SEPTEMBER 2023
networkingplus.co.uk

NETWORK+

The security arms race

CRaaS is the new tool MSPs need

Ahsan Siddiqui, Arcserve, p5

Revolutionising connectivity

Unlocking tomorrow's connectivity with 5G

Damian Hanson, CircleLoop, p14

Questions and answers

We live in an exciting time when the pace of change is rapid

Oliver Ledgard, Zebra Technologies, p16

UK cities go smart with SIPP

The government has announced a £1.3 million pilot project across towns and cities in the UK to deploy smart streetlamps to test next generation technology, offering EV charging and improved wireless connectivity, including 5G and free public WiFi.

"The way we stay in touch, access information, and do business is underpinned by digital connectivity - and a world-class wireless infrastructure will be the foundation for the jobs, skills, and services of the future," said Sir John Whittingdale, minister for data and digital infrastructure.

Six areas will receive a share of the £1.3 million funding - Cambridgeshire County Council (£220,000); Tees Valley Combined Authority (£202,500); Royal Borough of Kingston upon Thames (£245,700); Westminster City Council (£165,000); Oxfordshire County Council (£250,000); and North Ayrshire Council (£242,765) - through the Smart Infrastructure Pilots Programme (SIPP), and will match the funding, bringing the total investment to £4 million.

"We want to ensure that towns and cities across the UK are right at the forefront of this connectivity revolution, ready to seize the opportunities it will bring for local communities, which is exactly what these pilots are about," said Whittingdale. "They will help demonstrate how advanced wireless technology can enable areas to innovate and deliver better public services, from rolling out electric vehicle chargers to boosting business growth and helping keep our streets safe."

Under the pilot, Boldyn Networks is partnering with Kingston Council to deploy smart columns equipped with small cells to enhance digital connectivity and improve CCTV camera quality. 20 CCTV sites will be installed around the borough, with the design also supporting IoT sensors for service management, including road usage, footfall, and air quality.

"The funding offers a great opportunity to trial smart infrastructure and showcase the benefits that high-speed connectivity offers to local communities," said Bill D'Arcy, CEO of UK & Ireland, Boldyn Networks.

The pilots can be adapted to carry out a range of functions - from charging EVs to monitoring air quality, and displaying public information to saving energy with street lighting - that will enable councils and combined authorities to unlock new opportunities and improve public services. The aim is to show how wireless technology can become an integral part of UK infrastructure, connecting public services and businesses in new ways to realise the full benefits of 5G and advanced connectivity.

Julian David, CEO of techUK, described the pilots as a welcome step in putting wireless connectivity at the heart of local infrastructure deployment. "We must empower more local authorities so that they can foster the greater use of advanced connectivity in their areas, helping unlock growth and innovation across the whole of the UK. We hope these pilots can help other local areas realise the benefits that smart infrastructure promises."

The SIPP will support the government's Wireless Infrastructure Strategy, which "sets out a clear vision for how advanced wireless infrastructure plays an ever-increasing part in the UK's economy and society by 2030," said Nick Johnson, head of UKTIN. "A critical part of this centres around the need to identify and break down barriers to deployment at a local level. These pilots are an important part of the innovation process, considering the practical ways in which local authorities can efficiently deliver better connectivity to their communities."

The pilots herald a step forward for the future of the UK's smart cities; however, we've yet to see data on the projected impact on local authorities in terms of communications management; how will this new smart technology be secured and maintained, now and in the long term? Moreover, as the new connectivity becomes increasingly utilised by businesses, schools, the public sector, etc., what are the consequences for already-overloaded network management teams? ■

Cannon Hall Farm goes high tech with Virgin Media O2

Virgin Media O2 has created the 'Connected Farm of the Future' in a trial with Cannon Hall Farm in Barnsley, designed to showcase how enhanced mobile connectivity could transform rural agriculture.

Agriculture has faced some of the toughest challenges over the past few years, from extreme weather changes to labour shortages compounded by Brexit and the pandemic. In DEFRA's latest Farmer Opinion Tracker, farmers on over half (52%) of holdings do not feel positive about their own future in farming, up from 41% in 2022.

Virgin Media O2 is bringing connectivity to every corner of Cannon Hall Farm's 126-acre estate, including historic blackspots and not-spots, to explore how a network of sensors and monitors can work together to transform the farm, saving time and money.

As the two most common rural crimes, equipment and livestock theft cost the rural agriculture industry a combined £49.5 million in 2022 alone. Compounding the issue are gates being left open on public footpaths that run around and through many farms, leading to livestock escaping fields and being lost or injured. Trackers, sensors, and switches like those installed across Cannon Hall Farm's equipment, livestock, and gates as part of this trial enable the farmers to monitor in real time the location of these high-value items or receive alerts about gates left open. This means that farmers can be alerted instantly if equipment moves unexpectedly or leaves the farm, helping minimise the risk of loss and freeing up time previously spent doing manual checks.

With farmers often working alone across big areas and remote locations with little to no signal, access to connectivity can be a game changer, and in the most extreme instances be the difference between life and death. According to data from the Health and Safety Executive (HSE), agriculture has the highest workplace injury rate of 4,100 per 100,000 workers, 3.5 times higher than the all-industry average. The trial improves safety by removing not-spots, providing reliable mobile signal across the farm, and giving workers the ability to get help should they need it.

Over the past 30 years, major crop yields have decreased globally by 4-10% due to climate change. To combat the impact of increasingly extreme and unpredictable weather events such as floods and droughts on crop viability and yield, part of the trial sees the installation of connected soil moisture, atmospheric temperature, and humidity sensors. These sensors show the potential to monitor the health of crops and assess irrigation needs, reduce water use, improve crop quality and allow for targeted interventions based on real-time conditions.

"We are thrilled to be partnering with Virgin Media O2 to trial the 'Connected Farm of the Future.' Rural connectivity opens the door to a range of new technologies that could completely change farming as we know it," said Rob Nicholson, owner of Cannon Hall Farm. "Being able to monitor in real-time soil and atmospheric conditions, provide remote support and have round-the-clock monitoring of livestock, machinery and equipment is a total game-changer. The potential for this technology to help create a more efficient, profitable, and sustainable future for not only our family farm but many other farms across the UK is huge."

"This trial is an example of the transformational power of connectivity and how it's being used to power a Great Rural Revival. Through this innovative trial with Cannon Hall Farm, we have demonstrated how a network of sensors, underpinned by excellent connectivity, can make a real impact and transform the way we live and work in rural areas," said Jeanie York, chief technology officer at Virgin Media O2. ■

Royal Fleet Auxiliary ship Argus utilises LEO satellite for critical communications at sea

The crew of the Royal Fleet Auxiliary ship Argus is using internet with coverage provided by low Earth orbit (LEO) satellite from OneWeb in collaboration with distribution partner Airbus.

The connectivity is being provided by the company's Kymeta Peregrine u8 terminal, which was fitted while Argus was docked in Falmouth this summer. It is the first military vessel to be using the technology.

"The maritime terminal will provide reliable, low latency, high-speed broadband connectivity anywhere in the world, even during challenging sea conditions and high-speed motions," said a spokesperson.

"Crew welfare and morale is a key tenet of a platform's fighting capability. Enhanced connectivity, such as that delivered by low Earth orbit satellite networks is an area that the Royal Navy are looking to exploit," said Lieutenant commander Ben Slater from the Royal Navy's digital unit. "Through close collaboration with industry partners, we have been able to fit a capability onboard RFA Argus that will enable her crew to keep in touch with family and friends. We are looking forward to seeing how it performs at sea for the first time on a naval vessel."

RFA Argus performs several important roles for the UK armed forces, including being their primary casualty-receiving ship, equipped with a 100-bed hospital in times of conflict. It is also a training vessel for military helicopters operating at sea. ■

IoT market heats up, says ABI Research

Wide-area Internet of Things (IoT) connectivity vendors are fighting for space in an increasingly crowded market.

According to ABI Research, Low-Power Wide Area Networks (LPWAN) will reach 5.3 billion connections in 2030. LPWAN companies are competing in integral IoT applications such as smart metering, asset tracking, and condition-based monitoring, with a vendor's competitive advantage often hinging on factors beyond a network's technical capabilities.

"The business environment surrounding a networking technology can be as influential to its success as its data rate, bandwidth, and power requirements," said Lizzie Stokes, IoT hardware and devices and IoT networks and services analyst at ABI Research. "As new connectivity technologies enter the market and others pivot or leave entirely, it is important to understand how various market dynamics – such as regional availability and stages of development - impact a technology's successes and failures."

When competing against newer technologies and other wide-area networks, cellular LPWANs struggle with fractured regional deployments and higher device and connectivity costs than other LPWA technologies. LPWA solutions are increasingly confronted with complexity concerns as IoT users demand user-friendly, end-to-end IoT systems. To maintain market share, vendors must dynamically respond to these obstacles while navigating new, potentially disruptive standards and protocols such as DECT-2020 NR, MIOTY, and ZETA.

Short-Range Wireless (SRW) technologies face a different competitive landscape than LPWANs in the IoT domain. WiFi and Bluetooth are primarily used in home automation use cases but are also finding greater use in commercial IoT applications. Bluetooth Low Energy (BLE) and WiFi HaLow expand the technologies' place in industrial and wide-area IoT deployments. Hybrid use cases, where customers deploy SRW and LPWA technologies simultaneously to optimize an IoT deployment, have further increased Bluetooth's and WiFi's presence in long-range applications. Though the wireless IoT networking market has a history of intense competition, trends in hybrid use cases suggest some IoT vendors are leaning toward collaboration.

"Competition in the wireless connectivity market continues to be fierce," said Stokes. "Vendors should attempt to carve out a unique place in the market by thoroughly understanding their client's coverage and power requirements. Vendors should cater to specific use cases and regional needs while acknowledging that customers will respond to technologies that can work well with others." ■

EDITORIAL:
Editor: Amy Saunders
amys@kadiumpublishing.com
Designer: Ian Curtis
Sub-editor: Gerry Moynihan
Contributors: Ahsan Siddiqui, Nadav Avni, George Barnes, Alastair MacLeod, Nick Earle, Damian Hanson, Iratxe Vazquez, Oliver Ledgard

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

Retail requires urgent data resilience work

Arcserve has released a segment from its annual independent global research during Cybersecurity Awareness Month that highlights an urgent need for enhanced data resilience in the retail sector.

The results reveal a lack of preparedness and confidence in data backup and recovery strategies, raising concerns about the industry's readiness to protect sensitive customer and business data.

Key survey insights include that 54% of retail executives disclosed they were targeted by ransomware in the past 12 months; 26% of the attacks resulted in compromised data, and a quarter confirmed paying ransom. Some 66% of retail executives surveyed were not very confident in their ability to recover all lost data in the event of a ransomware attack. Nearly half (42%) of retail executives admitted being unable to recover all data during their last significant data loss incident. 57% reported they lack well-documented or updated disaster recovery plans. The vast majority (72%) revealed that they do not have specific data resilience goals within their data and backup strategies.

"As we head into the Cybersecurity Awareness Month and the holiday shopping season that follows, retailers can't afford to be caught off guard," said Aftab Alam, chief product officer at Arcserve. "Our latest research is more than a cautionary tale; it's a call to action. Retailers must urgently overhaul their disaster recovery plans to match the ever-evolving cyber threat landscape. Data resilience isn't a 'nice-to-have'; it's a non-negotiable business requirement with clear, measurable objectives. And don't wait for a crisis to test your recovery protocols; make it a regular practice, akin to a fire drill. By taking these steps, retailers do more than protect their bottom line - they retain the trust of their customers."

Arcserve recommends three immediate steps for retail organisations to be better prepared:

Review and update disaster recovery plans: Assess the robustness of data recovery strategies and ensure they align with the evolving threat landscape.

Invest in data resilience: Define specific data resilience goals within data and backup strategies to minimise potential losses.

Test recovery procedures: The wrong time to test disaster recovery plans is during a crisis. Test them now to ensure seamless and orchestrated recovery when it matters most. ■

NHS to miss £1 billion in annual savings without 5G

According to research commissioned by Vodafone, the NHS will lose out on £1 billion of savings every year if 5G is not rolled out quickly across the UK.

Local councils also stand to miss out on significant savings, with 5G-enabled technologies having the potential to reduce social care spending by 5%. On top of the £40 million 5G Innovation Regions funding currently available to councils, this would help plug the existing gap in social care funding.

The findings, calculated by WPI Economics, come as projections show that the ageing population will put an increasing strain on the NHS and social services in the years to come, with £79 billion of public spending required to meet these needs. 5G-enabled technologies will be essential in addressing these challenges.

5G will enable more patient care to be delivered remotely. For patients at home, 5G will enable high-quality and high-speed video connections, enabling doctors to deliver quality care quickly and efficiently. This will empower people to better manage their health, allowing them to live independently for longer and could prevent people from needing additional care either in the home or in non-residential settings. The NHS has already recognised the importance of this technology for bringing down waiting times and reducing hospital stays, as it is due to introduce remote care for 10,000 patients from September 2023.

Within care homes, residents and staff will also stand to benefit from the rollout of 5G. Sensors could help staff monitor residents in real time, improving care and alleviating staff burnout. Sharing data between care providers and hospitals becomes easier, faster, and more secure.

Trials have shown that these innovative measures could save £296,000 per 100 users each year, equivalent to nearly £1 billion based on the current number of users of public social care services. With this number set to increase by 61% by 2038, the rollout of 5G could save up to £17.5 billion over the same period. However, these savings will not materialise unless nationwide 5G is rolled out quickly. ■

OMNIA - solving network and security problems for businesses of all sizes

OMNIA is a comprehensive solution addressing critical challenges faced by businesses in the UK, irrespective of their size. Here's how OMNIA tackles these issues:

1. *Cost Reduction:* OMNIA consolidates network, security, layer 4 encryption, and 4G functionality into a single device. This approach saves on initial investment, ongoing management costs, insurance, and power expenses compared to running multiple separate appliances. The cost savings extend across all business locations, significantly reducing operational expenses.
2. *Flexible Payment Models:* OMNIA offers month-to-month Pay-As-You-Go (PAYG) options and zero-install Operational Expenditure (OPEX) contracts. This flexibility eliminates the need for long-term commitments or upfront payments commonly associated with large SD-WAN vendors. Businesses can scale services up or down and move them between locations without penalties.
3. *Bandwidth Enhancement:* Replacing a UK MPLS network with OMNIA generally leads to increased bandwidth, resilience, redundancy, and a cost reduction of around 40%. Atomius SD-WAN removes expensive and restrictive traditional SD-WAN vendor software license tiers.
4. *Tailored Solutions:* OMNIA provides affordable packages to suit various business needs. OMNIA Lite caters to one-person businesses and remote workers, OMNIA BIZ serves single-site locations with up to 3 simultaneous connections, and OMNIA PRO delivers true SD-WAN capabilities for businesses with 2 to thousands of sites.
5. *Security:* OMNIA offers security solutions at the edge device, in the cloud, or through in-country Secure Web SASE Gateways. This multi-layered approach ensures robust protection against cyber threats.
6. *Layer 4 Encryption:* OMNIA Data Assurance includes Layer 4 encryption, a crucial feature that many businesses overlook. This encryption can prevent data breaches, theft, and ransomware attacks. Notably, companies that suffered recent security incidents always lacked Layer 4 encryption. Read more here: https://www.sdwan-solutions.global/layer-3-encryption-vs-layer-4-encryption-what-you-really-need-to-know/
7. *Seamless Connectivity:* OMNIA integrates SDWAN CLOUD for seamless multi-cloud connections, SDWAN CONNECT for global connectivity, and SASE REMOTE to replace outdated VPNs with true zero-trust access to the network.

OMNIA provides a cost-effective, flexible, and secure solution to address the challenges faced by businesses in the UK, making advanced technology accessible to a wide range of enterprises, from one-person businesses to larger corporations. OMNIA is being rolled out across the UK, EU, ASIA, and African markets: Full details here https://www.sdwan-solutions.global/omnia

The Very Group migrates to public cloud

Kyndryl has expanded its partnership with The Very Group, which is modernising and migrating applications and infrastructure to a leading-edge multi-platform public cloud environment.

Kyndryl will migrate applications to the public cloud, moving to a cloud native architecture whilst taking on application support, enabling a simplified architecture and a more carbon efficient service. The new partnership will allow The Very Group to grow its service to support growth and to gain greater technical and commercial flexibility. As one integrated team devoted to mutual cultural diversity and operational values, The Very Group has trusted Kyndryl's knowledge of their business and track record of transformation and application management.

To facilitate this transformation, Kyndryl will combine The Very Group's core service management toolset with cloud native tooling and the implementation of Kyndryl Bridge and AIOps, enabling greater links between global teams. This process will build an optimised, integrated service that is simple, flexible, automated, and delivered with velocity with improved service observability.

"We are delighted to partner with The Very Group to help them transform their IT estate with speed and flexibility. Kyndryl and The Very Group teams are united by a consistent, agile, and transparent operating model, delivering on the 'value for you; value for us' principle," said John Chambers, Kyndryl's UK and Ireland president.

"We're amid a tech transformation that will allow us to offer our customers an outstanding digital experience, improve the ways our teams work together, and deliver efficiencies for our business," said Matt Grest, CIO at The Very Group. "Kyndryl have proven to be an innovative, supportive, and committed partner, and we are pleased to extend our agreement with them to migrate more of our applications to the cloud, as well as benefitting from their support capabilities." ■

Healthcare sector's approach to security lacking

Arcserve has released findings from its annual independent global research focusing on the healthcare sector's approach and experience of data protection, recovery, and ransomware readiness.

The findings reveal gaps, vulnerabilities, and misconceptions in the healthcare sector, potentially hindering its ability to effectively safeguard and recover data in the event of malicious attacks and accidental data outages stemming from human error or natural events.

Across all industry sectors, healthcare was the most targeted by ransomware attacks; 45% of healthcare respondents experienced a ransomware attack in the past 12 months. Healthcare providers face high ransom demands, with no guarantee of recovery. 83% of ransom demands were between $100,000 to $1 million; 67% paid the ransom; and 45% did not recover all their data after ransomware attacks.

Against this threat backdrop, there were apparent preparedness weaknesses. 82% of healthcare IT departments lack an updated disaster recovery plan; nearly 75% of respondents believe data backed up to a public cloud is safer than data backed up on-premises; and more than 50% of respondents mistakenly believe the cloud provider is responsible for recovering their data.

"In the face of growing number and sophistication of ransomware attacks, the healthcare industry continues to grapple with inadequate data protection and recovery mechanisms," said Vitali Edrenkine, chief marketing officer at Arcserve. "An ounce of prevention may be worth a pound of cure - but our latest market research shows that when it comes to ransomware resilience, too many healthcare institutions have neither. A robust backup and disaster recovery strategy is critical for healthcare organisations to build resistance to malicious attacks."

Arcserve advocates for a transformative 'unified data resilience' approach within the healthcare sector to bolster preparedness. By adopting a unified data resilience strategy, organisations strengthen their defensive posture and have the necessary tools to expedite data recovery in the aftermath of ransomware attacks. ■

UK leads the pack in EMEA's DDoS attacks

Akamai Technologies, Inc. has released a new State of the Internet report - The High Stakes of Innovation: Attack Trends in Financial Services – which finds that financial services is the third-most attacked vector in the Europe, Middle East, and Africa (EMEA) region, with approximately 1 billion web application and API attacks, which represents a significant 119% year-over-year increase when comparing Q2 2022 with Q2 2023.

In EMEA, insurance is by far the most attacked sub-vertical of financial services with 54.5% of all web attacks, which represents a 68% increase year over year. Insurance companies hold a huge amount of personally identifiable information, which makes them an attractive target for cybercriminals in contrast with other financial services organisations that hold mostly financial data.

The report also finds that as a region, EMEA experienced the most DDoS attack events (63.5% of attacks worldwide), which is nearly double the number in North America, the next top region (32.6%). The UK tops the list in EMEA at 29.2% of DDoS attack events, followed by Germany at 15.1%. Akamai surmises that the attacks on the European banks that are allies of Ukraine are financially and politically motivated by Russia's continued war in Ukraine and are the primary reason for the increase in attack events in EMEA.

Between January 2022 and June 2023, DDoS attacks on financial services in EMEA equated to 1,466 of the 2,590 attack events across all verticals in EMEA and resulted in a 40% increase year over year in DDoS attacks when comparing Q2 2022 with Q2 2023. DDoS attack events against the gambling, commerce, and manufacturing verticals in EMEA each also exceeded all other regions combined. 24% of the scripts used by financial services organisations in EMEA come from third parties, which is notably lower than in other verticals (36%)

"As cybercriminals continue to follow the money, financial services remain a hugely attractive target. At the same, this is one of the most regulated sectors and hence it is essential for companies to align their security strategy with emerging laws and regulations," said Richard Meeus, Akamai's director of security technology and strategy, EMEA. ■

Word on the web...

4 tips for choosing a COSU device management software that delivers the Best ROI

Nadav Avni, CMO, Radix Technologies

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

CRaaS is the new tool MSPs need in the accelerating security arms race

Ahsan Siddiqui, director of product management, Arcserve

There's a security arms race going on. As technology advances, so do the weapons and tactics of cybercriminals. Organisations must constantly raise their game and develop better ways to protect themselves against attack. The stakes are high. A recent report by Cybersecurity Ventures predicts cybercrime will cost the world $10.5 trillion annually by 2025, up from $3 trillion in 2015.

That's a trend in the wrong direction. It shows that organizations need new strategies — defenses and disaster-recovery methods — to protect their sensitive data and critical systems against attack.

One of the most promising new strategies is cyber-recovery as a service (CRaaS). This service enables businesses to recover data and restore systems after a cyberattack rapidly. It is explicitly designed to repair the damage caused by a cyberattack, unlike traditional disaster-recovery tools primarily built for floods, fires, and hardware failures. CRaaS creates a secure and isolated environment where an organization can quickly restore its critical data and systems in case of a breach.

The old scenario: a cyberattack hits your business, compromises your data, and panic sets in as you realise that your business could collapse. The new scenario: it won't because CRaaS has your back.

As mentioned, traditional disaster-recovery solutions resolve physical server failures or clean up after a natural disaster like a fire or flood. CRaaS provides a more modern, more comprehensive recovery. It enables businesses to restore their data after an attack and find and fix the security gaps that allowed the attack to happen in the first place.

But offering cyber-recovery as a service and delivering it are two different things. Even MSPs specialising in disaster recovery may not have the resources and expertise in IT security and forensics necessary to provide adequate cyber recovery as a service. Because recovering data after a cyberattack is just the beginning, MSPs must also be able to implement new security policies and solutions to prevent future attacks and keep their clients' data safe.

Cyber-recovery as a service can be lucrative, so many MSPs consider adding it to their arsenal. But robust CRaaS requires the correct skill set and technological solutions to meet customer service-level agreements. It also requires MSPs to stay updated with the latest cybersecurity threats and provide the solutions to stop them.

CRaaS-competent MSPs ensure that their clients' systems are secure, resilient, and protected against the cyberattacks of tomorrow. Cyber-recovery as a service is an ever-evolving field, and good MSPs know this. In turn, they know that ongoing collaboration with vendors is essential.

No one solution can completely solve the issue. Many tools and techniques are required to protect customers, get them back on their feet as soon as possible, and defend them against future threats. Top MSPs have those tools and the ability to get customers up and running fast after a cyber incident, find security gaps and fix them, and implement measures to prevent incidents in the future.

Another capacity that distinguishes CRaaS-competent MSPs is understanding how to work with cyber insurance companies and, if worse comes to worst, how to negotiate with cybercriminals in the event of a successful ransomware attack. Negotiating with the attackers is sometimes the only way out, and it requires a fine-tuned skillset and detailed knowledge base that MSPs need to keep updated.

Cyber-recovery as a service offers many benefits to both MSPs that can effectively provide it, and to end customers that buy it. For the customer, CRaaS assures continuity and, possibly, survival itself. A competent MSP partner can monitor their customers' data and networks around the clock and handle any incident promptly and efficiently, giving customers confidence in the service. Furthermore, customers can focus on running their businesses because the MSP does the heavy lifting when drawing up a comprehensive cybersecurity plan.

On the MSP end, those that deliver effective CRaaS can differentiate themselves from the pack, leading to more business and healthy revenue streams. Indeed, with the exploding threat of cyberattacks, MSPs that don't offer cyber-recovery as a service may fall behind their competition.

By going the extra mile and offering cyber-recovery as a service, MSPs can create stickier relationships with their customers and open new growth opportunities. But they must do it right. They must have the correct skillset and technological solutions in place. And they must provide comprehensive cyber-recovery as a service, which means restoring data in the event of a cyberattack and continuously delivering the new products and policies needed to take on tomorrow's threats.

Cyber-recovery as a service is quickly emerging as a viable — necessary — alternative to traditional disaster-recovery methods. In the ongoing security arms race, CRaaS is a win-win. For customers, it provides data security and peace of mind. For MSPs, it opens new revenue streams and helps them stay ahead of the competition. ■

Staying ahead of cybercriminals – why the utilities sector must mitigate threats from outside and within

Alastair MacLeod, CEO, Ground Control

Like all critical infrastructure, utilities are prone to cyber threats, even in peacetime. With foe, and believe it or not friends, constantly gnawing away at network weaknesses to determine resilience and potential holes.

This digital battlefield is being fought in myriad ways - from disruption to enterprise systems that underpin a utility company's commercial and human operations, to more malign intervention of operational technology, designed to inflict severe disruption to civil society.

The AcidRain malware attack in February 2022 caused severe, prolonged disruption to operations on a mass scale. The attack wiped out Viasat's KA-SAT broadband service's satellite modems, impacting thousands in Ukraine and further across Europe.

Ultimately in the age of IoT, where machines in the home, commerce and throughout industry are given an identity and the ability to communicate, this risk is only set to increase.

Countering the threat

According to IBM, the energy industry ranked fifth in overall data breach costs in 2021, and security in the utilities sector brings with it additional considerations: it is a highly regulated industry where breaches can be prohibitively costly by any other industry's standards.

Moreover, costs associated with ransomware or cyberattacks can quickly escalate. Between 2020 and 2021, there was a reported 10% increase from $3.86 million to $4.24 million per data breach incident.

Enterprise systems on the other hand are often routed through internet protocols, are inherently more visible and therefore exposed. Ideally then, SCADA and telemetry data will not be mixed with enterprise traffic. Secure separation helps ensure this data doesn't fall into the wrong hands.

There are plenty of examples, which illustrate the level of disruption water and energy supplies are prone to. In 2021, a cyberattack forced operator Colonial Pipeline to temporarily shut down 5,500 miles of pipeline and an attempt was made to tamper with the levels of sodium hydroxide in Oldsmar, Florida's water supply. Moreover, recently in Ukraine, hostile intervention has led to the disabling of energy - in this case wind farms.

The here and the now

As IoT becomes more embedded in industry day-to-day, it becomes vital that all devices and local networks associated with a grid carry technology and software to protect them. One such way is SD WAN technology (software defined WAN) which keeps data locked down and secure from the outside world. At the same time, the technology ensures consistent application performance and resilience by automatically steering traffic in an application-driven manner based on business intent, security protocols and WAN architecture.

Primary bearers and platforms need to have alternatives in place, which means satellite, LTE, 4G/5G solutions. One of the benefits of telemetry data is its relative size. Because telemetry data requires less bandwidth than much of the traffic going over an enterprise system, it can also be more difficult to trace. Though we advise all our clients to have these backup solutions in place, and if necessary, back-ups to back-ups.

"Costs associated with ransomware or cyberattacks can quickly escalate. Between 2020 and 2021, there was a reported 10% increase from $3.86 million to $4.24 million per data breach incident."

Then there is the length of time it takes to discover a breach; often the longer the breach goes unnoticed, the more expensive and/or disruptive the incident. And finally, there are the fines incurred from regulatory bodies. All that, before we get on to reputational damage.

Cybersecurity is already top of mind for many utility firms and thankfully there are many ways to counter these threats; starting with recognising this inherent vulnerability and embedding a culture of awareness that shapes more secure behaviour, processes, and system design.

The importance of private networks

Risk increases when or if data is exposed to the open internet, which is why utilities must leverage control using the latest IP technology – securely operating within public networks or operating via secure, private networks. Private networks, and dedicated hubs, such as those within a TSAT satellite system, maintain a vital air gap between telemetry and control, and open public networks.

At Ground Control, we advise clients of risks and trends facing their operations and ways to combat this and build better resilience within their networks. This includes satellite as well as terrestrial networks, which transmit and receive data vital to the monitoring and performance of systems.

In our recent paper, 'Data's journey in shaping digital transformation in utilities, and what it means,' we examine how data has been a catalyst for digitalisation among companies within the utilities sector, and how outages and supply interruptions can result in huge financial burden and penalties for the supplier, and severe (often prolonged) disruption for consumers.

Which brings us back to the beginning; being aware of the risks, including an acceptance that they may come from closer to home than one might at first think, is as critical as the data that needs protecting. ■

Is it certifiable not to have a certification?

George Barnes, CEO, Hamilton Barnes

You can't really escape it; the media is shouting about tech redundancies, but we're also hearing of skills shortages – surely there can't be both?

It really isn't all doom and gloom. In fact, redundancies hitting headlines isn't relevant for 95% of the market. When FAANG (Facebook, Amazon, Apple, Netflix, and Google) and similar companies make mass layoffs, it is going to hit the news, but the truth is that these companies are hugely overstaffed in the first place. You'd be surprised to hear of the inefficiencies at these businesses, where redundancies are often for roles that weren't needed in the first place, or because there's five people doing a job that one person would do elsewhere.

"So there aren't really tech shortages, then?" I hear you ask. Well, it might seem like a good thing to have these candidates available to the wider market, but they present a couple of problems.

A lot of candidates, once they break into FAANG, stay within that realm. It's like a badge of honour, and joining a network vendor, a bank, or an insurer, would be a step down the career ladder for them. When in actual fact, many FAANG positions are so specialised – because there are so many people doing siloed roles – that these candidates don't have the skills and expertise to thrive in the broader market.

Hence the skills shortages. Though, rather than a skills shortage, I'd say there's a shortage of people who are good. There are also a lot of magpies out there, interested in the new 'shiny' thing – take cloud technology. It has its place, no doubt about it, but it hasn't necessarily been the holy grail that people thought it might be and many candidates are opting to return to on-premises software and technologies.

Nor does the development of networking help matters, since it was historically very linear, moving in one direction like a train. From the Catalyst 6509-E Switch to the Nexus Series, networking didn't really change for a long, long time, meaning that even ten years ago, there was a very limited range of skills required from network engineers. It was pretty easy to upgrade your skillset every couple of years when Cisco released a new product. But the advent of software defined networking, network automation, network observability, and other innovations has forced engineers to think and learn differently.

If the take-up of certifications in recent years is anything to go by, we need a shift in mindset to drive the industry's continued progression. In short, fewer engineers are doing fewer certifications, all the way up to CCIE, which is considered the pinnacle of networking qualifications. Why? I think there are several reasons.

Firstly, I don't think Cisco has done enough to ensure longevity for their certifications; they're still quite traditional. Even if 80% is still highly relevant, many engineers are questioning the remaining 20% and wondering why they can't do a certification in 5G, for example. The launch of DevNet was big news at the time, giving developers the means to implement basic network applications using Cisco platforms, but that was almost ten years ago. Put simply, the certifications aren't progressing as quickly as the tech is.

Secondly, certifications aren't cheap so many are simply opting not to do them. It's not like being a lawyer, where you have to qualify in order to practise – there's no requirement to have a certification to prove you have the necessary networking skills. Indeed, some of the best network engineers I've ever placed haven't had any certifications, but they have excellent hands-on experience. Interestingly, though, it can make the recruitment process a bit stickier when companies begrudge paying for someone that isn't certified, but in a candidates' market, such as we're seeing now, they inevitably will pay.

And I think the shift in mindset will come as a result. Businesses are desperate to hire the best talent and are wising up to the need to offer candidates attractive propositions aside from merely salaries – which are grossly inflated now, but that's an article for another time. Sustainability is another area of focus, but if I'm honest, it's one that worries me. Since it's a must-have – not just a nice-to-have – for the younger generations to work for businesses that are demonstrating how they're minimising their impact on the environment, I think we'll see a lot of lip service from potential employers. They'll build out sustainability programmes, but it'll largely be greenwashing.

In the meantime, the positive is that businesses are investing more and more time, money, and resources in their staff, to get around the buoyancy of the market. They're paying for certifications, supporting graduates with training, and bending over backwards to ensure they attract – and retain – talent. And rightly so. Businesses that show this willing are likely to get a high return as grads have a sense of loyalty to the first company they work for and are less likely to hop around from job to job. With the right coaching and training, and progression, they can be developed to be proficient managers further down the line. They are, after all, the future of the industry. ■

Brad Liggett

Nick Oram

Sylvain Cortes

Matt Aldridge

Roundtable: the dark net

The dark net has emerged as a major boon to bad actors across the globe – but what do network managers need to know?

Are today's network managers fully aware of the risks posed by the dark net?

Brad Liggett, global director and threat analyst, Cybersixgill: The dark net often makes its way into pop culture. Network managers are likely aware of the risks and threats stemming from the cyber underground; however, they may not be properly alerted to those threats, if at all.

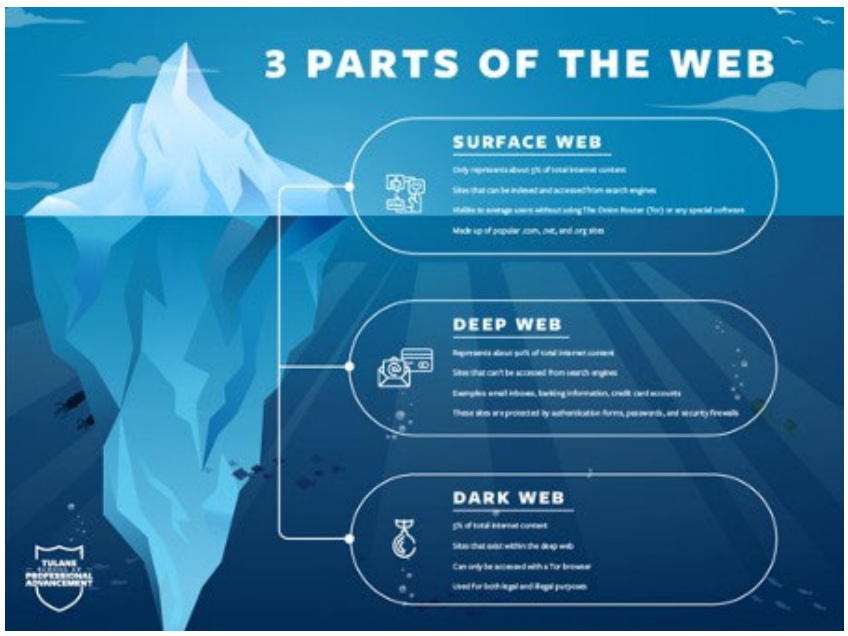
Nick Oram, operations manager – dark web & mobile app monitoring, Fortra's PhishLabs: I doubt that most network managers are aware of the full range of risks that threat actors on the dark web pose to their organisations. The dark web itself is not malicious, it's just a tool that can be used to do malicious things. The Tor browser was created to increase internet privacy and a way for people to have access to information in locations where censorship of the internet could take place. However, due to the nature of what the Tor browser does it is no surprise that threat actors have used this platform to sell their illicit goods and services to evade law enforcement.

The dark web contains many different marketplaces and forums that are used to sell drugs, weapons, counterfeit goods, malware, credit card data, and stolen credentials, but plenty of sources are completely benign and used just to connect with other users with similar interests. Most malicious items that end up on the dark web didn't originate there. If we are looking at stolen login credentials, those credentials were most likely swiped from users that attempted to log into a phishing website, or accidentally downloaded some form of InfoStealer malware and had their credentials stolen. Once those credentials are stolen threat actors will turn to the dark web to post the data for free or sell it for monetary gain.

Sylvain Cortes, VP strategy and 17x Microsoft MVP, Hackuity: Absolutely not... in fact, it's a recurring problem in organisations. There are three reasons for this:

- Dark net scanning solutions are currently technically imprecise, lacking certain information.
- Administrators and managers don't understand how the dark net works and are even afraid to connect to it.
- Legislation is unclear as to what is and isn't legal to consult on the dark net, so companies are afraid of breaking the law - what's more, legislation varies from country to country.

Matt Aldridge, principal solutions consultant, OpenText Cybersecurity: Most IT and network managers are aware of darknets, but perhaps have not fully accounted for them when assessing, prioritising, and managing risks to their organisation.



Should network managers block Tor and other dark net browsers as a matter of course?

Liggett: Network managers can provide one of the biggest defenses for stopping dark web usage in a corporate environment by ensuring that traffic destined to, or coming from, known Tor exit nodes is blocked. The dark web hosts malicious content and links which can be more difficult to block if users are able to access Tor on their work devices.

IP addresses are ephemeral and constantly changing. It's difficult for network managers to keep up on which CIDR blocks, or specific regions, to allow. There are a handful of companies that monitor IP traffic and usage. Whether traffic is coming from various proxies, tied to commercial VPNs, or have markers of running through anonymisation services, network managers have more tools available to them now than ever before.

Aldridge: Darknets and the dark web have an important place in the world when used for legitimate purposes, but in almost all cases they should not have a place in your organisation, so measures should be taken to control, or at least to monitor any such activity. Blocking access to Tor and similar darknets should be high on the list of priorities for any organisation. Raising alerts to the security team when access attempts are made is also important. This can be largely achieved through a combination of client-side and network-embedded security solutions, although be aware that a determined user will probably find a way around any network controls.

Admins should consider taking a whitelisting approach to allowed applications in their environment and consider Windows Defender Application Control (WDAC) for Windows devices and Google Santa for MacOS devices. Other third-party solutions are also available. This is not a silver bullet however, as certain user populations will need to be able to install and run code that may not yet be whitelisted, for example developers, IT and security teams, however, having whitelisting as the standard approach for most users can realise very strong security benefits for the organisation, as long as there are swift processes in place to help users to get access to new applications when needed. Whitelisting can also be a challenge when allowing BYOD (bring your own device).

Oram: Network managers don't need to block dark web browsers. Browsers like Tor can be used just like Chrome or Firefox, with the exception that Tor can help with browser anonymity and security, such as blocking targeted ads, unwanted external connections, and network traffic. The main difference with Tor is that it can be used to browse Onion sites. When using Tor, a user should be careful not to look up or stumble onto

something malicious just as they would on any other browser.

Cortes: The history of cybersecurity teaches us that banning things is never the solution. Tools and procedures need to be put in place to control use of the dark net, but trying to prevent people from logging on is pointless. Also, it's technically complicated: a lot of effort for little result in the end…

What is the biggest single danger from the dark net, and how can it be tackled?

Liggett: If accessing the dark web, possibly the most significant risk is exposing yourself or your organisation to malicious threat actors frequenting the cyber underground. Users need to be careful to not click any malicious links or download programs hosted on underground sites.

Cortes: By itself, the dark net is not 'so' dangerous. The biggest risk is not technical, but legal... Legislation varies from country to country. Some countries allow you to download files from leaks under certain conditions, while others prohibit it. Some countries consider that authenticating with login and password on a forum is illegal, others do not. It's important to make sure that the activities you're carrying out are legal - and even to make sure that the functionalities offered by an external supplier are legal in the organisation's country. I see a lot of French teams using American dark net scanning solutions, even though their usage is illegal in France!

Aldridge: By its nature, darknet traffic bypasses all security controls that an organisation has in place, directly exposing the user and their endpoint to significant levels of threat from unknown actors on the dark web. This can expose them and their organisation to data breaches, malware infections, legal liabilities, and reputational damage. Controlling and monitoring access attempts will help to protect legitimate users who may have been socially engineered or extorted to access the dark web and make it harder for attackers to stay under the radar for their command and control (C2) and data exfiltration activities – forcing them to use more visible, public solutions. Equally, blocking access to corporate assets from Tor users is extremely important, unless there is a legitimate business need to allow this for certain key applications.

Oram: Combating the threats on the dark web begins with increased knowledge and awareness in places where users already spend a lot of their time, the open web. Most users at some point will be sent a very convincing email or even a SMS message that wants them to log into one of their favourite sites, but it's a phishing website that was created for the purpose of stealing credentials. The link could also lead to a malware download link, and once that malware is downloaded, credentials and other personal information could be stolen, or the computer could be locked up using ransomware.

Common on the dark web is the sale of credentials that have been grabbed through InfoStealer malware, which can be delivered through traditional phishing methodologies. Once those credentials or other forms of personal information are stolen, they can be sold on the dark web. In addition, daily activity outside of the open web can lead to content posted on the dark web for sale. Threat actors who install sniffing software, skimming devices, or perform point-of-sale device compromise in the various areas where you spend your money, can easily grab your credit/debit card credentials. When your credit/debit card data gets compromised it is common for it to appear for sale on dark web marketplaces that sell dump and data.

Does every enterprise need dark net monitoring tools?

Liggett: While there are some justified reasons for using various privacy tools, if users in that organisation require the ability to connect to these services, each company should weigh the risks of not monitoring for such activities. If someone has a legitimate reason for this type of activity, network and IT managers should ensure that safeguards are in place to allow for access using independent hardware and connections.

Oram: For the safety of all enterprises' employees and customers, they should subscribe to some form of dark web monitoring. A user's information is most likely going to be stolen through the open web, a phishing site, malware, social engineering, or by the the illicit use of credit card skimmers, sniffers, and POS device compromise. Once that information has been stolen, threat actors can then turn to the dark web to post this information.

Cortes: A month ago, I was preparing a presentation for a show, and I wanted to demonstrate to the audience what information from ransomware gangs on the dark net looked like. I went to the LockBit 3 website and found a list of leaks which included companies I knew well. I then contacted the CISOs of each of these companies, who didn't even know their data was on the dark net! Dark net monitoring tools are not perfect, but they are critical.

Aldridge: Every enterprise should determine the need through a comprehensive and ongoing risk assessment, but I would suggest that at the very minimum, an ability to monitor access to the dark web should be present in the security arsenal of every organisation. ■

Modernising critical comms

As technical capabilities expand, how are critical communications networks evolving? We asked the experts for their insight and what the future might hold

Critical communications networks save lives every day, delivering uninterrupted service reliably, under exceptional circumstances.

"Critical communications networks must be available 24/7 and in particular when other networks are failing, supporting the ability to communicate during disasters, major incidents, times of civil unrest or when an element of critical national infrastructure becomes unavailable," says Duncan Swan, chief operating officer, British APCO.

Data-centric design

While the fundamental requirements for a critical communications network are the same as ten years ago, the possibilities to fulfil the requirements have evolved.

"Though group voice communications remain vital to fire, rescue, and law enforcement, innovative LTE-enabled data applications have arrived that deliver functionality significantly improving operational safety and effectiveness," says Ken Rehbehn, principal analyst, CritComm Insights. "Critical communications systems based on legacy land mobile radio technology, such as TETRA or analog radio, do not have sufficient bandwidth to support most new data capabilities. That gap drives a push towards LTE systems supporting mission-critical services."

Swan agrees that the underlying technology that comprises these networks has changed significantly: "using new technology opens up a wealth of new possibilities to communicate… data and video have an ever-increasing role to play to improve efficiency and effectiveness – in particular in determining how best to respond to a situation."

Though interest is growing, video plays a limited role, opines Rehbehn. "Video feeds from drones frequently flow over unlicensed spectrum that is not public safety grade. As agencies embrace LTE delivering critical communications with QoS, priority, and preemption, the use of video becomes more practical. For example, US FirstNet users with Axon body-worn cameras can now send video to the control rooms when a police officer removes their gun from a holster. This video-enabled perspective provides a crucial situational status that cannot be quickly transmitted by voice alone."

"They say a picture paints a thousand words – and data and video can both provide greater situational awareness; allow those relying on critical communications networks to receive real time information that is relevant to their current situation; and monitor the wellbeing of workers in difficult situations," adds Swan.

"The public safety radio communication operational model has been voice centric for the past hundred years," says Tero Pesonen, chair, TCCA Critical Communications Broadband Group. "[But] the ability to transfer dynamic on the spot-generated data such as video changes the situation. The paradigm can shift to information centric operation where the concept of information value chain can be applied. The data generated in one format may merge with other data and be presented in different forms and shapes to each receiver according to their need. Real-time image and video transmission are paving the way into this direction enabling both the leadership and field operatives to have more accurate situational awareness and take more informed decisions."

"Data access is an important capability in today's critical communications networks," agrees Rehbehn. "New LTE networks provide high throughput that supports mobile data terminals linked to computer-aided dispatch systems and general office desktop systems. Data systems are also essential in today's emergency medical service, enabling electronic patient reporting and hospital communications."

With the rise of data, security becomes an increasingly pressing concern. "Security is paramount to protect the network and services," adds Martin Duggan, principal network architect, Systal. "Automation is increasingly being used for repetitive tasks and has enabled integration to multiple systems enhancing the efficiency and effectiveness of the services."

Capacity vs coverage

Network operators design LTE networks to be commercially viable, which means some thinly populated or mountainous regions may not have universal coverage. Nations investing in LTE-based critical communications networks have required service providers to expand coverage to these areas, but some remote areas remain underserved.

"Beyond geographic coverage challenges, in-building coverage may be the weakest link in future LTE-based critical communications networks. Energy-efficient building design blocks radio signals, LTE included. Without in-building coverage systems to get signals in and out, emergency workers may be cut off when they need connectivity the most," says Rehbehn. "Legacy land mobile radio systems operate at lower frequencies, offering better penetration into and out of structures. Nations that move from legacy land mobile radio to LTE may quickly discover that the new network fails when responders travel to the bottom of a large structure."

"For 4G and 5G network technologies a tremendous amount of work has been done in 3GPP standardisation and elsewhere to enable these networks to address the original requirements; but the needs of present-day societies are not feasible for any narrowband technology to meet due to the limited bandwidth," shares Pesonen.

"There's a real dilemma as to how much you spend (in both money and time) both hardening a network and ensuring it has the right level of coverage and capacity," says Swan. Lower frequency solutions provide better coverage as well as penetration into buildings, "but that is at the expense of a true broadband capability," adds Swan. "The meshing of different networks is one way to achieve better coverage and functionality – as well providing the hardening of the overall solution through diversity."

A critical tomorrow

Critical communications networks will continue to evolve as new capabilities become reality.

"We see a use case for higher bandwidth, reduced latency and additional endpoints on the network, there will be more data to process, and attack vectors will increase meaning the network will need to provide additional levels of security by use of ML & AI," says Duggan.

"We expect the introduction of haptic capabilities to mature to enable humans to interact remotely with a combination of senses. These combined with augmented and virtual reality create interesting operational and technological avenues to explore," says Pesonen. "M2M communication with ever increasing data flow of IoT sensors will provide better situational awareness, predictive operation and much more, but at the same time it requires very sophisticated and balanced AI to manage the massive information amounts."

Swan agrees that diverse technology will be key going forwards. "We can expect device evolution that incorporates mission-critical services over LTE with push-to-talk, video, and data alongside a non-LTE radio that provides a backstop when LTE networks are not reachable," says Swan.

Additionally, a growing role for satcoms as LEO constellations expand, enabling 'vehicle as a node' concepts, will emerge. "Communications hubs mounted on a vehicle will select the most effective and lowest cost path for communications from a range of options: land mobile radio, LTE, mesh connectivity, and satellite links. The concept can already be found in Australia, and we expect it to gather momentum," concludes Rehbehn. ■

Why remote care and connected devices are becoming more commonplace in healthcare

Nick Earle, CEO, Eseye

The healthcare industry faces significant challenges with long patient backlogs, a shortage of staff and resources, all of which has been exacerbated by the COVID-19 pandemic. There are literally millions of people in the queue awaiting treatment and many more that simply haven't come forward for care or referrals, as patients put off engaging with healthcare systems.

Those with minor problems and early-stage symptoms subsequently develop more serious conditions, which are harder to treat and in turn increase the cost of healthcare provision.

Demand is outstripping supply

The crux of the problem comes down to demand significantly outstripping supply. As more treatments become available and the population ages so this increases healthcare needs, with evolving and more complex treatment paths required. As healthcare providers desperately look to release clinicians and professionals from the more routine or mundane tasks and free up their capacity to manage more challenging patients, more patient and healthcare services are moving to remote patient monitoring (RPM).

RPM is transforming the way that healthcare is delivered, resulting in easier access, reduced costs and improved patient outcomes.

Fuelled by COVID-19, with hospital visits limited, RPM has grown exponentially. Rather than revert to in-person appointments for monitoring or support, the use of RPM has continued to grow post-pandemic. Now, the goal for most healthcare providers is to have connected healthcare in every home that needs it, which is more than most of us realise. For example, one in three people worldwide suffer from hypertension, a condition that requires accurate daily monitoring to prevent serious illness.

Likewise, most of us don't realise how much of a burden long-term conventional monitoring puts on healthcare providers. This type of monitoring is also restrictive and inconvenient for patients, which is another reason why RPM has grown in popularity, because it enables patients to be monitored and support delivered, even in hard-to-reach locations, delivering data back to medical teams to review and act on where necessary.

Regardless of where a patient is located, healthcare providers are better equipped to monitor, evaluate, and respond to acute as well as chronic medical conditions in real-time with RPM technology.

Removing the barriers to RPM

The success of RPM depends heavily on device connectivity, accuracy, and ease of use for the target market, which is typically older people who may have lower confidence with technology. Healthcare providers must remove patient barriers by making healthcare technology easier to use, so that patients can just turn on a device and take a reading without having to worry about faulty connections.

"Delivering devices that are readyto-use and work straight out-of-the-box is essential to enhancing the user experience, building both patient and provider trust and more importantly improve patient health outcomes."

Currently there are two key technologies that are enabling RPM device communication: Bluetooth and cellular connectivity. Bluetooth has typically been the more conventional approach, however more recently healthcare providers have started to favour cellular connectivity.

To truly revolutionise the patient experience, doctors need daily readings of blood pressure, blood glucose, pulse oximetry, weight, and temperature levels so they can quickly identify changes and send out a professional, call a patient in, or alter medical care plans if and where necessary.

However, Bluetooth connections are proving unreliable with patients experiencing difficulties such as pairing their RPM device over Bluetooth with their mobile devices. Additionally, Bluetooth usually relies on the patient's personal mobile device for data transmission, and this means that while data is uploading the patient is restricted to staying within Bluetooth range.

This also makes remote support more challenging and likewise app store data restrictions can limit the amount of data accessible from the transmitting device. This level of unreliability creates a lack of trust: trust in the device; trust in the accuracy of readings and trust around whether there is a genuine problem that needs to be acted upon.

Why providers are switching to cellular

This is driving the switch to cellular devices which offer wider coverage – where devices are always connected to the strongest network possible – and more flexibility, enabling patients to transmit data from wherever the cellular network is available. It also means that patient health data can be transmitted in real-time, which enables immediate alerts to healthcare teams in times of distress or difficulty.

But most importantly, particularly in relation to older patients who may not be as tech savvy, cellular RPM devices are more user-friendly; all patients need to do is press a button and take a reading as usual.

This not only increases patient satisfaction, but it also improves adoption rates and reduces the barriers between the patient and the healthcare team.

Not only is cellular connectivity revolutionising RPM but it is also fuelling significant growth. In fact, new research from Kaleido Intelligence has found that cellular data usage by the healthcare sector will increase almost 500% over the next five years, driven by an increasing use of connected healthcare both at home and in clinical settings.

Kaleido Intelligence is predicting that cellular connected healthcare devices will transmit nearly 90 petabytes of data annually by 2027. The new report, Healthcare Cellular IoT Opportunities & Forecasts 2022 notes that this increase in connectivity comes both as a result of necessity from the COVID-19 pandemic and due to the maturation of IoT.

Reliable cellular connectivity helping RPM to meet future challenges

Going forward, the NHS' Long Term Plan 2019 (LTP) makes it clear that new models of health and social care are required to meet the population's needs now and in future. England's ageing population, the growth of chronic conditions and co-morbidities, and deployment of new technologies and treatments are all contributing factors to healthcare challenges.

RPM is one way that providers can reduce the burden on already over-stretched teams and cellular technology is revolutionising both the design and capability of healthcare devices. Delivering devices that are ready-to-use and work straight out-of-the-box is essential to enhancing the user experience, building both patient and provider trust and more importantly improve patient health outcomes. ■

ICS.AI streamlines communications for Derby City Council

Derby City Council and Derby Homes are on a journey to innovate how they engage with residents, supplementing their main switchboard with phone-based artificial intelligence (AI) assistance.

"It quickly became clear that AI had the potential to dramatically streamline our customer service operation. We started first with an AI-powered website assistant and followed by supplementing our main switchboard with phone-based AI," said Andy Brammall, director of digital & physical infrastructure and customer engagement at Derby City Council.

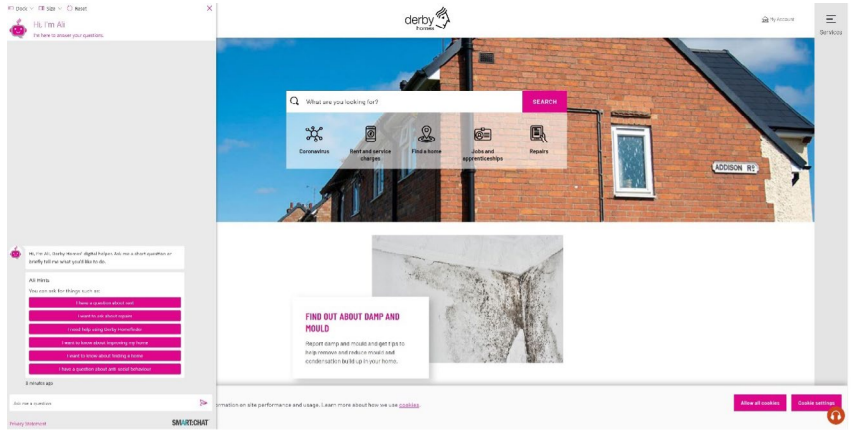
The council partnered with ICS.AI and leveraged their SMART AI platform for this transformation. This development sets a benchmark for using AI to streamline public services and enhance citizen engagement.

"We chose the SMART AI platform from ICS.AI for several reasons. Their strong reputation and proven experience in the local government sector reassured us of their capabilities," said Brammall. "They offered a 'human parity' council AI language model trained in over 1,000 council topics, which could be rapidly deployed, and we were confident in their performance and their proven commitment to innovation in the phone channel. Above all, what really appealed to us was ICS.AI's genuine interest in working as a true collaborative partner."

Simplifying interactions

Inbound phone calls represent 60%+ of resident contact with the council, and therefore was the cornerstone of Derby City Council's self-service strategy.

"Our new AI assistants not only allow citizens access to a range of council services and information around the clock and across multiple channels, but by automating routine tasks they also free up time for our colleagues to focus on more complex queries which require human conversation. This ultimately aims to provide a more personalised service for our residents, improving service delivery and achieving higher levels of resident satisfaction," said Brammall.



The new AI system employs advanced natural language processing, providing a user-friendly, 24/7 service in natural language to simplify interactions. The AI assistants - Darcie, servicing the council's customer service centre; and Ali, serving Derby Homes - are currently answering more than 1,000 questions each day, directly handling up to 45% of inbound calls. Beyond answering citizen queries, they can also direct calls to over 40 different departments.

"Trained in over 1,000 council services, it has exceeded our deflection target of 21%, handling over 62,000 calls and achieving an incredible 43% deflection. This success has allowed us to maintain our service levels while streamlining operations," said Brammall.

Streamlining operations

"Derby City Council's AI initiative actively addresses the surging demand for council services. Our AI assistants aim to streamline operations and manage demand peaks, enhancing citizen satisfaction and providing a seamless experience," said Martin Neale, CEO at ICS.AI. "By handling large volumes of inbound calls and common queries, they help reduce waiting times, improve call efficiency, and lighten the staff workload during peak times. This strategy commonly opens opportunities for staff redeployment to other tasks, contributing to potential operational cost reductions."

The council is committed to further exploring the potential of AI technology across additional contact channels and service areas. This initiative showcases their dedication to improving customer service and increasing efficiency for its citizens.

"Derby City Council's commitment to innovation was critical to successfully deploying one of the most sophisticated AI engagement solutions in the public sector. This significant development demonstrates the Council's leadership in the sector. We're delighted to continue supporting them in developing their new AI-driven strategy, which I can see is already making a substantial impact on their contact centre," said Neale. ■

Enhancing Barking & Dagenham council enquiries with EBI.AI

Barking & Dagenham council (B&D) was experiencing an overwhelming number of enquiries about missed bins. They identified that they needed an AI assistant that could confidently handle waste enquiries about missed bins, bin collection schedules and bulky waste collections, 24/7, 365 days a year, to take the pressure off their teams.

End-to-end journeys

B&D duly signed up for an EBI.AI assistant to tackle the problem. There were several queries about bin collections they needed to address urgently:

'When does my bin get collected?'

'What day does my recycling bin get taken?'

'Is my bin collected the same time each week?'

For their AI assistant to handle these kinds of enquiries from start to finish, it had to be able to understand the address first. B&D were able to link up their AI assistant with their council systems so it could access their catalogue of addresses and postcodes, and bin collection schedules. Now, when residents ask the AI assistant about waste collections, they're asked for these details. Over the past three months the success rate for the AI assistant to resolve these kinds of queries from start to finish is 98%.

Within six months of the new AI assistant for waste going live, B&D reported a 6% reduction in call centre calls. After nine months, it was trained to answer thousands of enquiries across five more departments too, including council tax, parking, permits and penalty charge notices, benefits housing repairs, and registrars.

Using EBI.AI's platform for conversational AI, B&D were able to expand their AI assistant across departments at no extra cost. The AI assistant is well publicised on their council web pages, now handling thousands of enquiries about multiple topics - and it's easy to add more.

"The chatbot is transforming the way our customers access information. We believe we can enjoy better customer relationships by allowing customers to contact us via the channel of their choice. Our next focus is to allow our customers to complete end-to-end journeys via the chatbot," said Dwain Nicely, CX & digital manager at B&D.

Saving on critical communications

With the new AI assistant, B&D began to make significant savings. Every enquiry into the B&D contact centre costs the council around £4.80 and they get 40,000 a month. With the AI assistant handling 10,000 of those in the first six months, that's a massive saving on council spending, which can only increase as the AI assistant takes on more tasks.

It's also proven popular with residents. Having an AI assistant online 24/7 showed B&D early on that 28% of their queries come in outside of office hours, at a time that's convenient to their customers. Getting to know customer preferences in this way means B&D can improve services and satisfaction.

Moreover, now that B&D can see customers are happy to use their AI assistant across a wide range of departments, they've seen a reduction in calls to their contact centre. Their agents now have more time to focus on more sensitive enquiries or difficult issues that need the human touch.

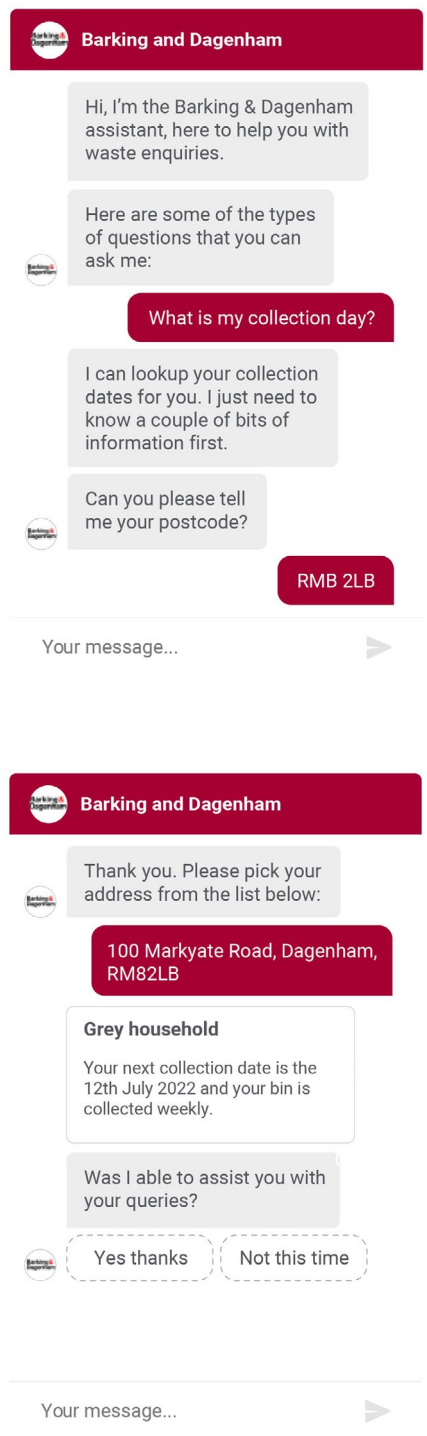
According to EBI.AI, the AI assistant enables responses to be edited in seconds to deliver consistent messaging on critical matters for the audience. For example, should schools be closed due to poor weather, instead of having to update websites and multiple agents manually, B&D can simply tell the assistant, which disseminates the information.

Shaping AI for local government

The EBI.AI team of conversation analysts continually review conversations between B&D residents and their AI assistant, looking for patterns to see where improvements can be made, and new departments added if needed.

Like many councils, B&D want to see reports and statistics for their AI assistant, to be involved and track progress, and to get a real understanding of the value they get from using AI. The EBI.AI platform has an easy-to-use dashboard, to view the most popular topics, track success rates, see the number of out-of-hour queries, and more.

Since residents need a council for help with everything from recycling and parking to marriage and benefits, EBI.AI's assistants are cross-departmental. Councils can add as many new queries as they like, from any department, to keep it growing. ■



Unlocking tomorrow's connectivity

Damian Hanson, co-founder & director, CircleLoop

As the countdown to the Public Switched Telephone Network (PSTN) Switch Off ticks on, business leaders are inclined to investigate the evolving landscape of 5G connectivity. However, recent analysis indicates that some UK businesses might encounter connectivity challenges post-Switch Off due to the sluggish pace of 5G deployment.

It is essential to keep an eye on the current state of 5G availability across the UK, the capabilities it offers, and the prospects it presents for your business today and in the future.

What's driving the Big Switch Off?

PSTN has been the backbone of traditional communication networks since its establishment in 1875, but BT Openreach feels it has become too unreliable and outdated. This transition will have a significant impact on various devices that depend on copper PSTN wiring, such as landline phones, fax machines, alarm systems, and door entry systems. To ensure continued functionality, every household and business in the UK will need to migrate to a digital network, specifically one that utilises Internet Protocol (IP), as conventional telephone lines will cease to be supported by UK networks beginning in 2025.

5G connectivity in the UK

The Switch-Off will transform the telecoms landscape. It will require businesses to adapt their communication systems to the new digital era.

A recent study by Vodafone suggests that the UK economy could see up to £5 billion in annual benefits with the adoption of top-tier 5G networks. The widespread adoption of 5G-enabled technologies is significantly influencing various aspects of society while supporting the government's goals of fostering digital transformation and job creation. But the big question looms, is Britain ready?

To understand Britain's communication infrastructure readiness, CircleLoop recently conducted an analysis. The analysis ranked major towns and cities based on their 5G availability from the country's four major phone networks: EE, Three, Vodafone, and O2. The findings revealed that only 51% of major UK towns and cities have full 5G coverage, indicating that the rollout progress has been slow, leaving many communities with limited or no 5G connectivity.

However, our analysis also offers valuable insights for businesses considering expansion or startups seeking optimal network support for their digital operations. It highlights the regions in Britain that excel in 5G connectivity. London, with a 96/100 score for 5G connectivity, Yorkshire at 86/100, and the East Midlands at 85/100 stand out as the leading regions, providing exceptional business 5G connectivity scores. These areas are well-equipped to deliver reliable and high-speed 5G services, presenting abundant opportunities for businesses to thrive in the digital age.

The situation is less favourable in certain regions. Scotland only scored 52/100, Wales at 65/100, and the South West at 69/100 demonstrate lower 5G service levels in comparison. This disparity highlights the importance for businesses in these regions to carefully strategise their communication plans to remain competitive in the evolving landscape.

Exploring business alternatives

Given the constraints imposed by the stoppage of traditional communication methods, businesses are presented with a range of options to ensure their readiness for the future of communication technology. Among these alternatives, Voice over Internet Protocol (VoIP) stands out as one of the most promising for future business connectivity.

VoIP technology harnesses the potential of the internet to transmit both voice and multimedia content. In contrast to conventional phone systems, VoIP offers numerous advantages that align perfectly with the contemporary demands of businesses.

As VoIP can be accessed via WiFi or mobile networks, businesses can embrace the transition to a cloud-based phone system. This adaptation positions them strategically for the future, ensuring they remain at the forefront of communication technology when 5G connectivity becomes universally accessible across all locations.

What to keep in mind

As we approach the PSTN Switch-Off, businesses must factor in the integration of 5G into their operational strategies. While concerns about the discontinuation of traditional telephone systems are legitimate, embracing the possibilities offered by 5G holds the potential to greatly enhance both internal and external business communications, promising a brighter future. ■

How to choose between traditional antivirus and endpoint detection and response (EDR)

Iratxe Vazquez, senior product marketing manager, WatchGuard

The wide range of devices and the need to access network resources from anywhere has blurred the traditional security perimeter and extended it beyond the office. As a result, endpoint security is now an essential pillar of any company's cybersecurity strategy. Both antivirus (AV) and endpoint detection and response (EDR) solutions have been designed to secure devices, but they provide very different levels of protection.

The six main differences between AV and EDR

Traditional antivirus software is installed directly on a device or server to protect it from malicious programs. An EDR system is software that detects and halts cyberthreats, while providing visibility and control over devices on a network. There is some overlap between the functions of the two solutions, however they differ in the following ways:

- Security approach: AV systems are reactive, so only acts when there is a threat. EDR solutions are proactive. So, as well as blocking access, as AV solutions do, they can also detect and stop threats that have somehow gained access to devices.
- Scope of protection: traditional antivirus is a decentralised security system with limited scope and is simpler than detection and response solutions. EDR provides centralised security and continuously monitors threats at all endpoints of the network, delivering more comprehensive and holistic protection.
- Detection method: AV systems are based on static threat signatures and patterns, so they only recognize known threats. EDR, is behaviour-based. It monitors and detects known or unknown threats in real time by identifying anomalous behaviour at network endpoints.
- Automation and visibility: EDR constantly collects and analyses data. Thanks to artificial intelligence (AI) and automation, EDR converts that data into actionable intelligence and provides full visibility into devices within a corporate network. This means data patterns can be isolated quickly to provide security teams with fast and accurate assessments of any behaviour that indicates a potential threat. This cuts down detection time and reduces the need to rely on highly skilled security personnel. AV relies on the antivirus developers adding viruses or variants to the malware list every time a new one is identified. Otherwise, this any new malware will remain undetectable.
- Response method: an AV solution acts when a threat has entered the system before it is able to perform malicious actions. This is usually by automatically preventing its execution, deleting the file and any traces it may have left on the way. EDR responds in an automated way with actions such as blocking execution and isolating endpoints to prevent malware from spreading. This provides time to investigate the potential threat, its impact and how to recover from it.
- Response time: Avs response is immediate and automated, but detection capability is limited to known threats. EDR systems can detect sophisticated and unknown threats that otherwise would go under the radar. However, detection and response time depends on the automated detection, visibility and containment and remediation that the EDR system provides. Some delegate responsibility to analysts, for example, when classifying files that are executed and have performed suspicious actions. Ideally, an EDR solution should detect, investigate and take automated action as early as possible to reduce response time, but it should also have a tendency towards zero false positives.

Which is the best option?

Traditional antivirus detection can be ineffective in identifying and protecting against advanced malware and new variants. Today, malware writers use techniques such as fileless malware to evade detection by traditional antivirus solutions.

Effective detection will often require more information and context. An EDR solution can pinpoint attack and compromise behaviours and indicators successfully, and by automating response capabilities, security analysts can delegate response to the system or act more quickly, providing efficiency gains in dealing with potential security incidents.

However, antivirus software may still be the right solution for a company with a small budget and those without a security manager to configure and monitor the automated actions for the protection selected.

EDR is the better fit where the endpoint security solution needs to be monitored from a broader standpoint, protecting a larger number of devices exposed to advanced threats, such as remote workers.

If you do opt for an AV solution over EDR it is important to make sure that this solution is advanced or next generation, so it covers a greater number of advanced threats, including those using malware-less techniques. ■

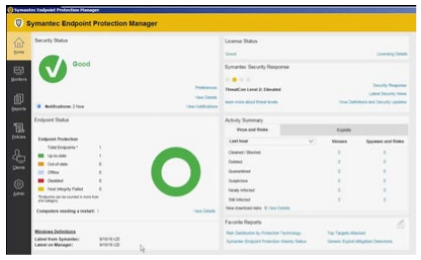
PRODUCTS

Symantec Endpoint Security (SES) Complete delivers comprehensive protection for all traditional and mobile devices across the entire attack chain.

Capabilities include behavioural isolation, active directory security, and threat hunter technologies to protect endpoints against sophisticated threats and targeted attacks. For higher return-on-investment and lower total cost of ownership, this single-agent solution supports on-premises, hybrid, and cloud-based deployments.

Endpoint security starts with prevention. Besides a safer, more compliant environment, the security team will have fewer alerts to investigate and endpoints to remediate. Attacks are rapidly accelerating, and the attack surface has grown with the increase in remote workers and proliferation of macOS and mobile devices.

Highly sophisticated attackers leverage 'living-off-the-land' techniques to blend in with normal activity and fly under the radar. While the enterprise can't turn off legitimate applications and dual-use tools, it can protect endpoints from these threats with adaptive protection.



SentinelOne Singularity offers unified prevention, detection, and response across a security estate. It simplifies modern endpoint, cloud, and identity protection through one centralised, autonomous platform for enterprise cybersecurity.

The platform makes machine-speed decisions against threats on the front lines, equipping every endpoint and workload — no matter their location or connectivity — to respond intelligently with powerful static and behavioural AI. Modern enterprises gain the visibility, analytics, and AI-driven automation they need to protect against known and unknown cyber threats, detect and hunt malicious actors, and remediate endpoints at machine speed, without human intervention.

SentinelOne supports threat hunting

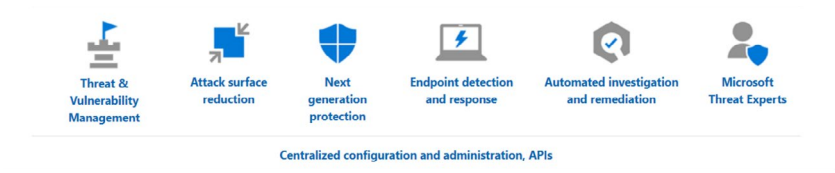
using MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs), the behavioural indicators mapped by the MITRE ATT&CK framework, to help analysts understand endpoints behaviour and accurately detect and respond to any anomalous activity. This helps uplevel analysts' skills and context and makes the EDR user experience more satisfying and efficient from day one.

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

Defender for Endpoint uses big-data, device learning, and unique Microsoft optics across the Windows ecosystem. Enterprise cloud products, online assets and behavioural signals are translated into insights, detections, and recommended responses to advanced threats.

Built-in core vulnerability management capabilities use a modern risk-based approach to the discovery, assessment, prioritization, and remediation of endpoint vulnerabilities and misconfigurations. To further enhance the ability to assess the enterprise's security posture and reduce risk, a new Defender Vulnerability Management add-on for Plan 2 is available.

The attack surface reduction set of capabilities



provides the first line of defense in the stack. By ensuring configuration settings are properly set and exploit mitigation techniques are applied, the capabilities resist attacks and exploitation. This set of capabilities also includes network protection and web protection, which regulate access to malicious IP addresses, domains, and URLs. To further reinforce the security perimeter of the network, Microsoft Defender for Endpoint uses next-generation protection designed to catch all types of emerging threats.

Embedded endpoint behavioural sensors collect and process behavioural signals from the operating system and send this sensor data to the private, isolated, cloud instance of Microsoft Defender for Endpoint. Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Defender for Endpoint to identify attacker tools, techniques, and procedures, and generate alerts when they are observed in collected sensor data.

The **CrowdStrike Falcon** platform is purpose-built to stop breaches via a unified set of cloud-delivered technologies that prevent all types of attacks.

CrowdStrike Falcon responds to today's challenges with a powerful yet lightweight solution that unifies next-generation antivirus (NGAV), endpoint detection and response (EDR), cyber threat intelligence, managed threat hunting capabilities and security hygiene — contained in a tiny, single, lightweight sensor that is cloud-managed and delivered.

The platform has revolutionised endpoint security by being the first and only solution to unify next-generation antivirus, endpoint detection and response (EDR), and a 24/7 threat hunting service — all delivered via a single lightweight agent. Using its purpose-built cloud native architecture, CrowdStrike collects and analyses more than 30 billion endpoint events per day from millions of sensors deployed across 176 countries. The unique benefits of this unified and lightweight approach include immediate time-to-value, better performance, reduced cost and complexity, and better protection that goes beyond detecting malware to stop breaches before they occur. These capabilities are based on a unique combination of prevention technologies such as machine learning, indicators of attack (IOA), exploit blocking, unparalleled real-time visibility, and 24×7 managed hunting to discover and track even the stealthiest attackers before they do damage.

Please meet...

Oliver Ledgard, government and public sector lead, EMEA, Zebra Technologies

Who was your hero when you were growing up?

As a Huddersfield Town fan growing up in the south of England, achievements to shout about were few and far between, but when the home-grown talent of Andy Booth joined the side and helped Town achieve promotion into the Championship, I could talk about my allegiance with pride. Andy Booth is a living legend and hero.

What was your big career break?

My big career break was probably very early on when I was offered a placement year with a major technology company within their computing division as part of my university degree, and after university was offered a role with the firm. Being part of that team driving mobile digitisation with rugged devices taught me early around how to understand customer challenges, develop long term solutions and driving return on investment. They're lessons I've used and built on throughout my career and shared with those who are entering the industry.

Speaking of which, my colleague Oliver Horrell was a recent recipient of the inaugural Ian Thompson Bursary Award at BAPCO in March. He's earlier on in his career, and the bursary will provide him opportunities to grow his network and knowledge around public safety and critical communications in different countries. He is keen to share his observations about the current levels of engagement in the public safety environment and make suggestions as to how partnerships and collaborations could grow to drive the next generation of future-proofed, economically viable, and environmentally sustainable solutions. I think sometimes 'big career breaks' are the ones you help others to achieve.

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

It would likely be around sport. If I could hit a golf ball longer, straighter, and more consistently a professional golfer would be the dream. Yes, I like a lot of sport as you can tell. There are the usual good reasons why those dreams will stay just that – dreams, although I still enjoy a round of golf and a good kickabout.

More realistically, coaching my son's football and rugby teams has been enjoyable, and reminds me how important that life-work balance is, especially if we're travelled a lot for work, for example. I'm lucky to be in a role and with a company that makes that balance possible and encourages it in fact. I've other colleagues who also coach sports teams or engage in sport (mountaineering, martial arts, triathlons, ironman) to a high level – there must be something in the Zebra water!

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

Growing up I was always into sport, so I aspired to be a professional sportsman, but never made the grade. I am still dreaming but based on my silver hair and aches and pains I think I'm grown up now. I keep active with various sporting endeavours too.

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

This is a tough one, but I think with his sense of humour and authenticity, Ricky Gervais would be top of the list for dinner. I am huge fan of his TV shows. I should probably be smart and say a celebrity chef too, so the food would be top class.

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

Open your ears and listen. Listening is essential for understanding customer needs, building relationships, problem-solving, decision-making and conflict resolution I see too often one way traffic on presenting vendor solutions without understanding the challenges the customer is going through. I like the saying "we've got two ears and one mouth for a reason." Listening is really a defining feature of the partner looking to create a solution that starts with the customer's pain point or modernisation goal.

What's the greatest technological advancement in your lifetime?

The internet and world wide web would have to be my top two. It's incredible how these have revolutionised global communication, information sharing and commerce. It has connected people worldwide, transformed industries and enabled the rapid exchange of knowledge and ideas. And lots of new industries businesses and jobs have been built off the back of the web and internet.

I think we live in an exciting time when the pace of change is rapid, and I wonder what's coming next. It'll be interested to see how AI shapes how we use the web and get new uses and insights from the mountains of data. I also wonder how the metaverse will take shape and grow, after the initial wave of attention from tech companies and the media. ■