high volume of water meters."

"Cellnex UK's innovative method of repurposing street fixtures for network deployment and densification brings substantial value to Netmore as we continually seek ways to lower network delivery costs while maintaining top-tier connectivity services for our customers. The cost efficiencies provided by Cellnex UK directly enhance the speed and scale at which we can integrate devices, such as smart water meters, into our network. We are excited to extend our partnership in this region and beyond," said Dominic Murphy, Director of International Network Delivery at Netmore. ■

NCSC-backed cybersecurity badges launched by Scouts

Four new badge activities have been launched for the Scouts, backed by GCHQ's National Cyber Security Centre (NCSC), to help young people learn how to stay safe online.

The activities will form part of the Digital Citizen Badge and have been designed to teach children aged 8-14 how to protect their devices and keep their data safe. The new activities have been launched during Cyber Security Awareness Month to encourage in young people good cybersecurity habits.

The four activities for the Scouts are focused on strong passwords, recognising phishing emails, understanding fundamental cyber security principles and identifying the importance of regularly backing up key digital assets. The activities have been designed alongside cybersecurity experts from the NCSC.

"Keeping your digital assets safe is a key modern life skill and here at the Scouts we want to help young people develop digital skills as well as the more traditional teamwork, navigation and leaderships skills," said Sally Milner, Scout partnership manager. "In 2024, it's just as important to know how to keep your data safe as it is to work in a team or navigate using a map; it's our mission to help young people develop all these key skills, and others so they are fully equipped to live and operate effectively in the modern world."

"Empowering young people with the skills to navigate the digital world safely is crucial," said Sarah Lyons, NCSC deputy director for economy and society. "By equipping Scouts with essential knowledge about online safety, we help ensure they can protect themselves against cyber threats and make informed choices in an increasingly digital society." ■

IPI migrates pension provider People's Partnership to the cloud

IPI has enabled People's Partnership, the workplace pension provider, to move to a cloud-based Contact Centre solution from Genesys; part of a wider programme of change designed to improve operational efficiency and offer greater customer choice.

The People's Pension is used by one in five workers across the UK, with its Contact Centre team serving the needs of its members, advisors, and employers who sign up for workplace pension schemes. As part of a wider customer experience programme focused on becoming 'Fit for Future,' People's Partnership wanted to put technology at the core of the business.

IPI took a staged approach to implementation, with phase one including a migration of voice, email, and web chat, as well as the adoption of Workforce Engagement Management (WEM) capabilities such as customer sentiment analysis, knowledge management, Quality Management (QM), and Workforce Management (WFM). Third party applications, available through Genesys AppFoundry's online marketplace, have also been incorporated, including social engagement via PureSocial, and customer surveys powered by Medallia. ■

Word on the web...

Navigating the Cloud conundrum in an AI-driven world

James Moore, VP EMEA Sales, DoIT

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

The hidden dangers of shadow IT: how unapproved SaaS tools are putting businesses at risk

Kirk Jensen, senior product marketing manager, WatchGuard

In today's digital workplace, the rise of Software as a Service (SaaS) applications has dramatically transformed how businesses operate, enhancing flexibility and productivity.

However, unsanctioned use of these tools, often referred to as shadow IT or shadow SaaS, presents a significant and growing risk to corporate security. As employees turn to unapproved applications to accomplish their tasks, they inadvertently expose their organisations to a myriad of cybersecurity threats.

Recent findings underscore the magnitude of these risks, with 65% of companies suggesting the biggest risks they perceive include data loss due to shadow IT, while 62% report a lack of visibility and control over their digital environments as a major concern. Some 52% of 250 security professionals interviewed in the survey, conducted at the Infosecurity Europe event suggested data breaches are a deep concern when it comes to using unauthorised tools.

"When employees deploy these tools without oversight, they may inadvertently share sensitive information or fall victim to social engineering attacks, resulting in data breaches and account takeovers."

Alarmingly, one in ten companies suspect that such unapproved use of software has already resulted in a breach, highlighting the critical need for tighter security controls and oversight.

Further underlining the depth of the issue of shadow IT, the UK's National Cyber Security Centre (NCSC) released guidance in 2023 on how to better manage the problem.

From a cybersecurity perspective, the proliferation of shadow IT and shadow SaaS can severely undermine an organisation's security posture. Unsanctioned applications that bypass corporate IT controls often contain vulnerabilities that cybercriminals can exploit.

When employees deploy these tools without oversight, they may inadvertently share sensitive information or fall victim to social engineering attacks, resulting in data breaches and account takeovers. Furthermore, the lack of control associated with shadow IT creates an entry point for malicious code, which can increase a company's susceptibility to ransomware and other cyberattacks.

Operational challenges

Shadow IT also introduces significant operational challenges. When unauthorised software is used, organisations lose control over their systems, making it difficult to apply necessary security patches promptly. This leaves the door open for potential exploits and increases the organisation's exposure to cyber threats. For regulated entities, the risks extend even further. The use of unsanctioned IT activities can lead to non-compliance with regulatory requirements, potentially damaging a company's reputation and exposing it to legal penalties.

Companies need to adopt a more proactive approach to detect and manage unauthorised applications and services. The challenge is not just in identifying these tools but in effectively monitoring and mitigating the associated risks.

Effective risk management begins with maintaining a comprehensive and up-to-date catalogue of all technology resources, including employee-owned devices, and conducting regular reviews to ensure compliance and security.

To safeguard corporate systems, it is crucial for organisations to implement tools and scanning methods that detect unauthorised software and devices on the network. Advanced solutions that provide full network visibility can automatically discover all connected devices, map network structures and classify each device according to its level of risk. This approach not only minimises exposure to vulnerabilities but also strengthens an organisation's overall security stance.

As businesses continue to navigate the complexities of digital transformation, it is vital to recognise and address the hidden dangers posed by shadow IT. By enhancing visibility and control over their digital environments, organisations can protect their information, ensure compliance and maintain the integrity of their systems, even as the threat landscape evolves. ■

What are the common pitfalls organisations should avoid for successful IoT integration?

Fred Whipp, VP of business development, mpro5

Many industries are turning to the Internet of Things (IoT) for real-time monitoring, data-driven decision-making and streamlined automation. With the market predicted to soar from US$714.48 billion in 2024 to a staggering US$4,062.34 billion by 2032, achieving a compound annual growth rate (CAGR) of 24.3%, the potential for digital transformation is immense. However, to exploit this potential effectively, organisations must learn how to bypass a series of common pitfalls during IoT implementation and maintenance.

The IoT market is expanding rapidly - its growth underpinned by the increasing reliance on data for strategic decision-making. IoT solutions enable more efficient management of facilities as they offer significant advantages such as increased automation, real-time monitoring and enhanced data collection. This trend is evident in the UK, where Eseye's 2023 study found that 79% of respondents plan to ramp up their IoT deployments. Yet, successful integration begins with identifying the specific IoT use cases relevant to each enterprise.

"IoT solutions enable more efficient management of facilities as they offer significant advantages such as increased automation, real-time monitoring and enhanced data collection."

Identifying IoT use cases

Before organisations deploy IoT technology, they should first identify specific parts of their operations that are particularly vulnerable to problems or disruptions. These are areas where quick responses are crucial to maintaining smooth operations. Additionally, organisations should identify the functions that are essential for their overall business performance. These are the tasks or processes that, if disrupted, would have a significant negative impact on the business. Setting clear goals for how IoT will be used in these areas is vital. These goals should define what the organisation aims to achieve with IoT implementation and how it will improve the experience for customers.

Research by Beecham highlights that one of the most common reasons for IoT project failures among 25,000 respondents is the absence of clearly defined business objectives. Organisations need to establish precise IoT goals to guide the deployment and ensure it aligns with their broader business strategies. This level of transparency enhances the likelihood of successful implementation while also maximising the positive impact on customer experiences.

Common implementation pitfalls

A frequent issue in IoT deployment is the misapplication of cameras and sensors. Organisations often install these devices without specific goals in mind or use them retrospectively to address issues rather than proactively for prevention. Forward-thinking is therefore required to utilise IoT systems effectively, which positions them in preventative roles where they can capitalise on important features such as real-time feedback.

Another significant pitfall is the mismanagement of triggering actions. Some organisations record data without triggering appropriate actions, while others overuse alerts, leading to alert fatigue where real issues are overlooked. This results in a passive approach to data use, with either a lack of action triggers or an overabundance, both leading to an ineffective priority matrix.

Optimising IoT investment

IoT applications can vary widely across industries. In catering, retail, and facilities management, for example, sensor-driven maintenance can trigger workflows in response to irregularities, such as temperature fluctuations, thereby alerting staff promptly and reducing response times. Understanding and planning for effective IoT use cases before implementation significantly increases the chances of project success.

The cost of installing IoT cameras, sensors, and the necessary network infrastructure is substantial. To optimise IoT expenditure and maximise return on investment, businesses can turn to three fundamental rules: Alert, Action, and Resolution. Firstly, define the conditions for triggering alerts. Secondly, specify the actions to be taken once alerts are triggered. Finally, outline the process for recording and resolving issues. This structured approach helps to avoid overcomplication and ensures that IoT systems genuinely enhance business operations.

Enterprises embracing IoT

Enterprises across various sectors are utilising IoT technologies to enhance their business operations. This includes retailers where IoT integration has offered unprecedented opportunities to optimise operations, improve safety, and drive sustainable growth. Examples include dynamic cleaning with IoT sensors revolutionising traditional cleaning practices in stores by identifying high-traffic areas during peak hours while scheduling deeper cleanings for quieter periods.

Retailers are also embracing IoT technology for crowd control with IoT sensors monitoring the number of customers entering and exiting the store in real-time, enabling store managers to adjust staffing levels and manage queues efficiently during peak hours, proactively preventing overcrowding and optimising space usage. IoT cameras also serve as a proactive safety measure, detecting spillages and other hazards in real time, enabling timely interventions, and reducing the risk of accidents, liabilities, and associated costs.

Other sectors embracing IoT in the UK include the contract catering sector. Impactful IoT technologies, such as barcode scanners, temperature probes and RFID infrared readers, are being utilised before produce reaches caterers, tracking changes in temperature and moisture, impacting food quality across supply chains.

Food service enterprises are also using IoT technologies to improve food safety. Operators are moving away from manual paper-based processes and are investing in IoT sensors that regularly monitor the status and temperature of refrigeration equipment. Such devices send automated real-time alerts to catering managers' devices, whether on-site or not, allowing them to resolve fridge temperature emergencies and avoid food spoilage.

Lastly, IoT sensors are utilised by catering enterprises to detect when a fridge or freezer goes above certain temperatures - alerting members of staff before the problem worsens, saving businesses thousands a year.

Conclusion

It goes without saying that avoiding common pitfalls in IoT implementation is crucial for achieving the full benefits of this transformative technology. A well-defined IoT framework, clear business objectives and a proactive approach to data use are essential components of successful deployment. While the IoT market continues to grow, organisations that understand and overcome these complexities effectively will be well-positioned to drive digital transformation and gain a competitive edge. ■

Storage – does size matter?

When it comes to storing enterprise data, the most important deciding factor varies widely from company to company…

Data volumes are notoriously booming across the world – current estimates say that today, some 402.74 million terabytes (or 0.4 zettabytes) of data are generated each day. Statista suggests that by 2025, more than 180 zettabytes of data will be generated daily, while the IDC has a similar forecast of 175 zettabytes per day in the same timeframe. Clearly, data is a big, booming business – so how will the UK's enterprises manage?

Is bigger always better?

When it comes to enterprise data storage, it's arguable whether bigger is always better. While large storage capacities are important in many cases, there are several factors beyond sheer volume that organisations need to consider for an optimal storage solution.

"While having ample storage capacity is important, bigger isn't always better," says Judy Kaldenberg, Senior Vice President of Sales and Marketing at Nexsan. "The key is to balance capacity with performance, scalability and efficiency. Enterprises must consider how their data grows and changes, ensuring that their storage solutions can adapt accordingly. It's more about having the right storage solution that matches your needs rather than just opting for the largest capacity available."

"The more data you have, the more you can potentially draw value from – but the real power lies in how effectively that data is managed and utilised. Bigger isn't always better," agrees Tim Hood, VP of EMEA & APAC, Hyland Solutions. "Larger storage can unnecessarily ramp up storage costs, elongate processing times, and increase the risk of silos fragmenting useful information."

It's important to highlight that bigger does not necessarily equate to better performance, and that high-speed, low-latency access is crucial for many enterprise applications. Instead, enterprises should scale smart, not big: hybrid solutions offer the best of both worlds by balancing on-premise storage for critical workloads and cloud for scalable, less-critical data.

Rainer W. Kaese, Senior Manager Business Development Storage Products at Toshiba Electronics Europe, however, disagrees: "bigger is always better. Data to be stored is exploding, data is the fuel of the AI age. Nevertheless, there are secondary attributes which should not be neglected."

These include:

- Cost (per capacity): With the exploding need for storage capacity, the cost of storage plays an important role.
- Performance: HDDs are slower than flash memory-based storage. For high performance storages, flash memory-based storage may be the better option. However, for large online storage, companies would need systems with up to hundreds of HDDs; such a system, appropriately optimised, can combine the power of many (slow and cheap) HDDs into a performance that matches systems with few (fast but costly) SSDs – at a fraction of the cost per capacity.
- Power consumption and data centre footprint: Here, HDD based storage for large capacities in the PB range remain competitive/comparable to alternative technologies. Flash memory-based solutions offer significantly lower size/footprint and slightly lower power consumption - but the difference in cost would take dozens of years to amortise.

Empowering the enterprise

The type of storage that truly empowers businesses for data storage, processing, and utilisation varies depending on specific needs - but hybrid, flexible, and intelligent storage solutions offer the most comprehensive value.

"The ideal storage solution for businesses is one that offers a blend of scalability, performance and manageability," says Kaldenberg. "Solutions that leverage technologies like hybrid storage arrays, which combine flash and traditional spinning disks, often provide the best balance. They offer the speed and efficiency of flash for high-performance applications while maintaining the cost-effectiveness of disk storage for larger volumes of data. Additionally, intelligent data management features, such as robust data protection, are crucial for maximising security of data."

"Types of storage that can be accessed across the hybrid multi-cloud are giving firms far more options when it comes to placement of data, workloads and applications," agrees Mark Molyneux, EMEA CTO at Cohesity. "The old days of picking a monolithic storage array to store your data have drastically changed now, as firms are catering for many landing-zones depending on the requirements of their disparate businesses. Those firms 'born in the cloud' will naturally focus on cloud-provided storage technologies, but what if you are a well-established player with your own data centres and a variety of technologies, from new to heritage? You are likely meeting requirements for on-premise, for private cloud, and for public cloud, so selecting the storage mediums that are right for your business is critical. Whatever you choose to deploy, you need to ensure they feature the latest capabilities both technically and from a security perspective."

Enterprises can utilise smarter storage methods to make the most of their data by adopting technologies and strategies that enhance data access, management, processing, and utilisation. These methods go beyond simply storing data and focus instead on optimising how data is used to drive business insights, operational efficiency, and innovation.

Smart Tiering - the ability to place data correctly in accordance with a relevant record strategy, and with business requirements in mind – offers game-changing results to businesses. It controls the placement of data on primary storage

Judy Kaldenberg

which ensures the most expensive storage is only being used for the right purposes, while assisting in sustainability goals, day-to-day capacity management which aids future financial outlay.

"This also ensures you know exactly what data is where at any time, thereby controlling the often out-of-control secondary data mountain," explains Molyneux. "Organisations should consolidate their disparate application data silos into a single centralised data management platform that is based on a scalable hyper converged file system. In this case, the data stored will be automatically analysed by the deduplication and compression functions to achieve the highest reduction rates across the organisation."

Data reduction techniques, too, with compression and deduplication, have a role to play, enabling businesses to make better use of existing storage.

"Data reduction can massively help companies to store data more cost-effectively, since these mechanisms automatically reduce the amount of secondary data in the background as soon as it is generated, without anyone having to actively initiate the process," says Molyneux. "This pays off immediately when you take a close look at the costs. Although hardware is generally becoming cheaper because the disks provide more storage per euro, the operating costs drive the price up. According to an analysis by Nasuni, it costs $3,351 a year to store one TB of file data. Existing storage resources are protected by data reduction, so that investments in new storage resources can be postponed."

One size fits all?

When selecting storage, each individual enterprise must closely consider its specific business needs and use cases. Storage solutions should directly support the performance, scalability, data management, security, and cost requirements of the enterprise's current and future workloads.

But what's the single most important deciding factor? According to Kaese, it comes down to cost per capacity…

In contrast, Kaldenberg believes that immutability is the most critical factor – and one that is often overlooked: "data can be stored as immutable with WORM data storage or as an immutable data backup. Immutable backups have become increasingly important as malicious cyberattacks target backups as they ensure that your critical data remains tamper-proof. By implementing immutable backup storage, businesses can safeguard their most valuable data, providing peace of mind that backup integrity is never compromised."

Security is the most critical factor firms must consider when choosing the right storage technology, both from a protection/defence and recovery standpoint, as well as a compliance perspective, asserts Molyneux: "even if a platform offers the best performance at the lowest cost, weak security — like a 'Swiss cheese' full of holes — renders it a poor investment. Inadequate security not only wastes money but also exposes the business to far greater risks, including brand damage, loss of customer trust and confidence and costly regulatory fines."

Meanwhile, "as businesses grow and data volumes continue to surge, it's incredibly important that storage can scale efficiently with them – without compromising performance, accessibility, or security," opines Hood. "Without scalable solutions, businesses are capped as to just how far they can grow without compromising themselves in some way, whether they're wrestling with newly applicable regulations, a simple increase in data volumes, or more complex workflows. Scalable solutions also provide the flexibility to integrate emerging AI and automation technologies, which become more of a non-negotiable as each day passes – particularly in insurance and financial services. The capacity to adapt and expand ensures that data remains an asset, not a burden, as your business evolves."

Clearly, not only is storage not 'one size fits all,' neither is there a single most important factor in picking the right technology. Indeed, the 'right' storage depends on how well it fits the organisation's specific business needs — whether that's high-performance data processing, vast scalability, cost efficiency, compliance, or a combination of these.

"The type of storage that truly empowers businesses for data storage, processing, and utilisation varies depending on specific needs - but hybrid, flexible, and intelligent storage solutions offer the most comprehensive value."

Long-haul future-proofing

To future-proof storage for the long term, enterprises must adopt strategies and technologies that ensure flexibility, scalability, and adaptability.

"If data is the fuel of the new era, make sure you always have enough capacity to store the fuel," advises Kaese. "And make sure you can expand as you go. Data creation will not stop. If data creation continues and there is no space to store, valuable fuel will be lost. Hence, it's important to secure continuous storage expansion, as well as the safe and reliable maintenance of existing storage."

Adopting a hybrid cloud strategy, combining the scalability of cloud storage with the performance and control of on-premise infrastructure, offers flexibility for future growth. With such a strategy, critical, latency-sensitive data can be stored on-premise or in private clouds for optimal performance; while public cloud storage can be used for less critical, long-term, or archival data - and which can scale as data volumes grow.

"To truly future-proof their storage, enterprises need to focus on cloud-native, scalable solutions that offer flexibility, security, and seamless integration," confirms Hood. "With data privacy regulations becoming more complex, such a solution can offer a dramatically streamlined approach to information security, with cybersecurity and compliance updates entirely automated by a provider."

"Organisations should choose solutions that can grow with their data needs and data protection goals," agrees Kaldenberg. "By opting for technologies that support a variety of data types and workloads, they are better positioned to adapt to new technologies and standards easily. Additionally, implementing unified storage systems enables efficient management of both block and file storage within a single platform, enhancing flexibility and performance."

Of course, every enterprise must also consider investing in robust data security and compliance to address new threats and evolving regulations; ensuring that storage solutions are equipped to handle long-term needs.

"Enterprises should adopt a comprehensive strategy built on zero trust principles and prioritise data resiliency," says Molyneux. "By embedding fault tolerance through redundancy, companies can eliminate single points of failure, which enhances the longevity of storage systems. Critical data should be protected through immutability and configurable persistence, safeguarding it from ransomware attacks and ensuring that its confidentiality and integrity are maintained over time."

Future-proofing enterprise storage requires adopting scalable, flexible, and secure storage solutions that can adapt to evolving data demands and technological advancements. By regularly reviewing and updating the storage strategy, enterprises can maintain alignment with business goals and technological progress. ■

Rainer Kaese

Disaster recovery planning is key in the modern-day business environment

Stephen Young, Executive Director, Assurestor

The scale, destructiveness, frequency and cost of cyberattacks is a major concern for many organisations, with the cycle of deploying, upgrading and testing the latest security defences all-pervasive. Often overlooked in this seemingly never-ending cycle of prevention and protection are the nuances in what we call the 'recoverability factor,' a company's readiness to respond and recover from a major disaster.

But with 78% of senior IT professionals admitting that their organisation has lost data due to a system failure, human error or a cyberattack in the past 12 months in a recent Assurestor survey, there's a clear message here that protection measures are being breached regularly.

Knowing that at some point your data, and your business, will be threatened, focus then shifts from security and prevention to recovery. The operational, financial or reputational implications can be catastrophic, so reducing the amount of data impacted and the speed of recovering operational status becomes the priority.

However, just 54% of IT respondents felt confident that they could recover their data and mitigate downtime in a future disaster. Unfortunately, during a hectic recovery phase, there are no second chances to conceive a new disaster recovery strategy. Businesses must execute on the plan they have implemented.

Low confidence leaves questions

The fact that most survey respondents lack confidence in their own recovery systems is a concern, with almost 40% describing a lack of technical skills or expertise in-house, 29% pointing to a lack of investment or budget and 28% criticising the lack of senior support.

In isolation, this may leave many feeling uneasy, but when looked at in their entirety, it leaves organisations with significant questions about their ability to survive a serious data threat or significant downtime.

We only need to look at the recent global outage that affected organisations across multiple sectors, from airlines to healthcare. While not a traditional data breach, it's been estimated to cost businesses up to $1.5 billion and is proof that no-one can afford to be complacent.

Measuring business readiness

Currently, there is no way to measure business readiness to recover from a major data threat or system failure, with the worst possible outcome impacting the very viability of the business.

Recoverability is no longer a choice but must be part of a company's fitness agenda. Support from the top down is critical, as is sufficient funding to avoid fostering a culture of complacency. I strongly believe that if those tasked with protecting the business in the event of system failure, an attack or human error do not feel that threats are taken seriously enough, then their approach and attitude may well reflect this.

Any business evaluating their recoverability procedures and solutions in the face of an increasingly challenging IT landscape should consider the following five-point checklist as part of their planning process:

1. **Test, test and test again:** Put in place a well-structured recovery environment to optimise data recovery testing and ensure it can be conducted in the least disruptive way to the business. Solutions are now available that run testing without consuming vital resources or impacting the day-to-day production environment, allowing for business-as-usual.
2. **Consider a Chief Recovery Officer:** Many put their faith – and ability to recover – into the hands of a small group or one individual. Consider what the role of a Chief Recovery Officer with more defined responsibility would look like as part of a broader team that includes IT, security and risk management collaboration, and one who reports to the Board on the business' ongoing recoverability status.
3. **Redefine 'disaster':** The traditional image of fire, flood and acts of God is outdated. The increasing threat and sophistication of cyberattacks is the new reality. When, not if, your security is compromised, and your backup data is potentially unavailable, what exactly is your foolproof backup plan?
4. **Fail to plan, plan to fail:** Two-thirds of our survey respondents said they review and update disaster recovery plans at least every six months, but this leaves it open to falling down the priority list. Disaster recovery and data backup is a priority that all business functions should push for and be adapted to meet any newly identified requirements after frequent recovery testing.
5. **Calculate your downtime:** How long can you afford to be down? Do some napkin maths on what the cost of just one hour of downtime would be. Can you afford to lose any data without significant impact? Without this visibility your recovery plan may be flawed. ■

Roundtable: Resilience by design

Achieving network resilience can take a lot out of an enterprise, placing pressure on known and unknown points. We chat with Chris McKie at Datto, a Kaseya company; Alex Grant at 24 Seven Cloud; and Rene Neumann at ZPE, for their insights on creating a truly resilient network.

When it comes to network resilience, what is the end goal for IT teams?

Chris McKie VP, Product Marketing Security and Networking Solutions at Datto, a Kaseya company: The end goal is to have a reliable, secure and available connectivity that enables workers, guests and apps that use the network maximum uptime, even if networking gear should fail or other outages occur.

Alex Grant, Director at 24 Seven Cloud: To create a network that can self-heal. A resilient network can be designed in such a way that it will essentially have the set-up and configuration that can be mitigated, meaning it can rectify issues autonomously. Designing a network right the first time means it can cope with future issues. The benefit of this also means that it will be able to solve issues itself without human intervention.

Rene Neumann, Director of Solutions at ZPE: The real question is whether resilience is high enough on their priorities list, especially given the fact that networks can fail due to configuration errors, cyberattacks, and even natural disasters. The answer largely depends on who you ask within an organization and their understanding of what resilience means.

How does resilience differ from redundancy?

Neumann: Whether critical systems are in the cloud, on-prem, or in a hybrid environment, when customers lose access to services, the business's bottom line is at stake. In such cases, the network team is often the first to receive a call, with an urgent request to fix the issue immediately and ensure it never happens again. This is where the distinction between redundant and resilient systems becomes crucial. Redundancy involves adding backup components, like load balancers, to increase system availability. But, redundancy simply reduces the risk of failure in specific scenarios, and in many cases, it can add complexity to the network and complicate future changes.

McKie: Resiliency and redundancy are often conflated to mean the same, which is not true. Redundancy incorporates duplicative technologies to address concerns of failure. For example, duplicative power supplies are often seen as redundant components to a switch. Resiliency, on the other hand, addresses not just network components, but includes network management, network security, operations, back-up and recovery. Resiliency is much more than failover; it's about hardening a network so that services, even if impacted, are restored quickly and reliably. A resilient network is easily managed and includes templates to automate deployment, as well as to track network configurations.

Grant: A business could have just one computer that does payroll; if this device fails then the company would lose its entire payroll function. However, if the firm had two computers that were able to do the payroll, then this is what is known as redundancy, which is essentially back-up, or in technical terms, N+1. In terms of a network, if you have a switch or battery back-up, then this would mean you have redundancy. Another example of this in action could be a firm going to a data centre and choosing where to host its servers, this would mean it then has redundancy one plus two. It's important for any company to have extra hardware or software, should there be a fault with its existing network. In short, redundancy can give you resilience, but resilience can exist on its own as this is how a network functions.

What characteristics are intrinsic to resilient networks?

Grant: A resilient network should be able to cope with issues by itself. Whether that be a power failure at a data centre or a contractor cutting a fibre cable in the ground, if it has been designed to mitigate these types of issues without human intervention, then it will be able to endure any future problems that arise.

McKie: Intrinsic characteristics will


Chris McKie

include cloud-based management for quick recovery and ease of use. A resilient network will have a minimal learning curve for management. This eliminates the dependencies of the few experts who know the arcane, command-line only keystrokes to keeping the network up and running.

Neumann: Resilient networks are designed to mitigate disruptions by having the ability to adapt to changing environments and recover before a major prolonged outage can occur. A good analogy is the evolution of airplane wings. Early wings were rigid and broke, prompting engineers to design stronger ones. Eventually, they realized that flexibility was key to resilience. Similarly, resilient networks must be flexible and capable of adapting to changing conditions.

How important are periodic status audits?

Grant: Status audits are extremely important. When audits don't happen, this is where glitches can creep in. You are more than likely to have an outage if you don't audit your hardware. Planning also becomes a waste of time if a firm doesn't keep up with its auditing process. Depending on the company size, disaster recovery should happen every 3-12 months where a company's servers are switched off. A firm can plan for the worst either in a test lab or using its actual live equipment – although the latter is dangerous and not recommended. Ideally, a company would perform disaster recovery in a test environment, by replicating its live network.

McKie: Real-time monitoring, not periodic audits, are a must. Service providers like MSPs deliver networking as a service, which requires networks that are always available and secure. Real time auditing can't be isolated and relegated to network management tools, it must be integrated into RMM and PSA tools because that's where technicians spend all their time. When something happens, the system must react instantly and provide visibility within technicians' tools. This automates the process of ticketing, tracking and troubleshooting.


Alex Grant

Why is resilience built in from the network foundations superior to add-ons?

Neumann: There are two challenges to achieving network resilience. The first is a lack of organizational mindset. Most believe that resilience can come from deploying more cybersecurity products or disaster recovery solutions, when the reality is incidents continue to increase despite these markets being worth hundreds of billions of dollars.

The other challenge has to do with the diversity of network environments themselves, as most are unique 'snowflake' architectures that require their own specific tools and implementations. This makes them slow to deploy, extremely complex, and resistant to changes. Addressing this challenge involves rethinking how networks are built. The single most important component of achieving resilience is the underlying network management infrastructure and the capabilities it provides.

Grant: If you want something doing right, do it from the start. If you think about building a house, you want to do it right the first time. This creates a more stable platform to work from; the same goes for networks. The danger in adding add ons at a later date is that they aren't properly tested or designed to work together, which can cause issues. Unexpected outcomes can cause unintended consequences through introducing more variables. Designing from the ground up is the best way to build resilience.

McKie: The issue with add-ons is that integrations are not always maintained by the various vendors. If one party stops support, then over time the integrations break or lose their functionality. Because of this, integrations from a single source tend to work better over time.

Does any single technology stand out for resilience?

Grant: Containerised software is the most advanced in terms of resilience and fit-for-future. A container is an independent software programme that lives in the cloud. These 'containers' can be created or destroyed on demand, which ultimately means a new network can be created instantly. When compared to physical hardware, containerised software is the way forward for the industry.

It all comes back to redundancy vs resilience; you could have N+ million just by pressing a button - instant on demand resiliency and redundancy. As we continue to use more data, using containerised software means the scale of a network can be increased on demand. It can also be switched on and off meaning firms can take a 'spend what you need' approach or 'burstable spend' rather than having to pay a lot of money up front.

Neumann: While it will take time for organizations to educate staff with a resilience-first perspective, implementing Isolated Managed Infrastructure (IMI) is a major step that any company can take right now. IMI is a separate network dedicated entirely to management tasks. It is not just a lifeline for recovery in case of outages or failures; it serves as the platform for organizations to re-tool, rebuild, and adapt their networks without having to change their physical infrastructure. To build a resilient network, the IMI must have:

Security: The solution must address all supply chain vulnerabilities at the hardware and software levels and allow zero-trust enforcement on the management layer.

Isolation and Remote Access: The solution must use dedicated out-of-band management over multiple independent WAN links (MPLS, fibre, 5G, Starlink). As seen in the recent CrowdStrike incident, companies with resilient remote access recovered faster than those that required manual, on-site intervention.

Automation and Openness: The solution must be able to run automation tooling for routine operations and disaster recovery, as well as host VMs, Docker containers, apps, and services that can be spun up/down to adapt to changing environments.

McKie: Software Defined Networking is a front-runner, but it isn't a panacea for all. Advanced network resiliency requires multiple touch points, which eliminates singular points of failure and dependencies on singular products or technologies. There is no singular technology that stands out to make networking resilient.

How can an IT team know they've 'made it' on the path to resilience?

McKie: The short answer is that you've never made it. Resiliency is an ongoing effort that changes over time. Because it's a moving target, you're always getting close, but no one should ever be satisfied that they've achieved 100% resiliency.

Grant: The ultimate goal is to have everything working correctly. Some would say they've 'made it' when they have nothing left to do. A car manufacturer could build a car that lasts for a million miles for example, but this may not be the most logical or sustainable option in terms of value for money for the end user.


Renee Neumann

It comes down to cost vs benefit. If you have unlimited money, you could have the ultimate resilient network with thousands of replicated cables and data centres. This could also depend on the industry and the severity of the situation, should a network go down. For example, healthcare pendants need to always be active, however, if the phone line to a car dealership goes down and customers can't get through, the consequences aren't as severe. It's relative to the industry and the product that is being delivered to the end user. Some networks need to be more resilient than others. When deciding how resilient a network should be, it's important to keep the end user in mind. ■

Leverhulme Trust school students feel the benefit of future-proof networks

Leverhulme Church of England and Community Trust (LCECT) is a multi-academy trust based in Bolton. Its schools - Rivington & Blackrod High School and Harper Green School - operate as secondary phase teaching environments.

Both schools had ten-year old legacy Meru wireless networks with a mixed estate of HP switches, which were struggling to cope with the throughput and density required by classroom environments. The wireless performance was poor with slow connectivity speeds and the networks were difficult to manage. The Meru Wi-Fi support was also end of life which meant the trust's central IT team had no technical assistance in place for network troubleshooting.

Beyond legacy networks

LCECT wanted to improve the wireless performance with better security and control over school devices and improve network autonomy and management.

"With the existing network limitations, we required a more sophisticated network with better performance that could be managed easier at a trust level," said Richard Pycroft, ICT manager at LCECT. "I'd worked with Redway Networks before, so reached out to them to conduct technical Wi-Fi surveys at both school sites to review the networks and provide us with a comprehensive report for a future-proofed solution suitable for the next ten years."

Following the findings of the surveys - which included a detailed report of the network gaps - it was evident that both schools would be eligible for a Department of Education (DfE) Connect the Classroom (CtC) grant to upgrade the existing Wi-Fi and switching.

"With the documentation of works in place it was of strategic importance for us to upgrade our networks so we could support the direction of our technology plan," said Pycroft. "We asked Redway Networks to help us with the application process for campuswide networks that would support our future technology needs. Redway Networks provided us with a wealth of knowledge around CtC and looked after the whole process from start to finish and we were delighted to be awarded the grant."

Enabling security and control

With futureproofing in mind and to unify the networks, Redway recommended two separate Cisco Meraki WLANs, with a single trust-level login, to deliver reliable, fast wireless networks that would be easy to manage through the Meraki cloud dashboard. The solution was designed to manage and optimise the network for improving security and compliance.

Redway Networks' designed Meraki solution includes 16 x enterprise-grade MS355 and MS425 cloud-managed switches with a 10-year enterprise licence and support agreement. The switches are managed through Meraki's intuitive cloud-based interface, providing full 10G multigigabit access switching for demanding high-density classrooms. Redway's engineer deployed the switches as an overlay solution to increase density and PoE availability and provide easy power utilisation for future ICT projects and additional IoT network devices.

"With Meraki's switches we now have 10-Gigabit links so both schools are now benefitting from ten times the wireless speeds they had before. This means we can have more users on the network simultaneously accessing high-speed content which has created more inclusive learning styles," said Pycroft.

The MS switches serve 200 x high-performance Meraki MR46 wireless access points, designed to deliver exceptional Wi-Fi performance and efficiency, with enterprise-grade security and management. With Meraki, the schools now have different login flows for users with one SSID for teachers and admin staff, one for students with restricted access and one for guests. Meraki's Wi-Fi is, according to Pycroft, delivering more bandwidth and the network is more secure. Both schools are now benefitting from secure access to a high-speed wireless infrastructure with vastly improved wireless coverage and speed.

Indeed, school Wi-Fi speeds increased tenfold, asserts Pycroft: "Meraki is worlds apart from what we had before in terms of network reliability and speed. We now have a sophisticated, secure network which is the backbone to future learning. Meraki has improved delivery uptime, capacity, and coverage and users are now enjoying fast, reliable wireless connectivity. We now have the confidence to remove the wired network in our IT suite and lean on the Wi-Fi, meaning we can use our bank of laptops and Apple Macs which has saved on buying new IT equipment."

With Meraki, the schools benefit from reduced network complexity and increased control. All devices are visible in the Meraki dashboard enabling the IT team to resolve any issues easily which saves considerable time on network monitoring. The network is more secure and can now scale up new group networks based on distinct levels of access and security quickly. Staff can now login using their username and password instead of a pre-shared key and guests have a onetime-use password that's only usable for a day.

"Redway Networks was a great partner to work with and went above and beyond to install the networks out of school hours, so lesson time wasn't interrupted. From an IT perspective we can handle the day-to-day functions, but with a large wireless infrastructure project like CtC, it was great to have a trusted and knowledgeable partner like Redway Networks to work with," added Pycroft. ■

Agrovista moves from MPLS to co-managed private network with ZTNA

Agrovista is a leading supplier of agronomy advice, seed, crop protection products and precision farming services to farmers across the UK, working with arable, fruit, vegetable, horticultural and amenity sectors.

Agrovista's existing MPLS network and existing service provider was struggling to deliver - and a more solid foundation for future network evolution was needed to support the business.

The company's network of 24 storage and distribution centres, Agrovista head office and data centre needed a private network with reliable and secure connectivity. Of particular importance was the need to better support a largely mobile and remote workforce with a secure VPN and improved endpoint security, as was the need to work with a managed service provider able to respond quickly to changing needs.

A co-managed solution

Blaze Networks took up the challenge to design a co-managed private network. A fully integrated technology stack was provided, covering firewalls, switches, and wireless infrastructure across Agrovista's office and depot locations.

Professional project management by Blaze ensured a smooth deployment. All Agrovista locations are directly connected back to Blaze Networks' secure Private Core Network, with limited traffic going over the public internet. In some cases, alternative providers like Starlink were used to deliver better internet access at rural locations. SDWAN technology and security allowed Blaze to deploy and secure these connections with ease.

Each site has a FortiGate firewall, sized appropriately to the location and available connectivity, while direct connection and the use of SD-WAN enables the centralisation of Unified Threat Management (UTM). Running UTM on the Blaze Private Core Network saves expense and provides enhanced security by reducing Agrovista's cyberattack surface.

Meanwhile, all locations are connected via a primary and secondary connection through a combination of leased line circuits, FTTC, broadband and 4/5G (dependent on the number of staff, site location and service availability). The data centre firewalls are connected back to Blaze's core network on uncontended and dedicated 1,000Mbps connections.

Secure connection of remote workers is supported into the Blaze Private Core Network infrastructure through use of Fortinet's ZTNA (Zero Trust Network Access) solution that is incorporated in the Fortinet endpoint management services technology (FortiClient EMS). The Fortinet EMS security management solution enables scalable and centralised management of multiple endpoints. As well as providing remote user connectivity, EMS was also configured to provide remote web filtering, so devices are protected when outside of the secure network. Two factor authentication is provided, as well as additional capabilities as detailed above. Enhanced security technologies protect the Agrovista infrastructure and branch locations, including Unified Threat Protection (UTP), antivirus, BOT Net detection, Intrusion Prevention Services (IPS), and application control.

Securing the network

Use of the Blaze Private Core Network enables the hosting of integral elements including FortiAnalyzer and Fortinet EMS on a high availability basis through Blaze Cloud. With FortiAnalyzer - enhanced with Blaze Security Analyzer's add-on services including Indicators of Compromise (IOC) and Security Operations Centre (SOC) - Agrovista gains a greater level of value and protection.

All Fortinet equipment in Agrovista's SD-WAN sends logs back to the Security Analyzer which then provides comprehensive reporting and security operation functions. Blaze has tailored this to Agrovista's reporting requirements and provided training to the IT team on reporting and security operational functions available within Security Analyzer.

AI is used from FortiGuard to help combat virus outbreaks or ransomware using Indications of Compromise (IOC) licenses. As with content filtering, a co-management approach has been adopted and Blaze works directly with the Agrovista IT team. This transparent approach allows teams to work together to isolate and secure the network from threats - as and when they occur - aligning with Agrovista's security framework and incident management requirements.

Enhanced disaster recovery

The SD-WAN-based network design and combination of features provide Agrovista with a robust, secure and future-proof network – with enhanced disaster recovery strategy - in a highly cost-effective manner.

By using application-aware SD-WAN technology and application health monitoring, Blaze can automatically failover the traffic in the event of service degradation on the primary fixed line service. Use of SDWAN-enabled active / active paths and application steering over both the primary and secondary connections enabled more productive network utilisation as well as enhancing resilience. Provision of services to remote locations and mobile workers has been made much easier and a secure, capable, and resilient remote access infrastructure has been provided for mobile workers.

Cybersecurity has been enhanced by the network design and by the UTM system providing antivirus, content filtering and web filtering. Overall, through an efficient and secure network design, combined with the enhanced level of service delivered by Blaze, Agrovista has been able to improve the reliability and effectiveness of its wide area network whilst boosting cybersecurity and simplifying operations.

"Blaze has created a high-availability SD-WAN network which greatly assists the secure provision of IT services to our many remote locations and workers. The co-management of the network works well, and Blaze is highly responsive to our needs," said Alastair Battrick, Senior IT Manager, Agrovista. "Blaze has provided a flexible and easy to adapt network, and their responsiveness and customer-focus makes the company very easy to work with. I'd personally like to thank the team at Blaze Networks for the smooth transition from our previous MPLS provider, and the reliable service they are providing us." ■

Have VaaN, will travel!

Duncan Swan, Chief Operating Officer, British APCO

When achieving percentage mobile network coverage in the mid to high 50s is something to be proud of then you know that it is going to take innovative solutions to be able to communicate everywhere. And critical communication relies on connectivity wherever an incident occurs, and emergency responders are sent to work and provide help. Having just returned from Australia this is exactly the scenario faced with both self-contained government LMR solutions and commercial networks unable to provide connectivity across mass swathes of the landmass.

It's not a new problem; but it is one where we are seeing great leaps in the available technology to help overcome rural coverage challenges. With the latest smart devices providing the ability to get an SOS message delivered using satellite where there is no mobile network or WiFi available – Apple in partnership with GlobalStar and Google launching in the United States with Skylo – then it is imperative that those responding to the emergency message can do so effectively with comms they can rely on.

There are a host of solutions that provide fixed coverage extension – be that because of infrastructure outages, additional network demand, or beyond the edge of the normal coverage footprint. Rapid Response Vehicles provide temporary coverage in the UK for the Airwave and ESN solutions; the ubiquitous CoW – or Cell on Wheels – is rolled out in Australia; and tethered drones do the job in the United States – in essence flying CoWs.

But there is an emerging concept of VaaNs – or a Vehicle as a Node solution. VaaN is a cloud-based technology solution that turns a vehicle into a communications hub for mission-critical operations. And it is used by emergency agencies to improve communication and operational efficiency helping reduce service interruptions by bringing several bearers together – essentially it puts high-speed data and reliable communications into the hands of those who need it most – whenever and wherever they need it. Ericsson succinctly identify that the question of "Do I have connectivity?" quickly transitions to "What do I have access to?"

"With the latest smart devices providing the ability to get an SOS message delivered using satellite where this is no mobile network or WiFi available then it is imperative that those responding to the emergency message can do so effectively with comms they can rely on."

Whilst out in Australia I was particularly taken by a project that the New South Wales government was facilitating for the Rural Fire Service – and being delivered by relative new kids on the block, Hypha. Their company raison d'être stemmed from the simple observation that, for many years, progress in mobile technology in Australia was stagnant. With little investment into updating the ageing analogue terrestrial network outside of key metropolitan areas, poor coverage and outdated physical infrastructure, there were very few if any means to stay connected.

The rapid investment in LEO satellites – and their deployment in significant numbers by the likes of Starlink – finally provided the antithesis to the perceived stagnation, in those hard to communicate with rural areas. The NSW government sought to find a cost-effective means of solving the statewide conundrum of ubiquitous voice and mobile broadband coverage – the Vehicle as a Node solution combines Starlink satellite services and 4G & 5G mobile data onto an IP mesh network supporting LMR, location services, and other mobile device connectivity. And work has already started to roll out the VaaN solution to around 5,000 NSW Rural Fire vehicles of all shapes and sizes.

Of course, there may be challenges ahead – the choice of Starlink supports the goals of being cost effective, scalable and quick to deploy. It is renowned for constantly changing parameters – by way of example, a recent change in satellite altitude brought about a much-needed 6dB improvement in signal budget but there's no knowing just what may change next! Satellite connectivity relies upon line-of-sight to the satellite antenna; mobile communications require a different array of antennas; and the bringing together of the various communication networks clever router design and engineering. A key tenet of the VaaN solution is cost effective simplicity that is easy to deploy – and bringing all the technical elements together in a single roof mounted unit that includes the Starlink antenna helps achieve this.

There's no doubt that, in the not-too-distant future, we will see similar implementations closer to home as we look to take percentage mobile network coverage as close to 100% as is possible for networks supporting critical communications – without breaking the bank or compromising reliability and security.

Well, this is my last Talking Critical column – at least for the time being – and I've enjoyed exploring a wide range of topics that fall under this banner; I do hope that my musings have, if nothing else, given you a little something extra to think about. ■

Keeping the UK's data centres cool

Alan Beresford, Managing Director, EcoCooling Ltd

Choosing the right cooling solution for your data centre is essential to protect you and your stakeholders' assets and reputation. Overheating components can lead to costly system failures and interruptions to business, while well-cooled data centres are bastions of productivity and efficiency.

But the right solution right now could be woefully inadequate to keep up with the demands of technology in five or 10 years. High Performance Computing (HPC) has increased in power exponentially and its cooling demands have grown in step with this.

Future-proofing data centres with flexible designs that can accommodate rapid changes and meet efficiency standards while maintaining capital cost, efficiency and the speed of deployment is vital.

Where will your business be?

Before selecting a cooling solution for your data centre, businesses need to seriously think about what they're doing now and what they might be doing in the future. State-of-the-art data centres built 5-10 years ago are now inappropriately engineered for emerging technologies with high power densities and associated cooling demand. This is not a small evolution: there's a risk you could get the decimal point in the wrong place.

Consider space and power

The latest AI equipment can take 10 times the amount of power per rack and demand 10 times the amount of cooling as the HPC of yesteryear. That requires more infrastructure and space to accommodate it.

Ask yourself, what cooling redundancy am I going to have? N, N+1, 2N? Some Nvidia equipment requires 3N power! With that in mind, it's important to consider the size of cooling modules. A set of smaller modules can typically be adapted quickly and cost-effectively. Any liquid cooling solutions need to be very carefully designed to provide appropriate resilience. Don't forget, there is a big difference between redundancy and concurrent maintainability of cooling systems.

Measurement and reporting

The chase to net zero is going to affect how businesses operate. Data centres already have to meet reporting requirements to ensure they are efficient, particularly in the use of electricity and water. Making sure your designs comply with existing standards while anticipating future standards is essential.

Pay close attention to the measurement and reporting capabilities of new equipment. Not only do you have to be efficient – you need to prove efficiency. Also, consider whether your data centre will meet the standards when running at 10% or 90% capacity. Your designs must accommodate the whole range of rate demands.

Air cooling systems, if correctly controlled, operate at a far higher efficiency at low utilisation as the fans use less energy. It is quite common to see a cooling partial Power Utilisation Effectiveness (pPUE) of less than 1.02 for a pure ventilation system.

A hybrid solution is often best

In the past, you could deploy one cooling system for an entire data centre. Today, there is a distinct possibility that you will have two different cooling requirements. HPC will probably need a form of liquid cooling but a considerable proportion of the load will still be everyday computing that only requires conventional cooling.

Ultimately, you end up with a hybrid solution – part liquid, part air – and then have to decide on the proportion between the two. Think carefully about how much HPC you might be doing in a few years.

Designing a facility which can accommodate the rapid integration of new equipment is essential to enable you to develop as technology progresses. Speed is of the essence.

Take inspiration from cryptocurrency pioneers

Cryptocurrency mining equipment has increased in performance about a hundredfold over the last 10 years. The industry has moved into a zone where the only way to survive is by being huge. Hundreds of megawatts.

By building data centres in remote areas with naturally cold climates and cheap power, crypto pioneers are able to deploy giant data centres in a quarter of the time it takes to build a conventional data centre – and for less than 10% of the cost.

In these locations, cooling can be achieved with fresh air and no refrigeration, which challenges traditional thinking.

There is currently a trend for converting cryptocurrency facilities into high-performance data centres. Mining cryptocurrency is not easy – it requires enormous computational power, energy consumption, and specialised hardware. These facilities are now offering viable solutions to the rapid deployment of HPC.

Plus, a lot of AI is not latency-affected; requests do not have to be back in milliseconds. While it requires a lot of computational power, the actual traffic demands are, in some cases, much lower. Location will be dependent on the particular latency demands your business has. ■

PRODUCTS

New high-capacity models of the Vertiv™ Liebert® AFC inverter screw chiller range with low global warming potential (GWP) refrigerant are now available, providing up to 2.2MW of cooling capacity in a single frame, resulting in a smaller carbon emission footprint; requiring fewer units to be installed for capacity; and reducing installation and maintenance time and costs.

The newest Liebert® AFC models are high-density, outdoor, free cooling chillers that provide the industry's highest capacity in a single frame. These future-ready chillers enable hybrid operation for data centres deploying AI and HPC liquid cooling applications and are compliant with current regulatory requirements in the EU. The chiller is an integral part of the overall Vertiv solution to simplify data centre deployment and management. By pairing the Liebert AFC chillers with chilled water solutions such as Vertiv™ Liebert® PCW perimeter air handler system, Vertiv™ Liebert® XDU coolant distribution unit, Vertiv™ Liebert® CWA thermal wall system, and Vertiv™ Liebert® iCOM™ CWM smart control, operators can efficiently address the cooling needs of colocation and cloud data centre applications.

Vertiv™ Liebert® AFC offers up to 20% lower annual energy consumption compared to fixed screw solutions. The inverter-driven compressor allows for the reduction of energy consumption and, in particular, the electrical power required during peaks, which in turn allows more power availability for the IT equipment. The innovative regulation algorithms offer accurate control of the fluid delivery temperature to the indoor units, enhancing cooling continuity and reliability. The unit is designed to operate with a more eco-friendly refrigerant R1234ze HFO, which allows data centre owners to comply with the EU F-Gas Regulation 2024/573 and enables customers to support pressing sustainability goals.

STULZ has added a standard version of the cutting-edge CyberAir Mini CW precision server room air conditioning unit to its range of industry leading solutions.

In response to increasing demand for quickly available cooling systems for small to medium-sized data centres, the standard version is available with a delivery time of just 14 days, offering customers decisive advantages in terms of delivery time and costs, without compromising on quality and range of potential applications.

The standard CyberAir Mini CW is a compact and efficient precision air conditioning system which is available in four sizes with capacities from 9-35kW. It will deliver effective climate control in server rooms and telecommunication closets, and can be easily integrated into existing building management systems (BMS). Chilled water (CW) cooling technology ensures energy efficient temperature management and it is engineered for continuous 24/7 operation.

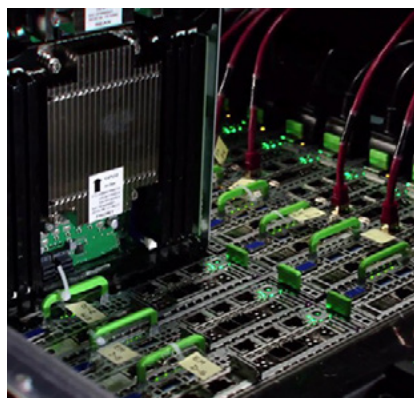
The CyberAir Mini's compact design allows for flexible installation in confined spaces, while the use of modular components offers scalability to meet growing cooling needs and adaptation to individual requirements. Customers can order additional accessories such as bases, blinds or humidifiers directly from STULZ, which are then delivered ready to be mounted on-site by a technician.

Transtherm's Air Blast Coolers can provide capacities from 5KW to 4,000KW and to within 3°C of the prevailing ambient temperature year-round.

With bespoke designs, various coil and fan technologies are available to suit low, medium and high temperature applications, while multiple cooler orientations – including full and ½V, horizontal and vertical flatbed designs – Transtherm Air Blast Coolers comply with the latest requirements.

The Fujitsu Server PRIMERGY Liquid Immersion Cooling System cools the entire IT devices equally by immersing it in cooling fluid.

The system cools the entire server equally, and because the heat generated by the server is not emitted into the server room, air conditioning equipment is unnecessary. The cooling system provides high energy efficiency because the server does not require internal cooling fans, boasting a power usage effectiveness (PUE) ratio of 1.07. This not only reduces the server system's overall power consumption, by approximately 40% compared to air cooling systems (including its cooling equipment), it also enables approximately double the server density in the same installation space, contributing to reductions in the total cost of ownership (TCO).



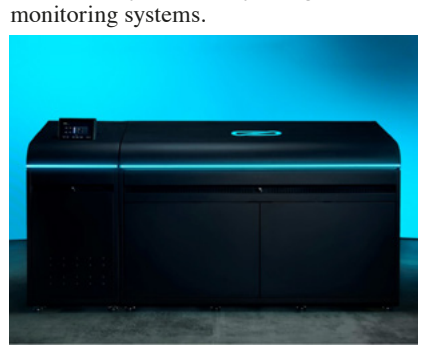
By using Fujitsu's specially developed, well-sealed 'immersion bath,' this system minimises vaporisation of the cooling fluid. Maintenance of the system is easy because the fluid used as a cooling medium is also non-combustible, not harmful to humans, and does not need to be regularly replaced as it does not deteriorate.

Submer's SmartPod EXO offers extreme density and ensures the data centre is climate-resilient.

With 99.999% availability and concurrent maintainability, the EXPO dissipates up to 361kW of heat. Heat reuse and dry cooling is optimised, with the opportunity to completely eradicate direct water usage. For smooth and Predictable daily IT operations, the system features modular cable management; is prepared for standard 19" patch panels; and has PDUs in the dry zone.

Designed for high capacity and high performance, the SmartPod EXO delivers exceptional high density per square foot, with a maximum power consumption of 3350W. Regulated water flow rate consistently maintains water usage at an optimal level, maximizes its temperature, and minimises energy consumption as a result. Meanwhile, operating with hot water makes free cooling a viable option, delivering more location choices around the world.

Independent access for IT at the front and power distribution at the back enable seamless operation, while Submer's API & SNMP system easily integrates with monitoring systems.



Please meet...

John McKindland, Head of Partner Channel, UK, Sona Business

Which law would you most like to change?

Tax and immigration laws. We are devoid of certain skills sets in this country and it's getting harder for people with those skill sets to get into the country and work and contribute. The NHS has suffered because of this. We need to make it easier for skilled workers to come to the UK and not restrict the numbers because illegal migration is so high. Tax is the government's only source of income to run our services. There are too many loopholes and too many sticking plaster fixes. The whole thing needs ripping up and starting again to make the tax burden fairer for all.

Who was your hero when you were growing up?

My uncle who was a fireman in the RAF. He won awards for bravery such as jumping on burning aircraft to save the pilots. He would tell the story as though it was nothing and just doing his job, which he was. But I was always struck by his courage, his calm and cool-headed approach to everything. I am proud to be named after him.

What was your big career break?

Without a doubt telecoms distributor Rocom in 1996. I found myself in a career desert and landed at the right place, right time and most importantly the right people who are still friends today. I learnt a lot from Rocom which has guided my career through distribution, networks and MSPs ever since.

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

It was always the military; we are a military family with every generation serving for the last 150 years so it was a given I would join the Army and did so at 16. Opportunities to do anything else were limited at that time and it was the right choice. I enjoyed 12 years in the Royal Signals and would have stayed longer but with my daughters back in the UK and no real hope of a UK posting it wasn't a difficult decision to leave and start a new career in telecoms.

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

Winston Churchill. I would love to hear his stories of his time as journalist in South Africa and of course just how much of close-run thing was 1940 and the Battle of Britain. I can't even begin to understand the weight of the burden he carried. Having led the nation through war I wonder what he must have felt following a devasting election defeat in July 1945. I am sure the brandy and cigars would figure somewhere in the evening.

The Rolling Stones or the Beatles?

Rolling Stones up to 1973 and then it would be Pink Floyd.

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

My role in the military required accuracy with no wiggle room for errors. Everything was black and white. Moving through my civilian career, I was once advised to learn to live in the grey, and that it was more important to be effective than right. Managing a large team, I had to learn to empower and listen to my staff, sit back and allow them to present their data and opinion so we could understand the bigger picture and act meaningfully. It was a learning experience, and it took a while for me to adapt and change. The first year was painful.

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

Right now, it would be renewable energy; in terms of technical development and advancement that it is the place to be over the coming years. It's an industry that will shape future generations and how they live and work.

What would you do with £1 million?

I'd build a solid financial base to power the next stage of my family's lives and careers. Secure our future generationally and look to see how we can make a positive effect on our local community.

Where would you live if money was no object?

I got married on the Amalfi coast in Italy in 2019 and fell in love with the area, but a recent trip to Westport in Ireland really has turned my head and I think that would be a great place to retire to.

What's the greatest technological advancement in your lifetime?

It has to be the mobile phone. It has driven development of nano technologies used in so many industries, created powerful voice and data networks, applications for everyday life and of course revolutionised the camera industry. Sadly, it's probably also the worst advancement when you look at the effect on people's mental health. We need to learn to use our tech better. ■