APRIL 2024
networkingplus.co.uk

NETWORKING+

Sustainable networking

We need capacity faster than we can build it

Steven Carlini, Schneider Electric, p9

Digital twins: the full picture

Have you heard of a connectivity twin?

Khuong Quan, BICS, p14

Questions and answers

It's hard to imagine a non-connected world now

Jim Liddle, Nasuni, p16

Businesses must stay vigilant to 'cybercrime-as-a-service'

The middle of April saw a huge win for the UK's cybersecurity sector when local police took down 'cyber fraud superstore' LabHost.

LabHost – which advertised itself as a 'one-stop-shop for phishing' - allowed users to produce realistic websites from household names like banks, utility companies, and fashion brands, to scam victims across the globe – 70,000 alone in the UK. After following a malicious link, the victims would enter their details; some were used to steal money, others were sold on the dark web. LabHost amassed 480,000 debit and credit card numbers, 64,000 pin numbers and made £1 million from membership fees from 2,000 people.

The site was first identified in 2022 by the Cyber Defence Alliance, a small team of investigators funded by UK financial bodies to infiltrate criminal networks on the dark web. This investigation is an example of a new approach involving police, the National Crime Agency and banking security experts.

Police have arrested 37 suspects in the UK and abroad, including one who they believe is the site's main mastermind, and contacted 25,000 UK victims. Notably, the arrests include a significant number of students with no particular technology skills – highlighting the recent growth in 'cybercrime-as-a-service.'

According to DI Oliver Richter, just five years ago a cybercriminal would need technical skills like being able to code – not anymore: "a lot of these users, they are younger, they're at university, they are very likely to go on to perhaps perfectly legitimate careers. They see this, because it is so easy to do, as something that is anonymous."

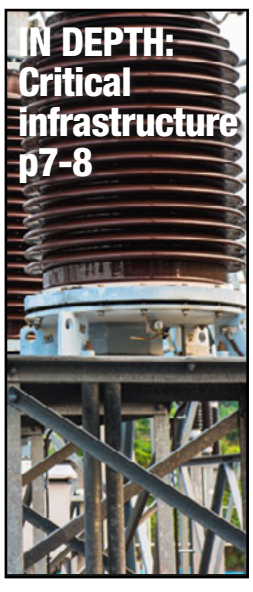
"This is a typical example of professionalisation within the cybercrime industry," explains Andrew Rose, chief security officer at SoSafe. "LabHost provides a real-life threat in action, acting as a platform which could enable almost anyone to conduct specialised phishing attacks. This is also a reminder that cybercriminals are not only in Russia and North Korea, but are operating everywhere and businesses must be vigilant."

"As tools become more easily accessible to commit fraud along with the promise of being able to remain anonymous, it is clear why so many people are trying out these techniques on offer," agrees Jake Moore, global cybersecurity advisor, ESET. "Crime-as-a-service is a very lucrative way that criminals have found to share their techniques with others willing to pay and these services are becoming more widespread on underground forums and dark websites."

Rose reports that phishing is still one of the most successful hacking tactics, targeting the human factor to enter technical systems and wreak havoc.

"Attacks of this kind psychologically trick users into clicking suspicious links, attachments or lead them to fake landing pages to steal data. 83% of security leaders in the UK rate phishing and the emotional manipulation of employees as a major security risk for their organisation," warns Rose.

The solutions to such attacks for the UK's enterprises include continued vigilance, ongoing training, and maintaining updated, secure systems. As evidenced by the April cyber-attack on Carpetright - which lost the ability to process online and in-store payments for almost a week - the threats are real, near-constant, and a significant danger to operations. ■



Royal Jersey Laundry goes high tech with RFID

Royal Jersey Laundry has introduced a new tracking feature of HID's linen management platform at each of its 5-star hotel customer sites to guarantee that drivers drop off and collect precise linen stock and that costly errors are avoided.

This new feature replaces a paper-based system used by drivers for the management of cages filled with clean/soiled linen delivered/collected at customer sites. It now provides detailed end-to-end tracking of linen cages across multiple customer locations throughout the whole cycle of washing, packing, delivery, and collection — a complex process given 550,000 pieces are laundered each week.

Royal Jersey Laundry installed a real-time linen inventory management system from HID combining LinTRAK RFID tags, a full set of RFID equipment including table-top and conveyor-belt scanners, one RFID portal and one cabin scanning unit, and cloud-based Acuity software. The discrete LinTRAK tags are sewn into linen items by laundry staff or by linen manufacturers at the production process. Some hotels also use LinTRAK tags to manage staff uniforms and restaurant linens such as napkins and tablecloths. Once cleaned, the linen is packed into cages, and scanned in seconds through HID's RFID cabin station. Items are automatically counted, with delivery notes generated including billing information. HID's Acuity software integrates with the laundry's Sage accounting software to generate invoices.

The implementation of HID LinTRAK textile tags, RFID stations and the Acuity software platform has radically changed how Royal Jersey Laundry operates, delivering a better use of human resources; fast return on investment; better visibility of stock levels; improved responsiveness and customer satisfaction; increased security of expensive linen assets; and enhanced reliability and productivity. ■

Vantage Data Centres enters Ireland with data centre campus

Vantage Data Centers has announced its entrance into the Irish market with the development of a multi-phase data centre campus (DUB1).

The company will invest more than €1 billion over multiple phases to support the construction and delivery of the campus in one of the largest data center markets in Europe. The first two phases consist of 52MW of IT capacity, with the first phase expected to be operational in late 2024. Upon completion, DUB1 will mark Vantage's 14th EMEA campus in a growing regional portfolio that spans seven countries.

The company's flagship Ireland campus will be located 15km from the Dublin City Center in Profile Park, Grange Castle, an area known for its data centers. The 405,000 square foot campus will consist of one 32MW facility and one 20MW facility and has available land and power to add a third facility in the future. The highly efficient campus is being built in alignment with Vantage's sustainable blueprint to deliver an industry-leading annualised Power Usage Effectiveness (PUE) of 1.2 using virtually no water for cooling.

Vantage Data Centers is committed to achieving net zero carbon emissions by 2030 and drives emission reductions using renewable energy and sustainable fuel alternatives across its value chain. This aligns with Ireland's climate action plans and with the environmental commitments of the company's key customers.

The DUB1 campus will include an on-site 100MVA multi-fuel generation plant capable of running a combination of fuels, primarily hydrotreated vegetable oil (HVO), a renewable fuel, and gas fed by Gas Networks Ireland. Given the temporary power constraints in Dublin, this on-site generation plant will support current capacity constraints by alleviating pressure on energy demand from the grid while achieving optimal efficiency and power output. The generation plant is also capable of funneling power back to the grid, further supporting power availability in the Dublin area. In addition, Vantage plans to deploy HVO in place of conventional diesel fuel throughout its fleet of back-up generators and is working to obtain corporate power purchase agreements (CPPAs) for green energy, such as biomethane from local providers. Currently, the company is leveraging HVO for 99% of its fuel requirements during the construction phase.

"The South Dublin Chamber warmly welcomes the confidence shown in our area through the €1 billion investment by Vantage Data Centers," said Peter Byrne, CEO, South Dublin Chamber. "Vantage Data Centers will not only be contributing to local employment and taxation but will be ensuring the safety of our data and future-proofing business for years to come with this major investment in technology."

"With Dublin being one of the biggest data center markets in the world, this expansion further solidifies Vantage's role at the forefront of the digital infrastructure revolution and signifies the start of a strong partnership with local officials and the community," said David Howson, president, EMEA at Vantage Data Centers. "Throughout this development, there will be a significant positive economic impact to the community as we employ more than 1,100 individuals during peak construction and create approximately 165 jobs to operate the campus. Vantage is committed to being a good neighbor where we build and operate data centers, and we are eager to continue working with community organisations such as Round Tower GAA Club, Newcastle Tidy Towns, St. Francis Football Club, Ballyboden St. Enda's GAA, St. Ronan's National School in Deansrath and others." ■

West Midlands Local Authority picks Absoft for SAP S/4HANA Public Cloud implementation

A west Midlands local authority has awarded Absoft the contract for its SAP S/4HANA implementation. The landmark partnership marks the first SAP Public Cloud implementation within a UK local authority.

Absoft won the contract following an internal ERP evaluation of the council in April 2023. And with the impending contract renewal for its finance system by the end of 2024, the council sought a new ERP solution through a tender process. After selecting SAP as its preferred ERP provider, the council extended the tender process to its partner network, leading to Absoft's success with a tailored package outlining a seamless cloud migration strategy.

The upcoming SAP S/4HANA Public Cloud implementation, scheduled to go live in December 2024, encompasses SAP SuccessFactors, and SAP Analytics Cloud. By integrating these products from the SAP suite and leveraging continuous innovation by SAP, the council aims to make data driven decisions that will result in cost savings across the organisation. This means that the local authority will be able to be more efficient with a single source of accurate and up-to-date information with cloud-based ERP solutions, automating and streamlining processes. With intuitive analytics, the public sector organisation will be able to forecast and plan for changes in business rates, council tax rates, headcount, or inflation.

Local authorities throughout the UK are facing growing pressures to accelerate their digital transformation programmes and budgetary demands are making it imperative to explore the power of technology to automate processes, improve efficiency, and enable effective service delivery at a time of endemic skills shortages. The benefits of digital transformation are clear. Not only are the cloud-based ERP systems incredibly functionally rich and intuitive, but the supporting tools are designed to ensure a local authority can get the best out of the system from day one.

"Absoft knows the public sector industry through and through, and we are very excited about the scale of this SAP S/4HANA implementation. Our services will ultimately enable the council to cut costs, improve efficiencies, and streamline their current processes. As a trusted advisor, we operate as an extension of our clients' businesses, and our dedicated team is committed to providing high quality support," said Don Valentine, commercial director, Absoft. "The contract for the Council is the first public cloud implementation into a local authority in the UK, a significant win for SAP and Absoft alike. We're thrilled to support the council's digital transformation, and we look forward to seeing what the future holds." ■

EDITORIAL:
Editor: Amy Saunders
amys@kadiumpublishing.com
Designer: Ian Curtis
Sub-editor: Gerry Moynihan
Contributors: Mark Grindey, Joe Sheehan, Simeon Tassev, Steven Carlini, Richard Brandon, VimalRaj Sampathkumar, Jim Liddle, Khuong Quan

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

Foundational technology skills named critical need for enterprise

Pluralsight's 2024 Technical Skills Report, which explores how organisations can leverage technology to drive business value in a world where budgets and headcount are decreasing and technology is evolving at a rapid pace, finds that foundational technology skills are the most critical need.

The results were unanimous across markets and career levels: cybersecurity, cloud, and software development, which are considered the most imperative tech skills to learn, are the top areas where skills gaps persist. Cybersecurity and cloud have been named the two largest skill gaps since 2021.

Thus, before prioritising skills for tech trends, an organisation needs solid foundational skills in security, cloud, and software development. 65% of respondents said cybersecurity skills were lacking most within their organisations, followed by cloud (52%) and software development (40%). Cybersecurity skills were cited as the most important to learn in the next year (63%), followed by cloud (47%), and software development (45%). Pluralsight's report found that AI/ML skills gaps are the lowest priority to address, but demand is growing. Compared to last year, 11% more technologists are interested in building AI/ML skills.

"While we know AI/ML skills are increasingly critical, we've also found that organisations have other, more immediate upskilling priorities," said Aaron Rosenmund, Pluralsight's senior director of security & GenAI skills. "Considering that the average cost of a data breach is $4.45 million and that successful cyber-attacks are continuing to exponentially increase year-over-year, it becomes clear why cybersecurity skills are top of mind for organisations."

When a skills gap is identified, organisations have two options: hire new talent or upskill current employees. Hiring is often regarded as a quick way to find top talent with the right skills, but the findings say otherwise. 66% of organisations say hiring takes longer or the same amount of time as upskilling existing talent.

"This year's report highlights the financial benefits of upskilling current workforces and how continuous learning boosts the confidence of employees and empowers them to thrive in their roles as the technology landscape continues to shift," said Will Clive, Pluralsight's chief people officer. "It's clear that investing in tailored learning paths to assess and address specific knowledge gaps can lead to significant business outcomes." ■

Malware stops Carpetright in its tracks

Carpetright was unable to process online or in-store orders for nearly a week due to a cyberattack.

Hackers targeted the company's head office, deploying malware to gain unauthorised access to systems. The malware also affected internal systems, with employees facing difficulties accessing payroll information. According to Carpetright, the attack was contained before any customer or employee data was compromised.

"The impact this attack has had on Carpetright's current orders and its future reputation has come at a very inopportune time for the retailer," said Matthew Walton, senior retail analyst at GlobalData. "Like many retailers, Carpetright has taken steps to reduce its costs recently to navigate a challenging big-ticket market and has already reportedly hired Teneo to explore possible cuts. However, this shows that whatever challenges retailers are under, they cannot afford to cut back on is cybersecurity."

The Carpetright incident serves as a stark reminder for retailers of all sizes. Robust cybersecurity measures and investments are no longer optional; they are essential for protecting business operations, customer data, and brand reputation.

"Financially motivated actors will target any organisation they think they can extract money from. You don't need to be positioned in a significant or prominent industry, you just need to have a level of cash flow and an exposed service on the internet. Attackers will see Carpetright as little more than an IP address/Host name/service that they can exploit," commented Tim West, director, threat intelligence & outreach, WithSecure. ■

Barracuda Networks: organisations struggle to implement company-wide security policies

Barracuda Networks, Inc.'s CIO report 'Leading your business through cyber risk' which explores the top governance challenges facing companies trying to manage cyber risk and boost their cyber resilience.

The findings show that many organisations find it hard to implement company-wide security policies such as authentication measures and access controls. 49% of the smaller to mid-sized companies surveyed listed this as one of their top two governance challenges. Further, just over a third of the smaller companies worry that senior management doesn't see cyberattacks as a significant risk, while the larger companies are most likely to struggle with a lack of budget (38%) and skilled professionals (35%).

Many organisations have concerns about a lack of security and control over the supply chain and visibility into third parties with access to sensitive or confidential data. Around one in 10 doesn't have an incident response plan to turn to in the event of a successful breach.

"For many businesses today, a security incident of some kind is almost inevitable," said Siroui Mushegian, CIO of Barracuda Networks. "What matters is how you prepare for, withstand, respond to, and recover from the incident. This is cyber resilience. Advanced, defense-in-depth security solutions will take you most of the way there, but success also depends on security governance — the policies and programs, leadership, and more that enable you to manage risk. When NIST updated its benchmark cybersecurity framework earlier this year, it added security governance as a strategic priority." ■

Secure I.T. Environments completes NHS DC upgrades

Secure I.T. Environments Ltd has announced the completion of data centre cooling upgrades at Royal Devon University Healthcare, NHS Foundation Trust, that will dramatically reduce energy costs, achieving ROI in under three years.

The works replace existing cooling infrastructure with three new indoor units that improve efficiency. The free cooling solution, allows the data centre to operate in a higher temperature free cooling configuration for a greater proportion of the year, taking advantage of ambient temperatures and lowering running costs.

Each unit combines direct expansion air cooling and an energy efficient FreeCool circuit, as well as including built-in compressors for the direct expansion circuit. External Hybrid Heat Rejection (HHR) units were also fitted on site. The new installation is projected to enable the data centre to achieve a PUE of 1.14, and Cooling PUE of 1.10

"The primary source of operating expenditure (OPEX) for data centres is electricity. Whilst maintaining the climate conditions within a data centre is critical, the ASHRAE TC9.9 2016 thermal guidelines now give confidence to operators that they can control the indoor temperature at higher levels," said Chris Wellfair, projects director at Secure I.T. Environments. "This combined with the efficiencies gained with new equipment will dramatically lower energy costs at RDEF and achieve a return on investment in under three years."

The installation was conducted over three phases, ensuring the data centre could remain live supporting hospital and patient services. Secure I.T. Environments was responsible for the decommissioning of existing units, installation of new equipment, including electrical works, configuration, and testing. ■

EveryCloud IT Security and Transmit Security join forces for fraud

EveryCloud IT Security has advanced an existing partnership with Transmit Security to tackle the prevailing challenges of fraud and friction in online consumer transactions.

This collaboration represents a significant stride forward in their shared commitment to enhancing security measures and delivering exceptional solutions to their clients. The partnership promises to offer businesses a comprehensive approach to security, significantly reducing the risk of data breaches and fraud.

"As Transmit Security, we're thrilled to announce the deepening of our partnership with EveryCloud. This collaboration signifies a significant advancement in our shared mission to revolutionise consumer identity and access management," said Transmit Security's VP & GM EMEA, Phil Allen. "By combining EveryCloud's expertise in IAM solutions with Transmit's identity management and fraud prevention platform, we're empowering businesses to provide the very best digital experiences to their customers. Together, we are committed to elevating cybersecurity standards whilst delivering exceptional experiences that cater to the evolving demands and expectation of customers, worldwide."

"By expanding our partnership with Transmit Security, we aim to revolutionise e-commerce security standards and empower businesses to thrive. We look forward to continuing this journey with Transmit Security as we collectively strive to elevate security standards," said Paul Richards, director of technology at EveryCloud. ■

Sepura scores Ambulance Radio Programme extension

As part of the Department of Health and Social Care (DHSC)'s commitment to delivering a first-class medical emergency service, the Ambulance Radio Programme (ARP) has extended its modernisation plans by awarding the contract to Sepura to deliver the next generation of handheld mission critical communications devices for front line paramedics.

The contract covers the supply of the new SCL3 broadband hand-portable device to Ambulance Services across England. The SCL3 hand-portable device will maintain communications on the existing Airwave TETRA network as well as encompassing the benefits of broadband data and a migration path to ESN.

Designed for mission-critical use, the SCL3 addresses the need for optimum performance even in the harshest of environments and working practices of ambulance staff. ■

Word on the web...

On-site hydrogen production for carbon-cutting energy

Joe Sheehan, technical director, i3 Solutions Group

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

Asset financing – and how to avoid getting stung by unexpected costs from hyperscalers

Mark Grindey, CEO, Zeus Cloud

To hyperscale or not to hyperscale' remains a key question for any CIO. And, while the majority of large organisations have already taken that step, for some, if not all, they question whether their IT infrastructure strategy is delivering the cost and flexibility benefits expected. At a time when capex budgets are coming under ever greater pressure, pushing CIOs even harder towards the hyperscale opex alternative, CIOs must read the small print – or pay the price.

Escalating costs

Drivers for the adoption of public cloud platforms vary, but for many larger organisations, the agility, innovation and scalability have outweighed the expected cost benefits. The ability to spin up new systems has improved time to market, accelerated digital transformation and enhanced business resilience. For CIOs, the shift away from on premise to the hyperscalers has met objectives – in the main. There is one, very notable exception: cost. While cost control may not have been the priority, it is always a factor in any IT strategic change. Few businesses expected to incur the level of 'additional' costs associated with the public cloud. And, given the on-going economic challenges, this upward trend is raising serious concerns.

"Drivers for the adoption of public cloud platforms vary, but for many larger organisations, the agility, innovation and scalability have outweighed the expected cost benefits."

The biggest problem is that, despite the perception, the price of public cloud service is not 'known.' Monthly costs are not consistent. The subscription model is just one element in a sliding scale of usage-based costs. Companies are discovering the additional fees demanded for extra security and support. They are incurring far greater storage costs, due to the tendency to charge for both storing and deleting data. Even a user inadvertently changing Active Directory settings can lead to an unexpected hike in costs.

Add in the limitations on bandwidth, the additional charges for cpu or RAM, plus the fact that if the business is using VMWare, it will be paying again based on those same usage factors. Therefore, it's these further hidden costs of the cloud that have caught many companies by surprise.

Security and latency risks

Of course, unexpected IT costs are nothing new. Big companies have deep pockets – if the public cloud is delivering the required agility and flexibility, is the higher price tag worth it? The problem is that the escalating level of security attacks on these high profile hyperscalers is also causing serious concerns, especially for organisations dependent upon 100% uptime and very low latency.

Financial services organisations cannot endure the increasing latency associated with essential additional levels of security. Key infrastructure providers, including telecommunications and utilities, are justifiably concerned about the risks associated with Distributed Denial of Service (DDoS) attacks occurring almost continuously on these organisations.

But what is the alternative? At a time of economic and geopolitical uncertainty, there is little if any desire to revert to the traditional IT finance model, however deep an organisation's pockets. Add in new compliance demands and the need to adapt to a changing marketplace, and capex projects are already oversubscribed. Further, large businesses have embraced the flexibility and agility associated with scaling up and down in line with demand. New business innovation is now predicated on the ability to accelerate IT development.

Retaining flexibility

The cloud model works on so many levels. The issue that organisations have to address is how to retain a cloud-based infrastructure without incurring unacceptable costs. Clearly, it is vital to read the small print. But it is also important to consider the alternatives. Would an on-premise private cloud option work, for example?

Using flexible financing, Service Integration & Management (SIAM) vendors can offer the agility of the cloud with the benefit of locating the kit either on premise or in a dedicated co-location centre. Unlike Managed Service Providers (MSPs), a SIAM doesn't mark up the equipment. It will simply use its market buying power to access the best prices for the kit required.

Critically, when compared head-to-head with the equivalent hyperscaler cost, this model is typically 50% cheaper. And, with simpler, transparent contracts, companies can – finally - achieve the known monthly cost model that was one of the original promises of the cloud. ■

Is API security the weak point in your cyber defence?

Simeon Tassev, MD and QSA at Galix

The Application Programming Interface (API) has, in recent years, become the primary method of communication online, from Software as a Service (SaaS) and Platform as a Service (PaaS) to mobile apps and cloud integrations.

A 2018 report estimated that 83% of internet traffic comprised API calls, and this number has grown in the years since. APIs form a bridge between various systems, which makes them immensely useful but also vulnerable to attack. They have historically been under-secured for several reasons, but the spotlight is now firmly shining on API security as an essential for businesses, particularly those that make use of online payment gateways. Without effective API security, businesses may fall victim to cybercrime while at the same time risking breaches of compliance legislation, including the latest iteration of the Payment Card Industry (PCI) Data Security Standard (DSS).

"It is critical to have the relevant controls in place to limit the data request, to have proper authentication according to business needs, and to validate the request. However, it is equally important to balance this security with usability."

You are the weakest link

One of the major reasons why APIs have become a popular method of cyberattack is because they are a link between different systems, and people tend to assume that if the systems or applications are secure, then the entire process is. However, API calls take place at various points between the systems, and if they are not secured, they can be misused.

While securing the front- and back-end remains critical, if API links are not secured, they can act as a side door that enables malicious actors to intercept data without anyone being any the wiser as to the breach. Alongside web application firewalls and other basic security protocols, it has become critical to bring in API security to analyse traffic and enforce additional controls.

A growing concern

For many years, the Open Worldwide Application Security Project (OWASP) has been working to improve the security of software, and the OWASP Top 10 has become a de facto standard, representing a broad consensus about the most critical security risks to web applications. Now, with API security increasingly a priority, the non-profit organisation also incorporates the OWASP API Security Project and produces a list of the top 10 API security risks on an annual basis. This helps organisations understand the nature of the threat, how it is evolving, and what frameworks need to be put in place to address these challenges.

API security is inherently complex, and it can be challenging to understand what a legitimate API call or request is, and what represents a malicious attack. One system may query another to confirm a username, date of birth, or other personal information, and this is a legitimate and valid call. But if that call is not effectively limited, or authenticated or controlled, a malicious actor may request a dump of a user list, and this will also be seen as a valid request.

It is critical to have the relevant controls in place to limit the data request, to have proper authentication according to business needs, and to validate the request. However, it is equally important to balance this security with usability. If you limit the number of API calls and a website is experiencing heavier than usual but legitimate traffic (for example, during a Black Friday sale), then payments cannot be processed because API calls are being blocked. By the same token, a malicious actor can use this strategy of inundating a system with API calls to create a Denial of Service (DOS) attack.

A matter of practice

The first step in effective API security is to understand what it is and how it relates to a business, as well as to create an inventory of APIs and the systems they are linked to. This is standard security practice: you cannot manage something without first being aware that it exists. Creating and maintaining API documentation is vital to this. Then you need a strategy around both application and API security, aligned with OWASP API security, business strategy, and best practice frameworks. It is also important to train developers and administrators to code securely with API security in mind, so that controls are in place from the start, which is infinitely more secure than patching them after the fact.

There are secure platforms available for monitoring the front, middle, and back of applications, including where APIs sit, and there are controls that can be implemented to improve management and control. However, API security is both critical and complex, and while there are tools available that can assist, these are only as good as their foundation.

It is essential to have a solid strategy in place, as well as a plan and a framework based on accepted best practices, and to incorporate specific requirements according to business needs, such as compliance with PCI DSS standards for any business that makes use of payment gateways, which themselves make use of API calls to function. In this landscape, it is highly beneficial to engage with a specialist security professional who will be able to help you understand what is applicable to your business and apply a framework and a solution to ensure the correct balance of security and functionality to address the threat without impacting business as usual. ■

Securing critical infrastructure

Securing critical infrastructure is a non-optional must in the modern world; however, with so many attack vectors and evolving threats, where should we even begin?

In an increasingly digital world, securing critical infrastructure – including but not limited to national defence, healthcare, emergency services, transportation systems, and utilities – is essential. The disruption of such infrastructure can ripple far beyond a single organisation to threaten public safety. But what exactly is the biggest threat to critical infrastructure today?

Availability disruption

"The biggest threat is any cyberattack that succeeds - but a highly disruptive one, particularly if it impacts services people depend on, will be the worst case," shares Piers Wilson, head of product management, Huntsman Security.

"The biggest threat to critical infrastructure in 2024 is the disruption of availability," agrees Andy Thompson, offensive research evangelist, CyberArk Labs. "Threat actors are continuously honing their skills, finding new ways to penetrate critical networks. And when they manage to do so, essential systems that are key to public health and safety - for food, water, and energy supplies for example, or for fundamental transportation, communications, and financial services - can experience major disruption. Without these services, it's near-enough impossible for society to function as normal."

According to Thompson, the attack by DarkSide back in 2021 is a perfect example of 'availability' disruption. The group carried out a ransomware attack against a large oil pipeline operator that disrupted fuel supplies and triggered panic buying and widespread gas shortages across the southeastern US. In the same month, Conti waged an attack against the Irish Health Service that impacted patient care for months, which led to healthcare providers having to cancel appointments, postpone elective surgeries and delay treatments.

"These attacks demonstrate just how vulnerable critical infrastructure is in today's digital world, and the severe consequences that cyberattacks can have on essential services," says Thompson.

There are several threats that could cause catastrophic loss of critical infrastructure, according to Duncan Swan, chief operating officer, British APCO, including bad actors; poor architecture that is increasingly prone to outages from ageing systems; where demand outstrips (cap)ability - especially at times of critical need. It's important to consider that we increasingly rely on critical infrastructure for everyday life; insufficient and/or ineffective planning of business continuity and disaster recovery scenarios where key 'what ifs' are poorly thought through.

Moreover, attacks could be orchestrated by any number of different actors, from nation states with vast resources, to lone disgruntled employees or ex-employees looking to cause chaos, to criminal gangs looking for ransomware opportunities. Each has its own goals, capabilities, and attack vectors.

Accordingly, "rather than focusing on one specific scenario, organisations operating critical infrastructure need to be prepared for any attack from any direction – and make their systems as resilient as possible," asserts Wilson.

"Many of these threats can be planned and, probably more importantly, budgeted for – with far and away the most unpredictable threat being that of

a bad actor which could take the form of cyber or physical attacks at key critical infrastructure vulnerabilities," adds Swan.

Staying one step ahead

With threats seemingly coming from all sides, how can critical infrastructure be secured, particularly in the face of increasingly sophisticated attacks?

"Staying one step ahead has to be the mantra," asserts Swan. "Meticulously planning the 'what ifs' and don't assume something cannot happen. There must be built-in capability/redundancy to be able to lose the use of one element of the infrastructure without losing everything (but also making sure that in doing so the level of complexity has not been ratcheted up to such a level that this poses additional risk). The level of proactive monitoring is key, as is the ability to mount a pre-emptive response to likely disruptions/attacks."

Most successful attacks still use tried and tested strategies against low hanging fruit. Getting the basics right, says Wilson, is critical.

"The most fundamental security mistakes are still the most likely to trip organisations up and lead to successful breaches," explains Wilson. "Patching systems, keeping up to date on threats, and good credential hygiene makes systems a much harder target. Having a way to regularly audit and automatically flag issues before they are exploited is key – not only for preventing most attacks, but for freeing up security teams' time to investigate and protect against more sophisticated approaches."

"The biggest threat is any cyberattack that succeeds - but a highly disruptive one, particularly if it impacts services people depend on, will be the worst case."

A large part of successful security is about shrinking the attack surface, removing opportunities for attackers: "for instance, when dealing with infrastructure there often isn't a need for all systems to be connected to the internet in an uncontrolled way," says Wilson. "Systems that can be protected from the wider internet should be, as this will greatly reduce attackers' options. In addition, automating the detection and resolution of 'basic' cyber threats will free up cybersecurity teams to detect and deal with the most significant threats."

The advent of modern connectivity, particularly cloud computing, IoT, hybrid working, etc., all bring in to play new opportunities for attack. Applications are often deployed in the cloud beyond the confines of the trusted enterprise network border; IoT endpoints are sometimes connected over the public internet; and remote working often results in bypassing the enterprise network, with system administrators routinely managing critical infrastructure from home.

"To secure critical infrastructure in the face of increasingly sophisticated attacks, it must be made less accessible remotely," opines Thompson. "This could involve implementing restrictions on remote login capabilities, or tightening authentication measures to ensure only a limited number of authorised individuals can remotely access these systems. Essentially, organisations need to create barriers to remote entry and reduce the number of access points. That way, you shrink the attack surface and make it more difficult for potential attackers to exploit vulnerabilities and launch cyberattacks against critical infrastructure."

The AI effect

The widespread entry of AI into the world in 2023 has shaken up government and enterprise activities significantly. The ultimate double-edged sword, enterprises are incorporating it into many levels of the network – just as bad actors are rapidly integrating it into their attacks.

"AI is having a big impact on the critical infrastructure sphere, allowing for more effective detection of malicious activity and threats – but it's no different to its impact on IT and OT," opines Thompson. "Just like organisations use AI to simulate cyberattacks, and test and enhance the security of their OT and IT systems, AI is a powerful tool to create appropriate response plans to protect critical infrastructure. More specifically, AI can be used to identify cyberattack patterns, predict threats, automate the response, and better protect the network."

"It is key to helping with detecting a change in trends; to spot inconsistencies; and to help stay one step ahead of any malicious activity. It will be at the heart of any proactive monitoring – as well as helping to best shape the necessary response and actions required," adds Swan. "AI also has a key role in helping to plan be that scenario planning and gaming; the ability to analyse and make sense of situations through big data. But it's also important to remember that the use of AI will rely on the critical infrastructure actually being available to get data feeds as well as power necessary to analyse and compute..."

Machine learning (ML) has been employed in the cybersecurity sector for years. Security Information and Event Management (SIEM) tools, often incorporating ML, effectively collect, aggregate, and analyse vast volumes of data emanating from devices, network, applications, etc.; detect anomalies, and either flag more complex threats or quarantine lower-level ones.

"However, AI is also being used by malicious actors to increase the volume and effectiveness of attacks," says Wilson. "Whether using automated bots at scale to probe networks for vulnerabilities to ransomware, or more focused attackers using deep fake technology to support advanced social engineering tactics. This means that it's not just cybersecurity teams that need to be on guard, but every employee of the organisation. With no way to anticipate each new attack vector is around the corner, the issue is less whether attacks are driven by AI or not, but whether organisations can deal with the unexpected."

Shouldering the responsibility

Securing critical infrastructure is non-optional in the modern world – and not a responsibility that lies on just one head.

"It has to be a mix of industry and government - government needs to ensure licence/operating/service conditions are clear in terms of responsibilities. And government has overall oversight of critical national infrastructure," says Swan.

Wilson believes that, ultimately, it's the operator of the facility or service that is responsible for securing critical infrastructure: "putting in place competent security teams, equipped with the right tools that help them to keep systems secure, is critical. Whether that's AI-based automation to deal with lower-level threats, or cybersecurity experts that can defend against complex nation-state level attacks."

However, Wilson agrees with Swan that "governments must play a role too due to the disruption and harm a major breach could cause; they have a vested interest in ensuring infrastructure is secure and aren't exempt from being the operators themselves. Government's role doesn't end at implementing legislation that ensures operators meet their obligations."

"Bad actors operate at high level - are well funded, often state funded, can access the latest tech (not always legally), and, just as the good actors use AI, they too will be using AI to their advantage," adds Swan. "So, we need high level government oversight – National Cyber Force as one example – with appropriate funding, checks, etc. Cutting corners is not an option given the reliance of society today on the connected networks of energy, communications and other utilities and systems key to the economy, public safety, health, and life generally."

Thompson explains that more and more, critical infrastructure operators are turning to cloud-based services to accelerate the pace of innovation and streamline operations. However, anyone with cloud access is a privileged user and a potential target for bad actors looking to exploit privileged accounts and attack critical infrastructure systems.

"Every employee with access to critical systems and networks is responsible for safeguarding their identity security and securing critical infrastructure – no matter whether they are part of the cybersecurity, operations, legal or HR team, all parties have an important role to play," concludes Thompson. ■

Piers Wilson

Duncan Swan

Andy Thompson

Sustainable networking: from data centres all the way to the edge

Steven Carlini, VP Of innovation and data centre, Schneider Electric

The UK's data centre world is an interesting place to be right now, and one facing critical pressures stemming from the need to expand to support more AI – particularly when it comes to training those in the ecosystem - and the overwhelming unmet demand for capacity. Today's need for data centre capacity is literally accelerating faster than we can build it.

There's also pressure being put on data centres for sustainability reporting. In Europe it's becoming mandatory to report environmental data, and impossible to gain new permits unless the data centres meet certain efficiency designs and utilise renewable energy. In the UK, meanwhile, data centre operators are coordinating on how to manage peak power situations.

Prioritising sustainability

Building the most sustainable facility means exploring efficiency, water use, and circularity.

There are three ways to do that: utilising the most efficient architectures; using the most efficient components; and managing the deployed facilities efficiently. But operators are also having to start recording and minimising water use, while exploring recyclability and building things in the most circular way. One of the things a lot of operators are doing is extending their IT refresh cycles from three years, some to as high as ten years.

Almost all data centre operators have either carbon neutral or net zero commitments that they're trying to meet; not just because of the regulations, but because of power supply issues. When designing a traditional data centre, there's UPS, and there's a generator backup – and management of these resources becomes a priority. The operator might wish to use these resources for demand response for peak shaving, or to harmonise the pitch, or to enhance sustainability. For example, management software enables operators to automatically charge backup batteries while running on renewable energy only, and then switch to using this stored renewable energy at times when the data centre switches to fossil fuels.

"Today's need for data centre capacity is literally accelerating faster than we can build it."

In the search for sustainability, distribution management software is going to be key for power management for utilities.

Accommodating AI

As AI applications become more integrated into business operations, and they start doing more with video inputs - HD facial recognition, traffic control, etc. – that data is going to need to be processed at a central location, and in real time.

This will drive the move to a local edge, although the rollout is going to take many years. These edge data centres will incorporate cloud applications, with one or even multiple clouds. We see that as a catalyst system driving deployment. How fast depends on how fast AI is integrated into business applications…

When it comes to deploying edge AI inference servers at scale, it's not really the size of the data centre - which some people believe must be a single rack data centre to be considered edge – it's about the central location.

Data centre design is already changing to accommodate AI. The servers are different, in fact they're very similar to high performance computing type workloads where they're just crunching as much data as possible.

With workloads like these, the servers run very close to their design capacity all the time. In a traditional data centre, you may design it to run a 12kW per rack, and normally it runs at 3kW per rack, and it spikes up occasionally. With AI workloads, if they're designed for 100kW per rack, they're going to run at 100kW per rack. Accordingly, the designs on the power and cooling systems must be accurate to support those workloads. We're seeing higher power components in a small dense area, requiring some serious cooling systems designed for that density.

Hot topics for 2024

AI is front and centre for data centres and networks this year, but sustainability is still going to be important. The coordination of the power sources and supply is another big issue, particularly in the UK.

"Building the most sustainable facility means exploring efficiency, water use, and circularity."

People are worried that AI is going to take over the world, take over jobs, and do so with dubious ethics. But realistically speaking, it's going to take a decade of capacity building before we can enable some of the applications people are worrying about today. Just look at chatbots; AI is still very young, and we can all recognise it immediately. It won't be taking over the world any time soon! ■

Sustainability – affecting real change for the IT sector

Advancing sustainability achievements in the power-guzzling IT sector is a worthy goal for sure – but how important is it to the UK's operators, and which technologies are paving the way?

Sustainability goals are increasingly having a significant impact on enterprises thanks in part to pressure from consumers and investors who are considering environmental, social, and governance (ESG) factors when making decisions. And in a world where reputation is everything, businesses must do everything possible to avoid getting caught with their pants down.

Moreover, like many world regions, the UK government has been active in implementing stricter regulations related to environmental protection and sustainability. Enterprises must comply or face penalties and the loss of their operating licenses.

"It looks like sustainability goals are significantly influencing UK enterprises, particularly as the government encourages all businesses, regardless of size, to commit to net zero," reports Andreas Nobell, development manager at TCO Development. "Over 40 of the UK's FTSE 100 companies have signed up to the United Nations Race to Zero campaign, which reflects the UK's corporate sustainability efforts. This initiative is part of a broader movement to integrate sustainable practices into business models, aiming to significantly reduce carbon footprints by 2030. It indicates a strong trend among UK enterprises towards adopting more sustainable operating models."

But not all enterprises are acting equally. While green initiatives can lead to long-term cost-savings, the upfront capex can deter smaller or cash-strapped businesses.

"At the moment, sustainability focus is concentrated in larger companies and within certain verticals – especially financial services and professional services – as smaller companies perceive being more sustainable to have a higher cost implication – so it is considered to be a luxury," says Steen Dalgas, senior cloud economist at Nutanix. "The IT industry is seeing the impact of this increased focus on sustainability as a business outcome, and we are being asked to demonstrate how our solutions can reduce carbon emissions during the vendor selection phase. Most government customers are applying a score for Social Value (which includes sustainability) of between 10-30% of the total tender scoring. We are now starting to see similar procurement criteria appearing in private sector tenders as well."

Maintaining a greener network

Designing, building, managing, and maintaining a more sustainable network is no mean feat. Whether exploring the supply chain, energy consumption, or transportation network, one of the biggest challenges is achieving comprehensive collaboration and coordination among stakeholders.

Dalgas reports that Scope 3 emissions (those consumed within the supply chain) account for the majority of emissions for most organisations. "Therefore, to reduce emissions, organisations need to be able to measure these emissions and have trust in the data. The problem in the IT industry is that these indirect emissions are often hard to quantify accurately. Greenwashing and making under-stated claims on these emissions is rife within the industry and many companies are publishing inaccurate emissions data."

Some believe that a lack of standards relating to the whole measurement process allows companies to come up with their own systems of measurement, which may be little more than guesswork.

As such, "there is a need for greater transparency of data under-pinned by standardised reporting on supply chain emissions," opines Dalgas. "At the moment, too many companies are happy just to get an answer to the supply chain emissions question and are not asking questions or testing the number they are given by the vendor. IT operations teams are lacking training on the sustainability topic and are simply viewing this as a compliance and tick box exercise without understanding the underlying business value that a sustainability first approach can offer to businesses."


Steen Dalgas


Andreas Nobell

Nobell, meanwhile, believes that the biggest challenge in maintaining a green network often revolves around balancing the need for technological innovation and infrastructure development with environmental sustainability.

"This involves investment in energy-efficient technologies, sustainable procurement practices, and managing the lifecycle of IT equipment in a way that minimises environmental impact. Additionally, ensuring that these practices are economically viable and do not impede an organisation's operational efficiency or financial stability can be challenging," says Nobell. "In the end it all comes back to one thing: as long as there is no demand for more sustainable IT networking products, a sustainable journey cannot kick off for real. When there is demand, development can kick off fast."

Making sustainability pay

Investing in more efficient, sustainable technologies often leads to lower energy consumption, which can decrease operational costs.

"However, initial investments in green technologies or infrastructure adjustments can be higher. The key is to adopt a long-term perspective, where the initial higher costs are balanced against the benefits of reduced emissions, energy savings, and potential improvements in corporate reputation and compliance with environmental regulations," says Nobell.

"At the moment, there is a market perception that reducing carbon emissions is viewed by many as an expensive luxury that requires an upfront investment. If we look at the car industry, electric cars are typically twice the price or more of their petrol equivalents," explains Dalgas. "From an IT perspective, when energy costs were cheap, owning your own data centre and running traditional on-premises servers and storage arrays was seen as the lowest cost option for running IT even though the carbon emissions impacts were high. This can be considered to be the IT equivalent of petrol cars. Public cloud (think electric cars), was perceived to be more sustainable but more costly."

However, the IT industry has recently seen increased price shocks which have disrupted the traditional IT infrastructure cost model. Energy costs have risen three or even fourfold compared with the ten-year historical average.

"Owning and operating your data centre has become much more costly in terms of capex and red tape. The complexity of owning your own data centre and infrastructure can lead you more exposed to ransomware attacks such as the recent British Library attack in October 2023, which can lead to a bill in multiple millions," shares Dalgas. "All of this has combined to make the business case for a more sustainable IT platform much more palatable."

TCO Development was part of a report from PwC on circular electronics that came out in 2023; 'Future Proofing the Electronics Industry – the case for circular business models.' The report showed that new circular models provide both better cost efficiency and reduce carbon emissions.

"PwC's analysis showed large financial gains for those daring to challenge the business models," reveals Nobell. "The most advantageous is a product-as-a-service (PaaS) model, providing a product as an ongoing service, rather than selling them as physical goods. A transition to a PaaS model would mean a reduction in operational costs for the global electronics industry by an average of 31% until 2035. In addition, the carbon dioxide impact from the industry is reduced by 15%. Without a change to circularity, the operational costs in the electronics industry are expected to increase by at least around 15% until the year 2035."

The role of HCI

One solution to meet growing sustainability pressures and emissions targets is hyperconverged infrastructure (HCI). With it, enterprises can benefit from improved resource utilisation, scalability, and reduced physical footprint.

"Customers moving from the traditional IT model with five-year-old storage arrays to the public cloud HCI model can expect an 80% or more reduction in Co2 emissions based on AWS data," reports Dalgas. "As well as the underlying architecture which eliminates the need for a storage area network (SAN) and reduces the physical footprint when compared to owning storage arrays, HCI enables IT operators to achieve higher resource utilisation."

HCI can help deliver more sustainable IT, particularly since the software defined approach avoids the need to buy extra infrastructure and uses AI to predict future capacity needs.

Nobell believes, however, that while HCI can play a role in meeting binding emissions targets, it's not the only viable alternative: "cloud computing, virtualisation, and adopting renewable energy sources also contribute to reducing emissions in IT operations. The choice between HCI and other alternatives depends on specific organisational needs, existing infrastructure, and long-term sustainability goals."

Ultimately, meeting sustainability goals will likely require a combination of strategies tailored to the specific needs and constraints of the enterprise. While HCI can play a role in optimising IT infrastructure and reducing emissions, it should be part of a broader sustainability strategy. ■

Will today's networks hold back the progress of artificial intelligence?

Richard Brandon, VP strategy at RtBrick

Artificial intelligence (AI) is all the talk recently, and adoption into daily work life is something that is taking off globally. The UK has already shown its interest in being a global leader when it comes to AI research, as it hosts the AI Safety Summit in November. In 2023 alone, we've seen a 48% increase in searches for various AI platforms in the UK.

Clearly the level of interest in AI has grown drastically recently, however before we get ahead of ourselves with AI innovations, it is important to consider the basics and remember that to achieve the required processing speeds, AI can demand a significant network capacity. For AI to realise its full potential as a valuable tool in the workplace, networks must possess the capability to dynamically adjust to various real-time situations.

"AI has the capacity to process and compare virology reports and patient symptoms from anywhere in the world, potentially detecting and tracking potential pandemics before they escalate."

Are today's networks strong enough for AI?

Think about how we currently depend on the capacity of AI to handle and assess vast volumes of data. In the realm of business, AI's remarkable processing and automation capabilities will transform into an indispensable resource, liberating us from mundane tasks and allowing us to be more imaginative and socially engaged. However, AI, as a technology, is still in its early stages.

As AI advances, its hunger for computing resources will grow. It seems we often assume that our conventional network infrastructure will also cope with this increased demand. However, the truth is that it won't, unless it undergoes its own evolution.

What is the relationship between AI and networks?

Drawing parallels between AI and networks to how the human brain manages intelligence is a great way to understand the role of networks in AI.

A common mistake is to perceive AI as being 'smarter than us,' yet we often overlook the fact that our brains are proficient at processing a similarly impressive network of cognitive, emotional, and dynamic data. Interestingly, our brain's capabilities are also constrained by the size of our neural networks. Furthermore, another crucial aspect of our intelligence lies in our capacity to receive and process new information from our environment. Our brains continuously contend with vast amounts of intricate sensory data, akin to an 'Input and Output (I/O) capacity' when considered in terms of computing.

AI is still relatively nascent as a technology, and as it matures, it will aspire to expand in both dimensions. This will require stronger, scalable networks when we consider time-critical applications.

Presently, a substantial portion of AI applications primarily revolve around learning processes, such as language acquisition, medical symptom-to-cause correlations, or the analysis of financial patterns. These tasks heavily demand 'processing and storage' capabilities but are seldom time-sensitive. They are unlikely to strain the input/output capacity, even if the computational and storage resources within the data centre or AI-cloud need to be interconnected to facilitate scalability. So, these current uses of AI are well-suited for the current state of networks.

What does the future of AI look like?

Everything takes a different turn when AI must adapt to real-time scenarios. To unlock AI's full potential, especially in critical domains like disaster recovery and emergency healthcare, network adaptability is essential.

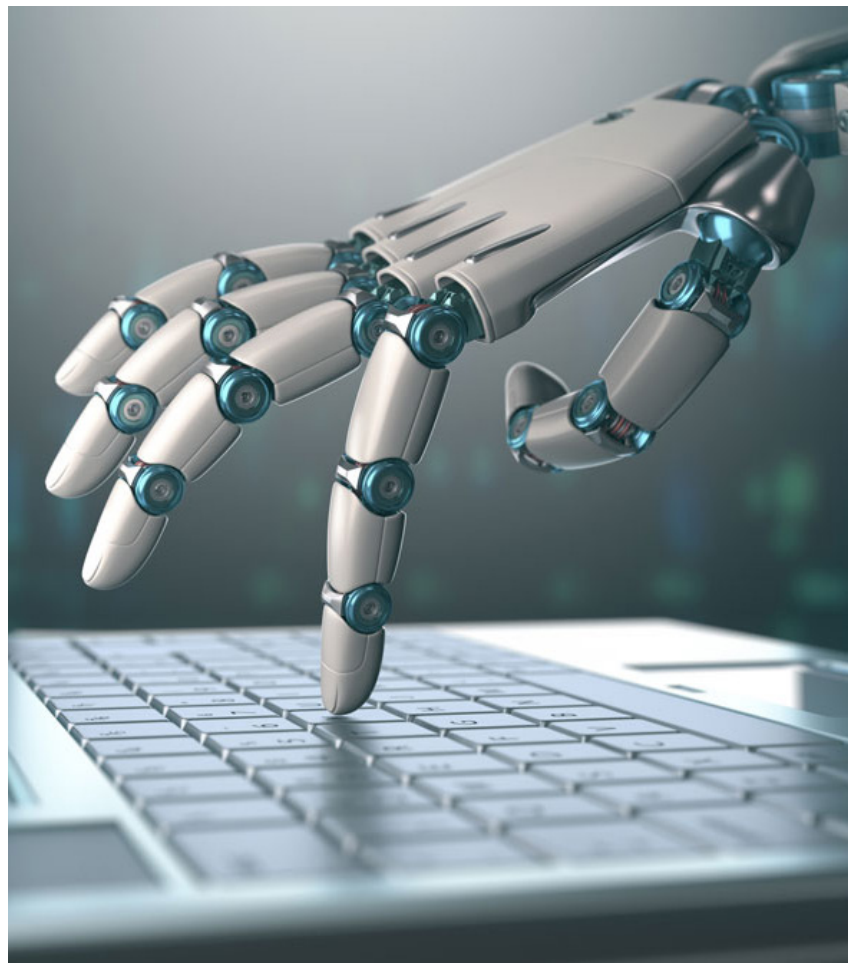
Consider these scenarios as the potential AI paired with strong networks has to better the world: AI has the capacity to process and compare virology reports and patient symptoms from anywhere in the world, potentially detecting and tracking potential pandemics before they escalate. Similarly, it could analyse seismic data to predict earthquakes or monitor cybersecurity activities, mapping vulnerabilities and forecasting potential attacks. The possibilities of AI are extensive.

What will the future implications of AI development be if we don't upgrade our networks?

For the situations listed above to become a reality, we demand a greater network capacity than that we currently possess. This means that we must make upgrades to keep up with the formidable computing capabilities of AI innovation.

It's important to note that we're not just talking about bolstering the network capacity within data centres but expanding the capacity to individual users and devices at the network's periphery – essentially, mobile, and broadband networks. However, currently these networks are ill-prepared for the impending growth of AI, and the only viable solution lies in either enhancing these networks or imposing limitations on AI's progress.

As experts continue to discuss the potential risks and benefits of AI, it remains somewhat 'up in the air' until we address the issue of our network capacity. Unless we act promptly, we risk having an incredibly advanced AI that operates far below its true potential, and that would not be smart. ■



Scottish Water goes smart on wastewater

Scottish Water provides drinking water to 2.46 million households and 150,000 business customers across Scotland. It supplies 1.34 billion litres of drinking water and removes 847 million litres of wastewater from customer properties daily, treating it before returning it to the environment.

Treating and delivering water for more than 2 million customers is an incredible task, especially in the face of rising environmental issues. Scottish Water recognised the need to move to a proactive and predictive approach that would transform how it manages the wastewater network. The operator would have real-time insights, allowing it to schedule interventions rather than just respond to events, avoiding customer inconvenience and environmental impact.

Transitioning to a smart sewer network and utilising real-time data insights would give the provider control to reduce the risk of flooding and pollution incidents with real-time event notifications. Additionally, this would help Scottish Water to align with statutory regulations from the Scottish Environmental Protection Agency (SEPA).

Overhauling the network

Eager to overhaul its wastewater network management systems to align with eco-friendly environmental mandates, Scottish Water selected Eviden, an Atos Group company, as its lead partner for the Wastewater Intelligent Network (WWIN) project.

Eviden suggested that Scottish Water maximise the value of an intelligent network by targeting areas for the most beneficial deployment. The installation required a phased roll-out of intelligent network technology and leveraging data from business information modelling to assign resources effectively.

A third-party professional services company was initially engaged for the physical installation, field validation and configuration. Eviden arranged the procurement and selection of the level and flow sensors in the pilot phase, and provided the necessary cloud integrations, system architecture, built environment and associated data processing and visualisation.

The first phase included several activities that played a pivotal role in transforming Scottish Water's wastewater network management, including establishing a strong data collection infrastructure by selecting advanced IoT sensor technology to ensure secure, uninterrupted data capture; managing the installation of IoT sensors; delivering a robust, secure and scalable data platform that receives data from the installed sensors in the network, routes and processes it, and raises necessary notifications or alarms to any abnormal behaviour; extracting data insights from the IoT platform to populate dashboards, reports and future predictive models, as well as analytics to understand and maintain normal operations; and managing day-to-day operations to ensure seamless functioning, and maintain or handle any changes.

The six-month pilot phase involved the rollout of nearly 300 sensors at four Drainage Operation Areas (DOAs), and the implementation of an IoT platform, data analytics and visualisations. Real-time insights from the sensors, dashboards and timely reports were instrumental in quicker deployments and clean-ups in those areas prone to flooding and choking, thereby reducing the number of incidents following the pilot phase.

The second phase is ongoing, due to be completed in August 2024, and will see the solution scaled up to ensure that nearly 3,000 sensors are deployed across Scotland with increased capabilities added to the platform. This includes integration with existing telemetry data and the introduction of enhanced artificial intelligence and machine learning. Eviden will also support the people and process change management that will be needed to transfer the intelligent network into business as usual.

"The number of stakeholders and complexity and scale of the existing processes in place across our organisation requires a high degree of consultation and cross-team collaboration," said Ally Gorst, product owner – WWIN Solution, Scottish Water. "Not only did Atos steer the WWIN project successfully from end-to-end but also worked closely with our teams and partners to launch the pilot phase within six short months."

Real-time visibility

Eviden's solution has proven a win for Scottish Water.

The utility provider can now detect, respond, and mitigate incidents quickly, with accurate real-time insights to proactively manage the wastewater network. The enhanced monitoring network around Scottish Water's bathing waters has proved a boon, as has the reduced environmental pollution events from the network. Moreover, with the project, Scottish Water has achieved increased compliance with Scottish Environmental Protection Agency (SEPA). In addition, the solution has afforded a decrease in environmental pollution events from the network, as well as the number of customers impacted by incidents such as flooded sewers.

"The data insights from this project have already proven instrumental in helping us detect and avoid pollution incidents in the last few months," said Gorst. "The pace of delivery has resulted in some challenges along the way, but the initiative has exceeded expectation and is delivering benefits to our customers and the environment even in its infancy."

One particularly noteworthy win came from the pilot in July 2022, when the level monitor within the drainage area showed a significant increase and raised an alarm via the dashboard, triggering a notification to the response team. There was a communication fault with the pumping station, but the control room was unaware that the pumps had failed. The platform ensured that the problem was clearly identified, and action was taken to repair the pumps and prevent any release into sensitive bathing water. ■

Critical connectivity enabled for Thames Water

Thames Water Utilities Ltd is a large private utility company responsible for the public water supply and wastewater treatment throughout most of Greater London, Luton, the Thames Valley, Surrey, Gloucestershire, north Wiltshire, far west Kent, and some other parts of England.

The operator is the UK's largest water and wastewater services company and supplies 2.6 billion litres of drinking water per day and treats 4.7 billion litres of wastewater per day.

In-building challenges

Thames Water was keen to solve mobile signal issues in the main control centre and pump building at Lane End Water Treatment Works. The energy efficient metal cladding of the building was blocking the mobile signal and health and safety for employees was a huge concern.

Signal Solutions was appointed, but prior to beginning the project, was required to achieve Achilles accreditation, a lengthy process which included a comprehensive audit as well as two additional on-site inspections of an active installation. After this was completed, Signal Solutions' engineers conducted a full site survey which included several signal tests throughout the building. The area is 700sqm over a single floor and the priority was to provide signal on all mobile phone networks for lone working and emergencies.

Following the site survey and solution design, the Signal Solutions Amplifi-Qx Analogue solution was selected. This included four CEL-FI GO G32 boosters and seven internal omni-directional antennas. With no operator licence required, the installation was completed in just two days with little disruption to Thames Water. Every Amplifi-Qx signal solution is licence exempt and meets the regulatory requirements in the UK.

Solving connectivity shortfalls

Following the installation, Signal Solutions' engineers completed a walk around the building to test the signal in various locations – comparing the boosted signal to the original signal readings.

Signal testing equipment is used to take dBm readings and compared to the pre-install readings to calculate the increase in mobile signal. A very good dBm reading will be somewhere between -70dBm and -90dBm. For 3G, all networks were recorded with very good readings: Vodafone (-67dBm), O2 (-70 dBm), EE (-72 dBm), and Three (-75 dBm). The same was true of 4G networks: Vodafone (-79 dBm), O2 (-77 dBm), EE (-79 dBm), and Three (-78 dBm).

All areas of the building now receive a consistent mobile signal, providing voice and data coverage on all networks. The facility now benefits from productivity and operational advantages of being able to use mobile devices on the move throughout the site. Health and safety concerns have been addressed now that the emergency services can be contacted.

"Network connectivity must be readily available so that contact with emergency services can be made. Signal Solutions came up with a proposed solution for a boosting system," said Phil Howe, technical coordinator (South East London Water Production), Thames Water. "It was evident that on this, Signal Solutions' very first job with Thames Water, that the engineers acted responsibly and professionally. I was impressed by their work ethic. They provided me with frequent updates and they left the site tidy on departure." ■

Digital twins don't give manufacturers the full picture

Khuong Quan, senior product manager – connectivity solutions, BICS

You've heard of a digital twin…but have you heard of a connectivity twin? There's not a single soul in the manufacturing industry who hasn't at least thought about digital twin implementation – 9 in 10 global manufacturing organisations are considering it today. The digital twin market is supposed to grow at a CAGR of roughly 30% until 207 – a similar growth rate to the overall market for IoT manufacturing, expected to reach $970 billion by 2028.

It's easy to see why. Digital twins – which create virtual replicas of systems and objects – are the answer to analysing and testing the effectiveness, efficiency, and accuracy of IoT systems and devices without affecting the real-world system. Neat, but how intuitive are these digital twin solutions, really?

The short answer? Digital twins don't give manufacturers the complete picture of potential faults and inefficiencies. In fact, without cloning their devices' connectivity, manufacturers are leaving a lot of intelligence on the table that could be used to unlock even better value out of their IoT ecosystem.

Why IoT matters in the supply chain and manufacturing

The thing about manufacturing plants is that they're immensely complex beasts. Changes in products and the processes to create them happen often, which means time and money can sometimes be flushed down the drain.

This is why over the last few years, manufacturers have been keen to leverage IoT to connect machines that can optimise that process, creating a safer, more efficient facility. They can have devices communicate with one another, sharing data to make autonomous decisions based on real-time information, or alert workers to performance and maintenance issues. Some of the popular use cases for IoT include safety monitoring, automating production line processes such as quality control, and providing more accurate data and analytics.

In the supply chain, IoT solutions can help track, manage, and deliver goods. Applications can help automate or monitor specific picking and packing processes, which brands like Amazon already make use of. They can even monitor the entire supply chain, just as Volvo has done by using IoT to track the delivery of vehicle parts across various countries.

If IoT provides the data, then digital twins are the thing that visualises and provides better visibility over the data – and there's a whole lot of data. More specifically, digital twins are quite handy for the simulation and operational phases of manufacturing products and processes. Inevitably, different batches of products have variable levels of quality – some even have defects or inefficiencies in the process of how they're made. By virtually cloning these assets, digital twins basically give manufacturers a way to get to the bottom of this by easily obtaining deeper insights and better visibility on their assets, production lines, end products, etc.

In theory, this all sounds great, but there's a lot more to IoT that needs troubleshooting than just the devices themselves. In layman's terms, any IoT application is made of three components: devices, application, and connectivity. You need the IoT devices to collect the data in the first place, the application to analyse and unlock value from the data, and finally, the connectivity to bind it all together.

It's the last bit that often gets overlooked in IoT management. The importance of connectivity cannot be understated here. Many IoT applications are developed under the assumption that there will always be a fast and persistent internet connection powering the flow of real-time data from devices. In reality, though, if you're not troubleshooting connectivity with twin technology, you're effectively blind to a sizable source of problems that may slow processes down.

Connectivity needs a digital twin, too

Unfortunately, connectivity isn't always persistent. We've seen on a bigger scale how entire factories can come to a halt during a network outage, but intermittent connectivity isn't always easily visible. Often, the connectivity issue is device-specific, or the issue might be 'poor' connectivity as opposed to 'no' connectivity.

Just imagine if your smartphone told you how much battery it had left, but not the number of bars on your signal level. Sure, you could probably open up Safari on your iPhone and manually test for an internet connection, and that would work. But if you're a manufacturer at a plant, imagine you've now got that same visibility problem for hundreds, if not more, IoT devices. You're essentially guessing and praying that those devices are connected at all times even when they might not be.

This is where enterprises in manufacturing and beyond need to evolve their thinking about digital twins into 'connectivity twins.' In practice, this means virtually cloning the SIM or eSIM of a device to access information on connectivity. The end-to-end security view you get allows faster troubleshooting and service improvement. Time is money, as they say, and the last thing any manufacturer wants is poor connectivity slowing down their time to market.

To unlock the full potential of IoT data, any enterprise in manufacturing transitioning into large-scale IoT deployment must consider how they merge device or sensor data with crucial connectivity and network data. The synergy from this would provide profound operational insights, not to mention boost the service level delivered to customers, ensuring a more connected, efficient, and intelligent IoT ecosystem.

From an IoT management perspective, enterprises often have too many disparate platforms managing different elements and producing different data sets. They might have a device management platform and a separate SIM/connectivity management solution, both hosted on the cloud.

While the emergence of digital twin platforms from hyperscale cloud providers like AWS IoT TwinMaker and Azure Digital Twins has helped with the interconnection of data sources, connectivity management has to be brought inside the device management platform. This is the missing piece to IoT.

When having twins actually reduces stress levels

On a more granular level, twinning your connectivity comes with other benefits, too. Monitoring device firmware upgrades and managing data volume aggregation would certainly be simpler, for instance. Devices with poor coverage or performance could be identified quickly. Troubleshooting disconnected devices, network ID verification, and Radio Access Technology availability would be faster. You can imagine other use cases, such as accelerating GPS signal acquisition for efficient fleet management, or predicting the remaining battery life of devices to ensure uninterrupted service. You could even quickly block connectivity in cases of suspected fraud activity.

For this future to become a reality, manufacturers may have to lean on the expertise of telco vendors. While some manufacturers and enterprises may eventually be able to develop connectivity twin solutions themselves, if the ongoing digital skills gap in the UK is anything to go by, that seems unlikely anytime soon. More likely, we'll see manufacturers collaborate with vendors offering low-code and no-code tools that streamline processes for developers building IoT apps and managing IoT data. The easier these connectivity twin solutions are to use and integrate, the more easily teams will be able to extract value from their IoT solutions.

If you want the complete picture of your IoT ecosystem, including all its bottlenecks, make connectivity another important branch to troubleshoot with digital twins. Connectivity twins aren't just about a cool technological innovation. They could be the key to a future where IoT solutions are far more intuitive, powerful, and seamlessly integrated into enterprise operations. ■

Enhancing workplace security through mobile device management solutions

VimalRaj Sampathkumar, technical head - UK & Ireland, ManageEngine

In today's fast-paced digital landscape, mobile devices have become indispensable tools. That's particularly true in the workplace, with employees even relying on their mobile devices to access apps such as WhatsApp to communicate about work.

For IT teams, keeping track of these devices and everything on them poses a cybersecurity challenge. And businesses that follow a bring your own device (BYOD) policy, where employees can access private work data and channels from their own devices, are especially vulnerable.

In this new mobile-centric world, the importance of mobile device management (MDM) solutions, from a workplace perspective, cannot be emphasised enough. These solutions are the first line of defence when it comes to ensuring mobile devices are secure and properly supported.

Implementing an MDM solution not only assists IT and security teams in enhancing security but also streamlines device management processes, boosts productivity, and ensures compliance with company policies and regulations. Some of the advantages of having an MDM solution include effectively achieving surface-level compliance and enabling remote wipe and lock. Here are three key steps to fortifying your organisation's MDM strategy:

Remote cyber monitoring

Ensuring the implementation of optimal practices and security measures for remote connections is crucial. Inadequate remote access security may enable cybercriminals to infiltrate privileged systems, leading to the potential for data breaches. By contrast, a robust secure remote access solution integrates essential tools and best practices to guarantee comprehensive cybersecurity and remote access security measures. This ensures that corporate data is not copied and accessed in an unmanaged or untrusted application.

As employees access company servers daily from various uncontrolled networks — such as cafes and co-working spaces — implementing robust security measures is imperative to protect sensitive company information. IT teams must find the right balance between giving employees privacy while controlling who can do what with their apps. Setting up strong security measures, including enforcing secure authentication, managing app permissions, monitoring device compliance, detecting unauthorized devices, and applying data loss prevention policies, will help boost your cybersecurity strategy.

Employee training as a preventive measure against cyberattacks

While employees are often seen as weak spots in cybersecurity, they can also play a big role in shaping a security-focused mindset. IT teams are vital in teaching employees to spot and handle cyberthreats effectively. An increasing number of organisations are providing comprehensive training and support to their employees, with some even sending fake phishing emails to their employees to monitor the responses. It's also important to make sure employees keep their devices fully up to date and educate them on how this can prevent malware and other attacks.

Fostering a culture of vigilance and continuous learning will empower your employees to become proactive defenders against cyberthreats, creating a stronger overall security posture within the company.

The importance of endpoint protection

To enhance security, IT teams need to focus on protecting the increasing number of devices connecting to their networks. These devices are vulnerable to attacks that can compromise security through unauthorised access.

Laptops, phones, tablets, and other endpoints frequently encounter unknown data channels when connected to a corporate network. But the risks extend beyond just the devices themselves. Using public WiFi to temporarily install apps on a phone can lead to serious consequences, potentially triggering phishing attacks or introducing malware or spyware onto the device. A single unsecured network connection is all it takes for a hacker to exploit a device's vulnerabilities.

Once compromised, these endpoints serve as easy vectors for launching attacks on the corporate network, underscoring the importance for organisations to adopt unified endpoint management practices. Organizations can implement policies such as geofencing (enabling/disabling features like microphones and cameras in certain locations), app control (allowing/disallowing apps to be installed), and kiosk modes to increase their security posture.

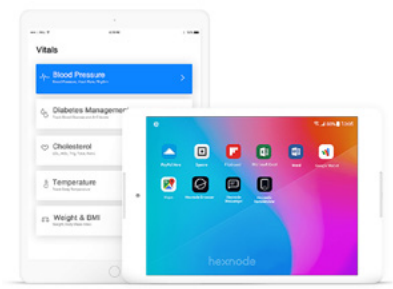
Safeguarding your organisation against cyberthreats in today's mobile-centric world requires a multi-faceted approach. By prioritising security across devices and networks, and by empowering employees with the knowledge and tools to combat cyber risks effectively, organisations can navigate the modern workplace landscape with confidence and resilience. ■

PRODUCTS

Hexnode's Unified Mobile and Desktop Management supports all major platforms – iOS, Android, Windows, macOS, tvOS, Fire OS – streamlining large scale deployments and securely distributing apps, saving IT time for enterprises of all types. Applications can be blacklisted or whitelisted, while app catalogues can be set up.

With Hexnode's web-filtering capabilities, the business can improve security by restricting inappropriate content and websites. Device configurations can be set up over the air, and features such as camera, app store and iCloud can be disabled – helping boost worker productivity.

Digital signage management can be simplified; Android devices can be seamlessly converted into full-fledged digital signages, and content can be managed and provisioned in real-time to multiple devices from a single portal. Peripheral settings like volume and screen brightness can be remotely configured.

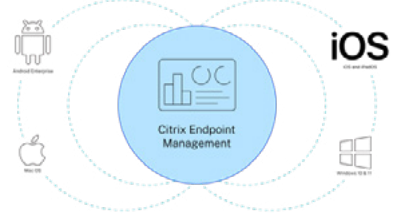


Citrix Endpoint Management is the ideal solution for customers where security and compliance are a top priority, supporting Android, Apple and Windows operating systems.

The solution includes more than 300 policies for additional security and advanced MDM compliance for context-aware security. In addition, with Citrix Endpoint Management cloud or on-premises, businesses get all the same features and can manage devices from anywhere.

The business can increase productivity while reducing support calls as Citrix maintains infrastructure, scaling, monitoring, and delivery, reducing the burden on IT and delivering updates faster. Automatic updates mean users have instant access to new features and bug fixes.

Citrix maintains a 99.9% uptime SLA, so the workforce stays connected. It also offloads upgrades and operational management tasks, reducing IT time spent on operations.



Miradore MDM enables the enterprise to gain visibility over the entire device fleet of Android, Apple, and Windows devices and manage them remotely from a single platform.

The solution allows employees to choose the devices they prefer to work with, pre-configure devices with the right settings and apps to ensure smooth onboarding, and improve work efficiency by decreasing the number of IT issues.

Devices can be kept up-to-date with centralised and automated device management, preventing human errors, and cutting down on technical issues and focus on more essential things. The enterprise can be protected against financial and reputational risks by keeping devices and data safe, while achieving faster growth with rapid device setups and a smoother device user experience.

With Miradore MDM, the IT team can view real-time device data and analytics; control and manage devices in one place; secure company data and assets; manage applications on devices; automate device enrolment and other manual tasks; and offer remote support for device users.

SOTI MobiControl's MDM software enables the enterprise to efficiently manage multiple device types like mobile rugged devices, mobile computers, handhelds, smartphones, vehicle mount computers, wearables and laptops – on any operating system.

Exclusive to SOTI MobiControl, SOTI XTreme Technology speeds up the time it takes to distribute apps and data to devices by a factor of 10. With Lockdown Mode, a mobile device can be restricted to business-critical apps to ensure productivity and stop the download of rogue apps or malware. Moreover, with geofencing, access can be granted to specific features when devices enter a location-based geofence, and removed when the devices exit.

MDM from SOTI MobiControl delivers full visibility into the status and performance of device deployments. The operator can resolve small issues before they become big problems and proactively make decisions to boost device performance based on simple things like network access. Business-critical apps can be quickly deployed for remote workers.

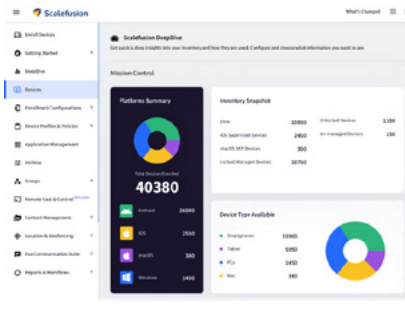
SOTI XTreme Hub communicates directly with SOTI MobiControl from distributed locations to receive data and app transfers, in place of each individual Android device. This greatly reduces the number of times new data and apps are required to be sent to large numbers of Android devices by up to 60%.

Scalefusion MDM software provides IT teams with the visibility and control required to secure, manage, and monitor any corporate-owned or employee-owned devices that access corporate data. The solution supports Android, iOS, macOS & Windows devices.

With Scalefusion, the team can manage endpoints in an enterprise environment, including smartphones and tablets to accelerate employee productivity; and to improve business visibility by managing point of sales systems and digital signage. It offers wide-range of security policies that enables IT administrators to keep data secure and prevent data leakage, and to enforce strong security policies to protect corporate data.

The Unified Mobile Device Management dashboard is powerful, intuitive, and insightful, coupled with data-driven mobile analytics that feature DeepDive, the user can get a 360-degree overview of the entire device inventory. It is also fully compliant with the General Data Protection Regulation (GDPR), SOC 2, and HIPAA standards.

With Scalefusion MDM, the team can quickly enrol devices, streamline policy enforcement, automate application management, monitor and secure device inventory, troubleshoot and fix on-field issues. The software is user-centric, crusading to help businesses generate measurable growth, improved efficiency, and reduced costs with mobility.



Please meet...

Jim Liddle, VP product, Nasuni

Who was your hero when you were growing up?

Muhammed Ali was always my big hero growing up. I'm old enough to have watched him with my father when I was young and those are still special memories. He visited London one time with his photographer, Howard Bingham, and I queued for hours for him to autograph a photo biopic of his carrier by Howard. That still has pride of place on my bookshelf!

What was your big career break?

I'm not sure there was one big break but certainly taking the jump into forming Storage Made Easy was a defining moment. Being a founder in a startup is never easy and you have to stay the course but ultimately that choice led me to where I am today and I will be forever grateful for making the jump (and I should mention that without the support of my wife Ana I probably would never have done it, so, thanks Ana!)

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

A tough one! Given how much I like my music I am going to choose one of my favourite artists, Bruce Springsteen. I'd love to hear directly from him about the early days with the E-Street band on the Jersey shore, about how he met Clarence Clemons and the other members, and what it was like back then. So, Bruce, if you are reading this... just saying!

"It's hard to imagine a non-connected world now and certainly many of the millennials won't. We can argue about its merits, but it has had a huge impact on society and the way we live."

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

I could not tell you who this was from, but I was doing a tour of Menlo Park trying to raise money for Storage Made Easy and one of the VCs gave me some advice that always stayed with me. It was: 'You will hear many reasons why startups fail: ran out of money; founder disagreements; too early in the market; burnt out etc. But let me tell you, startups fail because people give up. Pure and simple. Those that are successful find a way.'

That always stuck with me and when times were tough - as they always are at some point when you are running a startup - I always remembered that advice and it gave me the fire to double down.

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

I probably gave it away with a previous answer! It would be something to do with reporting and journalism, perhaps a field correspondent in which I would attempt to provide a balanced objective view on world news.

The Rolling Stones or the Beatles?

Oh, that is actually quite tough as I love both bands, but being a bit of a heavy rock fiend, I would have to go with the Rolling Stones. Sympathy for the Devil is one of my favourite all time tracks.

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

I actually wanted to be a journalist. For years from when I was younger that was what I wanted to be. I remember being very young and being bought a typewriter that I learned how to use and then at school I even took typing classes to learn how to speed type. I used to write short stories and enter competitions regularly, and then, somewhere along the way, I received my first piece of technology, a ZX81, and from then on, I was hooked. I moved onto a dragon-32, then a VIC-20 and then a Commodore 64, and the rest, as they say, is history!

Where would you live if money was no object?

Ibiza. My wife, Ana, is of Spanish descent and she lived there for a number of years. We visited recently and I fell in love with the island, so if money was no object, I would have a really nice villa there!

What's the greatest technological advancement in your lifetime?

Again, that is really difficult to pick just one. I think given the industry I am in and how it has affected and shaped my life, I would have to go with the internet. It's hard to imagine a non-connected world now and certainly many of the millennials won't. We can argue about its merits, but it has had a huge impact on society and the way we live. ■