

INSIDE TRACK

INNOVATIVE INSIGHTS FOR BUSINESS LEADERS

VOLUME 7, ISSUE 01

Top five networking challenges facing IT managers.

Navigating the growing
complexity of networking.

Page 10

**Supply chain cyber
resilience: why now is
the time to act.**

Page 14

**Why shadow IT is the
silent threat behind AI
adoption.**

Inside this issue...



Welcome to the latest edition of Inside Track.

Each time we publish this magazine, I am reminded of the privilege we have in working so closely with organisations across the UK. The insights, real stories and guidance we share here come directly from the conversations we have every day with leaders who are navigating change, embracing innovation and striving to do right by their people and their customers. Our role is to help bring clarity, confidence and a sense of possibility to an increasingly complex digital world, and that remains the spirit behind this edition.

This issue explores the challenges that are shaping the decisions leaders are making right now. We look at the quiet but very real risks of shadow IT in an AI-driven world, the growing pressures on modern networks and the evolving needs of sectors such as automotive, legal, logistics and property. You will also find stories from customers who are modernising their infrastructure, strengthening cyber resilience and building the foundations needed for strong performance and long-term progress.

One message shines through: the essentials truly matter. Secure, scalable and well-designed networks form the backbone of modern operations, supported by smart, intuitive collaboration tools that help people work effortlessly together. Cyber security must look ahead, not simply react, and cloud and connectivity strategies need to support both the present and the future. These

are far more than technical considerations. They are the foundations of resilience, growth and confidence. At Bistech, doing things properly is more than a value; it is a commitment that runs through every partnership, every design decision and every project our teams deliver.

Although technology continues to move at pace, our commitment to supporting you does not change. Whether you are exploring the opportunities of AI, planning a new phase of transformation or simply looking to understand where risks or performance gaps may lie, our people are here to help with honest guidance, grounded expertise and a genuine desire to see your organisation thrive.

If anything in this edition prompts you to think about how your own network is performing, I encourage you to take a look at the complimentary Network Health Check featured on the back cover. It is a simple, no-pressure way to gain a clearer view of your infrastructure today and the steps you can take to strengthen it for tomorrow.

I hope you find this edition both informative and inspiring. And as always, if a conversation would be helpful, we would be delighted to have one.

Warm regards

Jocelyn Brown
Chief Executive Officer, Bistech

“Our people are at the heart of our business — they truly are what sets us apart.”

Jocelyn Brown
Chief Executive Officer, Bistech

Contents.



4 Top five networking challenges facing IT managers in 2026.



14 Why shadow IT is the silent threat behind AI adoption.



6 Unified networking solution powers performance at premium dealership.



16 A new lease of life for the Shanly Group.



8 Why one in three motor dealership groups choose us.



18 Five signs it's time to switch to a person-centric network.



10 Supply chain cyber resilience: why now is the time to act.



20 Proactive security services protect architectural firm from emerging cyber threats.



12 Serving up a smarter customer experience.



22 Law firms are making their networks AI ready: Starting with managed SD-WAN.

Top five networking challenges facing IT managers in 2026.

By Chris Thomas

Navigating the growing complexity of networking challenges

As digital transformation accelerates, IT managers are facing increasingly complex networking challenges in maintaining secure, efficient, and reliable networks. These challenges, while not new, continue to intensify with the demands of hybrid work, the rise of cloud-hosted services, and evolving security requirements. Networks are no longer just infrastructure; they're the backbone of business operations, and being able to manage them effectively is critical for success.

In this article, we'll look at the top networking challenges IT managers are up against in 2026 and outline actionable strategies you can take to address them.

1. Providing a consistent user experience

Reliable connectivity and strong performance are important for any setup, but they're especially crucial in hybrid environments, where people move between the office and remote work. Traditional networks often struggle to keep up with distributed teams, leading to bandwidth overload, latency, and an inconsistent user experience. And all of these can have a detrimental knock-on effect impacting the experience customers receive.

On top of this, the shift towards cloud-hosted services has further decentralised network operations, increasing complexity and the need for cloud-level security that offers both control and visibility.

As gigabit-speed home broadband becomes the norm, companies need to invest in business-grade connectivity with an SLA that ensures the performance, reliability, and security that users now expect.

Secure Access Service Edge (SASE) solutions are designed for cloud and hybrid environments, bringing together SD-WAN, secure remote access, and centralised policy enforcement in a single, streamlined platform. This approach gives users secure, high-speed access to their applications and files from anywhere, backed by robust security and enterprise-grade service guarantees.

2. Adopting a modern security approach

As businesses move towards hybrid work and decentralised data storage, traditional methods designed for centralised networks are no longer enough. They must adopt an approach that provides consistent protection no matter where users are, not just in the office.

Zero Trust Network Access (ZTNA) offers a solution by enforcing the same controls across all access points, whether at home, in the office, or at a remote site. It operates on the principle that no device or user is trusted by default, and verifies identity, location, and behaviour before each session. Access is then granted only to the specific applications needed for the task at hand. With built-in encrypted connectivity, ZTNA ensures that all remote devices and users are treated with the same level of scrutiny, maximising security.

3. Managing resources effectively

Businesses are more dependent on technology than ever, and IT managers are under pressure to modernise their networks while managing limited budgets and overstretched teams. Finding the right balance between innovation and operational limitations remains an ongoing challenge.

A phased approach to innovation allows businesses to scale gradually while maintaining cost efficiency. Flexible licensing models, such as those offered with SD-WAN, allow businesses to scale their technology stack without overextending budgets. The solution's centralised network controls also make it easier for IT teams to manage remote and hybrid networks, freeing IT resource to dedicate time to further modernisation efforts.

4. Improving monitoring and visibility

Traditional network monitoring methods often fail to provide a comprehensive view of modern hybrid networks. As businesses adopt cloud-hosted services and SaaS applications, IT teams require enhanced observability tools to monitor the entire user experience.

Modern observability tools go beyond appliance monitoring to encompass SaaS application performance and endpoint activity. For example, centralised management platforms like Meraki and Fortinet stack solutions provide visibility across LAN, WAN, wireless, and application layers within a single ecosystem. This lets IT teams quickly identify and resolve performance issues, increase the company's security posture, and improve policy implementation, improving the efficiency and quality of network management and maintenance.

5. Adopting new technologies

In an era of digital innovation, IT teams contending with traditional, static networking solutions are unable to build agility and flexibility into their IT infrastructure to adopt new technologies. This hinders overall business productivity and performance.

Businesses looking to meet the changing needs of consumers and adopt new technologies must take a dynamic, flexible, and secure cloud-centric approach to networking challenges. With the ability to analyse real-time traffic, add or remove network connections and centralise network management, SD-WAN is the first step to adopting a SASE architecture, putting IT teams on a journey to optimum agility.

Empowering IT managers of the future

While the challenges of 2026 may seem daunting, they can be surmounted with the right tools and strategies. By taking a proactive approach to security, performance monitoring, and network scalability, businesses can benefit from seamless operations and adaptability in an ever-changing IT landscape.

At Bistech, we provide tailored connectivity solutions for businesses of all kinds. From SD-WAN and ZTNA to advanced observability tools and cloud-level security, we can provide your IT department with the flexibility and visibility needed to stay ahead.

Unified networking solution powers performance at premium dealership.

By Sally Bailey

When Chris Gensmantel joined LSH Auto in 2022, he wanted to build a stable IT infrastructure to support the dealership's appetite to embrace new technologies.

Their existing network was costly and slow to deploy, with recurring problems around latency and reliability. Following a thorough evaluation of the market, and impressed with their technical expertise and pedigree within the automotive industry, LSH selected Bistech.

The positive impact of the Bistech SD-WAN with a single vendor ecosystem was soon realised. Utilising the full Meraki stack, the single pane of glass solution allowed LSH to see all their products in one place, providing the ability to easily diagnose problems and find solutions in partnership with Bistech. This enhanced network visibility and ease of management has enabled Chris and his team to focus on more strategic IT projects.

The wider business has gained consistent and reliable connectivity, transforming operations. LSH's workshops were among the first to see the result, with network speed increasing tenfold, meaning cars could be more efficiently diagnosed and returned to customers on schedule. Another key improvement has been the rationalisation of kit, supporting LSH's commitment to environmental responsibility. Chris estimates the annual energy saving to be well in excess of ten thousand pounds.

Alongside the business benefits, the partnership with Bistech provides Chris, as CIO, with the day-to-day confidence that he can depend on Bistech to support LSH long into the future.



LSH AUTO

“ I love that it's a two way street. Bistech is attentive, innovative, and always looks to the future. ”

Chris Gensmantel
Chief Information Officer

Why one in three motor dealership groups choose us.

By Chris Thomas

The automotive industry is evolving at extraordinary speed. Through all this change, one thing has become increasingly clear: resilient, secure and high-performance technology infrastructure is no longer a nice-to-have. It's mission critical.

That's why we're incredibly proud that one in three of the AM-Online Top 100 motor dealership groups trust Bistech to deliver the services that underpin their operations. A milestone built not on marketing claims, but on decades of technical depth, industry understanding and doing things properly.

A partnership built on purpose, not products

For over 20 years, we've worked alongside dealerships, manufacturers and multi-brand groups – not simply as a technology provider, but as a strategic partner.

Across that journey, we've seen the pressures on dealerships grow:

- Rising volumes of digital customer interactions
- Growing cyber security risks
- Increasing complexity around dealer standards compliance
- The need for seamless connectivity across expanding networks
- Greater reliance on cloud applications and integrated systems
- Site flexibility to support brand changes and group mergers and acquisitions

As a result, our approach has always been the same. We listen first, design carefully, deliver flawlessly, and support without compromise – it is the same approach we have taken with **Snows Motor Group**.

That philosophy has enabled us to build tailored, resilient and scalable solutions that directly address the challenges their dealerships face today and the ones they have yet to come.

Trusted not just by motor dealership groups, but by manufacturers

Alongside our work with major motor groups, we're also proud to be trusted by two global automotive manufacturers, **Toyota** and **Volvo**, delivering the critical network infrastructure that powers their UK operations.

This depth of responsibility reflects what we hear consistently from our automotive partners: they value our technical expertise, our reliability, and our commitment to getting things right, every time.

High-performance managed network services

At the heart of our automotive success is our managed network portfolio – ensuring that dealerships, workshops, contact centres and remote operations stay connected, secure and performing at their best. Our work with **LSH Auto** is a great example of this in action.

Furthermore, from nationwide SD-WAN rollouts to modernising Unified Comms and Contact Centre platforms, our services give groups the confidence to operate efficiently in an increasingly digital world. And with our **“World Class” NPS** ratings across both support and project delivery, customers know they're in safe hands from day one.

As we move through 2026, our focus is clear:

- Continuing to deliver secure, high-performance managed network services at scale
- Sharing insights, expertise and learning opportunities with the industry
- Helping dealerships turn technological potential into operational value
- Strengthening our position as the automotive sector's trusted technology partner

Most importantly, we'll continue doing what has always set us apart: combining deep technical understanding with genuine partnership.

Driving automotive forward, together

Reaching the point where one in three motor dealership groups use our services is an achievement we're immensely proud of. But it's also a reminder of the responsibility we carry – and one we're committed to honouring with the same dedication, expertise and collaboration that has defined our journey so far.

Here's to another year of progress, partnership and pushing boundaries across the automotive sector.

“ The automotive industry is evolving at extraordinary speed. ”

Chris Thomas
Network and UC Practice Lead, Bistech

Supply chain cyber resilience: why now is the time to act.

By Andy Allison

The National Cyber Security Centre's Annual Review 2025 has made one thing clear – cyber risk is now a board-level issue.

With threats rising and the cost of inaction growing, organisations must embed cyber resilience into their digital strategy.

The report's findings are unequivocal. Over the past year, the UK has seen a 50% rise in highly significant cyber incidents for the third consecutive year. These attacks are no longer just IT issues, they disrupt operations, damage reputations, and threaten economic security across every sector.

Cyber criminals and hostile states are targeting supply chains, critical infrastructure, and organisations of all sizes. The cost of inaction is rising, and the window for preparation is narrowing.

“All business leaders need to take responsibility for their organisation's cyber resilience.”

Richard Horne, CEO, NCSC (Annual Review 2025)

Cyber threats are business threats and ransomware remains the most acute and pervasive threat. Attackers are sector-agnostic, targeting organisations based on vulnerability and likelihood to pay.

In 2024 alone, 50% of UK businesses experienced a cyber attack or breach, up from 39% just two years earlier.

This is not a trend; it's a trajectory.

The NCSC highlights that cyber attacks now have real-world impacts, from empty shelves in retail to service outages in healthcare. No sector is exempt.

50% year-on-year increase

We all need to recognise that there is a 50% year-on-year increase in 'highly significant' cyber incidents, the third consecutive annual rise. This is not showing any signs of decline.

Cyber resilience isn't just a technical challenge, it's a strategic one. The NCSC and UK Government are urging boards to take ownership, supported by the new Cyber Governance Code of Practice and free board-level training.

At Bistech, we believe that all boards should:

1. Make cyber risk a standing agenda item
2. Use NCSC guidance to translate technical risk into business risk
3. Regularly review cyber posture, not just reactively after incidents.

While also ensuring these key questions are discussed at board level:

- Are we investing in the right controls?
- Do we have visibility across our digital estate?
- Are our people empowered to act securely?

Cyber resilience in action

One of our customers, Corstorphine & Wright, a leading architectural practice, faced the challenge of securing sensitive project data while maintaining operational agility. We introduced a tailored cyber security solution aligned with their technical needs, budget, and long-term goals, which are incorporating Cyber Essentials, segmentation, and incident response planning.

Crucially, we considered the unique challenges of the architectural sector, ensuring resilience without compromising creativity or collaboration.

The power of policy and planning

In 2023, a supply chain attack involving the MOVEit file transfer app affected thousands of businesses globally. This is a stark reminder that resilience isn't just about your own systems – it's about your partners, vendors, and third-party tools.

Having clear, actionable security policies, and ensuring they're understood and lived across the organisation is essential. It's not enough to have a document on the intranet: it needs to be embedded in daily practice.

Don't wait for the breach

Cyber resilience is economic resilience. It protects your people, your data, and your reputation. The NCSC's message is clear: It's time to act.

Six practical steps to build resilience

The NCSC offers clear, actionable guidance. Here's how to get started:

1. Make cyber risk a boardroom priority

Proactive planning is essential. Boards should review cyber posture regularly and ensure cyber risk is embedded in strategy and culture.

2. Invest in foundational controls

Cyber Essentials is more than a compliance badge, it's a framework for good practice, now updated for hybrid working and cloud adoption.

3. Leverage free NCSC resources

The Cyber Assessment Framework (CAF) and Early Warning service help identify vulnerabilities before attackers do.

4. Build a positive cyber culture

Security is about people as much as technology. Empower staff to make secure decisions, report concerns, and understand their role in resilience.

5. Engineer for resilience

Go beyond prevention – test your ability to recover from disruptive attacks through regular incident exercises and resilience engineering.

6. Assure your supply chain

Only 14% of UK businesses reviewed supplier cyber risk in the past year. Use NCSC's supply chain guidance and encourage suppliers to achieve Cyber Essentials certification.

2025 cyber threats at a glance

Ransomware

Still the top threat, with attacks disrupting operations and targeting critical data.

State-backed actors

China, Russia, Iran, and North Korea are actively targeting UK organisations for espionage, disruption, and financial gain.

Supply chain attacks

Incidents like the MOVEit breach show vulnerabilities in third-party software can have global repercussions.

AI-enabled attacks

Threat actors are using AI to automate phishing, enhance reconnaissance, and accelerate vulnerability discovery.

Legacy system vulnerabilities

Outdated systems and unpatched software remain a major entry point for attackers.

Proliferation of intrusion tools

The global market for cyber intrusion products is expanding, enabling more actors to target a wider range of systems.

Critical national infrastructure under fire

Ransomware and disruptive attacks on energy, healthcare, and transport sectors have had real-world impacts.

Human factor

Social engineering and phishing remain common, exploiting gaps in cyber awareness and organisational culture.

Serving up a smarter customer experience at Creed Foodservice.

By Sally Bailey

With a five-decade legacy and a reputation for exemplary service, Creed Foodservice continues to set the standard across the UK's care, education and hospitality sectors.

As an award-winning, family-run business with three strategically located distribution centres, Creed prides itself on delivering exceptional customer experiences every day.

In 2021, the team faced a pivotal moment. Its on-premise phone system had reached end of life and no longer aligned with the organisation's growing demand for agility, resilience and smarter customer engagement. To maintain its industry-leading service levels, Creed knew it needed a futureproof voice solution and a trusted partner to guide the journey.

A strategic partnership

After a comprehensive market review, Creed selected Bistech as its strategic IT partner. The decision was driven by Bistech's consultative approach, depth of industry insight and ability to translate complex requirements into a clear, achievable roadmap.

Clare Bailey, Head of IT at Creed, recalls the moment the partnership began: "We were looking for a partner who truly understood our business. Bistech listened, guided us and helped shape a solution that supports our teams and our customers."

The right solution for the road ahead

Bistech recommended Bistech Managed Voice Solutions powered by 8x8, a cloud-based, feature rich contact centre platform designed to elevate both customer and employee experience.

The deployment included:

- advanced call handling and monitoring
- real-time analytics for deeper operational insight
- flexible remote working capability
- smoother communication flows across departments
- a scalable architecture that supports long-term growth

The solution equips Creed's teams with the tools they need to respond quickly and consistently, whether they are supporting customers, coordinating deliveries or collaborating internally.

Transforming the customer experience

Since go-live, Creed has benefited from a robust, highly resilient voice platform with maximum uptime. The contact centre solution has significantly reduced inbound support incidents, enabling the IT team to focus on enhancing business processes rather than resolving legacy system issues.

Insights from the Creed team highlight several standout improvements:

- greater transparency over call flows and customer demand
- more efficient resource planning across the business
- improved responsiveness and first-time resolution for callers
- enhanced reporting to support decision-making

Clare summarises the impact simply: "Bistech has given us a secure platform we can totally rely on."

Built for the future

The success of the initial project has strengthened the partnership further. With Bistech's support, Creed is now exploring additional API-driven integrations to streamline workflows and bring even more efficiency to its operations.

The vision is clear: a connected, collaborative environment where technology enables teams to focus on what matters most: delivering exceptional service to customers.

For Creed, it is not just about adopting new technology. It is about investing in a modern, resilient foundation that continues to evolve with the business. And with Bistech by its side, the future looks promising and full of opportunity.

“ We were looking for a partner who truly understood our business. Bistech has given us a secure platform we can totally rely on. ”

Clare Bailey
Head of IT

CREED
THE FOODSERVICE COMPANY

Why shadow IT is the silent threat behind AI adoption.

By Craig McLean

Artificial intelligence is changing the way businesses operate. Tools like ChatGPT and other large language models (LLMs) promise instant answers, faster content creation and smarter decision-making.

For organisations with remote or decentralised teams, these capabilities can feel indispensable. Yet behind the convenience lies a growing risk that many businesses underestimate: data security.

Picture a financial services firm, let's call them Parker & Wells, who have employees working across multiple locations, client visits and remote working. Keen to improve productivity, they start exploring AI. Before they can implement a secure solution, employees begin using public AI tools to speed up tasks. It seems harmless at first, until someone pastes sensitive client data into a chatbot. That information does not stay within the company. It is retained by the AI provider, creating a compliance nightmare and a reputational risk that could cost millions.

This scenario is not unique. It is the reality of shadow IT in the age of AI.

What is shadow IT and why does it matter?

Shadow IT refers to any unsanctioned or unmanaged technology used within an organisation without the knowledge of the IT department. In the past, this might have been a file-sharing app or a personal email account. Today, it is often AI tools.

Employees want to work efficiently, solve problems quickly and deliver results. Public AI platforms promise exactly that. But they are not designed with your organisation's security in mind.

Every time someone enters confidential information into a public AI model, that data can be stored, cross-referenced or even exposed outside the organisation. For Parker & Wells, who handle regulated and high-value information, the consequences could be catastrophic, with potential compliance breaches, reputational damage and loss of client trust.

Public AI vs Centralised AI: The reality check

Public AI

- ✗ Open model architecture
- ✗ Data retention risk
- ✗ Limited compliance controls
- ✗ No visibility or governance
- ✗ Potential reputational damage
- ✗ False sense of security with paid tiers

Centralised AI

- ✓ Secure environment
- ✓ Enterprise-grade compliance
- ✓ Full visibility and control
- ✓ Integrated with existing systems
- ✓ Enhanced productivity
- ✓ Futureproof approach

Why remote and decentralised teams are most at risk

Imagine Parker & Wells has teams spread remotely across five countries. Without the physical boundaries of an office, enforcing security policies becomes harder. Employees feel disconnected from central IT governance and start seeking their own solutions. This decentralisation creates blind spots, and blind spots are where breaches happen.

For organisations managing sensitive transactions, these blind spots can be devastating. A single data leak could expose confidential financial information, damage



client trust and attract regulatory scrutiny. In industries where reputation is everything, the cost of a breach goes far beyond fines. It erodes confidence, undermines relationships and can take years to repair.

Managing the misconceptions about AI tools

One of the most common questions we hear is: "If we buy the business version of ChatGPT, is our data safe?" The short answer is you need to check. These platforms still operate on public models, meaning your data can be stored and potentially used to train algorithms. While some providers offer enhanced privacy controls, they do not provide the same level of security as a fully integrated, enterprise-grade solution. For businesses that need robust protection, relying on public AI is a risk they simply cannot afford.

The smarter approach: centralised AI

So, what is the alternative? Centralised AI solutions. If Parker & Wells adopted a tool like Microsoft Copilot within a controlled environment, their businesses will unlock the benefits of AI without compromising their security. The centralised platforms will keep data inside their organisation, applying guardrails that prevent external access and reduce the risk of leaks. Whilst giving their IT team visibility and control, ensuring compliance and peace of mind.

Centralised AI does not just protect your data, it enhances productivity in ways that public tools cannot. Integrated solutions work seamlessly with your existing systems, enabling employees to access insights without leaving the secure environment of your business applications. This means faster workflows, smarter decision-making and a consistent user experience across the organisation.

How to make it simple

At Bistech, we understand that adopting AI can feel complex, and we work with hundreds of companies in the same position as Parker & Wells. That is why we make it simple. Through our Managed

“For businesses that need robust protection, relying on public AI is a risk they simply cannot afford”

Security Services we combine advanced protection with proactive monitoring, while our expertise in Microsoft technologies ensures your AI strategy is both powerful and safe. We work closely with your teams to design solutions that align with your business goals, giving you the confidence to embrace innovation without fear.

We do not just deploy technology, we help you build a framework for secure, sustainable AI adoption. From policy development to user training, we ensure every aspect of your strategy supports productivity and compliance. We ensure that your teams work smarter, your data stays secure and your business remains futureproof.

The bottom line

AI is here to stay. The question is whether Parker & Wells and companies like yours will embrace it safely. Public tools may offer convenience, but they come with risks that no organisation can ignore. By choosing a centralised, managed approach, you can harness the power of AI without compromising security. And with Bistech as your partner, the transition is seamless.

A new lease of life.

By Sally Bailey

Since its beginnings in 1969 as Michael Shanly Homes, the Shanly Group has grown into a collection of four privately owned businesses within the property sector.

Today, the Group includes Shanly Homes, an award winning housebuilder in the south east, Shanly Partnership Homes, a provider of quality shared ownership properties, Sorbon Estates, a regional commercial property owner and developer, and Shanly Foundation, the charitable arm that has donated over £25m to date.

By 2022, the Group recognised the need to optimise its technology estate. Inter-site connectivity had become overspecified for the operational needs of the business, and systems required modernisation to stay aligned with long-term strategy. Having worked with Bistech for several years, Shanly turned to its trusted partner for guidance on the best way forward.

A trusted partnership focused on value

Already established as Shanly's technology partner, Bistech was ideally placed to lead the project. The team worked closely with Shanly to understand the requirements and build a clear plan to rationalise and modernise the existing setup.

A connectivity refresh formed the first phase of the programme. Alongside this, Bistech carried out a detailed IT assessment to identify opportunities for further consolidation and cost optimisation.

Optimising spend and simplifying operations

The results of the refresh were immediate. By rightsizing the inter-site connectivity through Bistech Managed Network Services, Shanly achieved a **cost saving of more than 75%**. Further rationalisation of licensing delivered even greater financial gains, while also simplifying administration for the internal IT team.

The partnership continued to evolve. When Shanly's legacy on-premise phone system neared end of life, Bistech guided the Group through the selection of a modern alternative. The move to Bistech's managed voice solutions powered by 8x8 enabled a seamless transition to cloud based telephony with improved flexibility, reliability and scalability.

Bringing multiple services together under one partner has streamlined Shanly's setup and created a more manageable, cohesive technology environment.

Driving long-term efficiency and resilience

The partnership with Bistech now plays an integral role in Shanly's ongoing IT strategy. With greater visibility, reduced complexity and improved operational control, the Group is well positioned to support its continued growth.

They have seen great results including:

- improved cost control across core services
- simpler IT administration with fewer touchpoints
- stronger strategic alignment across systems
- a scalable foundation for future transformation

Ross summarises the value clearly: "Working with Bistech gives us the confidence we have a partner we can trust and rely on."

Prepared for what comes next

With an optimised network, a modern voice platform and clearer insight into its overall technology landscape, Shanly is equipped with a resilient setup that supports both day-to-day operations and future strategy. Through Bistech's proactive, partnership based approach, the Group continues to unlock efficiencies and create value across its businesses.

“Working with Bistech gives us the confidence we have a partner we can trust and rely on.”

Ross Marvin
Operations Director & Company Secretary



Five key considerations for choosing the right UC platform

Effective communication is vital for success in today's business landscape, with Unified Comms an essential tool in the modern workplace. However, with the vast number of platforms available, how do you know what's right for your organisation?

1. Customer experience

With customer service a key differentiator, it's probably no surprise to see it top of the list, so it's important to look for features such as call queuing, analytics and real-time monitoring to optimise customer interactions. Additionally, you should consider the ability to handle high call volumes during peak times to safeguard against long wait times and dropped calls.

2. Scalability and flexibility

As your business grows and evolves, so do its comms needs. A cloud-based UC platform (UCaaS) will scale up or down seamlessly to adapt to your changing business requirements, enabling your organisation to stay agile and responsive in a competitive marketplace.

3. Service continuity

Downtime can seriously impact business operations, resulting in lost productivity and missed opportunities. Look for solutions that offer robust infrastructure, redundancy and failover mechanisms as well as 24/7 support to minimise the risk of service disruption.

4. User experience

A user-friendly interface and intuitive design are essential for the successful adoption of UC. Your people should find it easy to navigate and use its features, as well as communicate effortlessly across different channels. A well-designed UC solution will empower your workforce and require minimal training, improving productivity and collaboration within your organisation.

5. Security

From cyber attacks to accidental deletion, keeping your data secure is increasingly challenging in today's world. You should ensure the platform implements stringent security measures including data encryption, access controls and compliance with relevant industry regulations such as GDPR or PCI-DSS. Further, by their very nature, cloud-based systems support a more holistic approach to security than their on-premise counterparts, for example, with regular automated patching one of many advantages.

Five signs it's time to switch to a person-centric network.

By Chris Thomas

The way we work today is worlds apart from how we did just ten years ago. Work now happens across multiple devices, from just about anywhere, and often outside the traditional 9-to-5, a far cry from the office-based routines of the past.

Naturally, this means business networks have had to evolve too. Traditional, location-based setups just weren't designed for today's flexible work styles, and when a network doesn't align with how a team operates, problems can surface quickly.

As a result, more and more organisations have been adopting a person-centric approach to their networks. This means that their IT infrastructure focuses on the needs, behaviours, and roles of individual users, rather than devices or physical office spaces.

If you're still relying on legacy systems, it might be time for a rethink. So, how can you tell if your current setup is falling behind?

Let's start by looking at what makes a network truly person-centric, before breaking down the five biggest signs it's time to make the switch.

What is a person-centric network?

A person-centric network is designed around the people who use it, rather than being structured around machines like servers, IP addresses, or hardware. This approach has a few key characteristics:

Identity-based access. Instead of tying access to a specific device or network, users are authenticated based on credentials like usernames, biometrics, or multi-factor authentication. Security policies move with the user, not the hardware.

Context-aware security. Access decisions take into account the full picture: who the user is, where they are, what device they're using, and what they're trying to do. This is aligned with Zero Trust principles: "never trust, always verify."

Mobility and flexibility. It supports remote work and BYOD environments, allowing people to switch between devices (like a laptop and a phone) without disrupting their flow or compromising security.

Personalised user experience. Access to data, apps, and permissions is tailored to each user's role, needs, and preferences, making the experience more efficient and intuitive.

Improved collaboration. Tools and resources are built around how people communicate and work together, rather than just how systems are technically linked.

How to tell if it's time to adopt a more person-centric network

No matter the size or focus of your organisation, there are some tell-tale signs that your network might need a more people-focused approach:

1. Your remote workforce is struggling

If your team is constantly dealing with lag, dropped connections, or unreliable access to applications while working remotely, your network architecture may be to blame.

Traditional, centralised networks send all traffic through a fixed data centre or company HQ before reaching its final destination.

That setup worked when most employees were in the office, but it creates serious bottlenecks when people are working remotely. Here's why:

- Even if someone's trying to access a cloud service like Microsoft 365, their connection still has to loop through the central network first. This detour increases latency and slows operations down.
- Bandwidth is limited in a centralised network. As more remote employees log on, the system gets congested, like too many cars trying to squeeze through a single-lane road.

- Traditional infrastructure isn't built to handle rapid growth. If your remote workforce doubles suddenly, the network might not keep up without major (and slow) upgrades.
- If the central data centre goes down (whether from hardware issues or just heavy traffic), it can disable access for everyone, no matter where they are.

A person-centric network, on the other hand, gives people direct access to the apps and data they need, wherever they are. It offers faster, more reliable connections, cuts down on latency, and delivers a smoother experience across devices and locations, making it much better suited for a dispersed workforce.

2. Security is getting harder to manage

As your business brings on more employees, contractors, devices, and cloud-based tools, your security environment naturally becomes more complex. With that complexity comes a broader, more diverse attack surface, increasing your overall threat risk.

A person-centric approach helps you manage this by making identity and continuous authorisation the foundation of your security strategy. Identity-based access controls mean that users can only access the resources they're actually authorised to use, while continuous authentication validates those identities in real time. This reduces your organisation's reliance on static passwords and makes it much harder for attackers to exploit stolen credentials.

On top of this, context-aware policies factor in elements like device health, location, behaviour, and risk level before granting access, adding another layer of protection.

3. You lack visibility

Traditional network architectures offer limited visibility into who's accessing what, from where, and how. This fragmented perspective makes it difficult to track usage patterns, identify potential threats, or stay compliant with regulations.

A person-centric network architecture changes this by linking activity directly to individual users and delivering real-time, detailed insights into their behaviour across the network. This bridges the visibility gap, letting IT and security teams detect anomalies faster, allocate resources more efficiently, and move from a reactive approach to a proactive one.

4. Onboarding and offboarding are difficult

If giving or revoking access is still a manual, time-consuming, or error-prone process, it's a sign your network isn't keeping up. These delays can slow

down onboarding and offboarding while leaving your organisation exposed to unnecessary security risks.

A person-first approach to access management helps solve this by connecting identity and access from day one. Automating the entire user lifecycle, from onboarding to role changes to offboarding, makes transitions faster and more secure. It also eases the administrative load, improves efficiency, and makes sure that everyone has the right access, when and where they need it.

5. Your network costs keep rising, without better results

If you're increasing your infrastructure spending but not seeing better performance or higher user satisfaction, you may be investing in the wrong places.

Traditional network strategies often focus on expanding hardware or increasing raw capacity, without really considering how people use the network or what they need to work effectively.

A person-centric approach does the opposite. It aligns infrastructure and resource allocation with real user behaviour, usage patterns, and how applications are actually performing. Instead of just chasing technical specs, it puts the user experience front and centre, helping IT teams invest where it matters most. This might mean shifting resources to support mission-critical apps, cutting latency for remote teams, or boosting reliability in high-traffic areas.

Network performance is directly tied to business outcomes, resulting in less money wasted on underused infrastructure, more productive users, and a stronger ROI.

Next steps

Networks should be built around people, not places or machines. If any of these red flags sound familiar, it might be time to move on from patching an outdated system and start building a network that supports how your people work today.

At Bitech, we have extensive experience designing modern, people-first networks for businesses of all sizes. We take the time to understand your requirements and design a secure, reliable, and scalable solution that fits them, setting up your business for success both now and in the future.

Proactive security services protect architectural firm from emerging cyber threats.

By Sally Bailey

Ranked 13th in the AJ100, Corstorphine & Wright is an award winning architectural practice recognised for its creative approach and cross sector expertise.

From refurbishing a century old Grade I listed landmark in Liverpool to designing cutting edge leisure destinations in central London, the practice prides itself on delivering commercial, civic and social value.

Like many organisations, the business has seen the growing risk of cyber security incidents. Recent industry figures show that fifty nine per cent of construction and engineering firms have experienced a cyber attack in the past two years. High profile incidents, including the theft of more than 5.7 TB of sensitive client and corporate data from US based CannonDesign, highlight what is at stake.

Corstorphine & Wright's IT team recognised the increasing risks. They needed stronger protection, especially around visibility into potential vulnerabilities, but with a small internal team, addressing these challenges independently was not feasible.

"We are a small team and while we are great at what we do, we needed specialists to fill the gaps we could not cover ourselves," explained Jonathan Carthy, Head of IT. The business turned to Bistech for support.

A proactive security strategy

Bistech began by reviewing Corstorphine & Wright's existing security posture to identify gaps and clarify their long term requirements. It became clear they needed a proactive approach to threat management, enhanced visibility and scalable capabilities that aligned with their compliance goals.

To meet these needs, Bistech introduced one of its trusted cyber security partners to design and deliver a tailored solution that matched the practice's technical environment, budget and growth plans. The solution also considered the unique challenges of the architectural sector, where safeguarding intellectual property and large client portfolios is essential.

The services included:

- Managed Detection and Response (MDR), a twenty four hour service that hunts for and mitigates threats before they escalate
- Security Operations Centre (SOC), providing real time monitoring, rapid incident response and forensic analysis

The rollout was smooth and straightforward, with the phased approach ensuring minimal disruption to day-to-day operations.

Reassurance and resilience, around the clock

Since adopting Bistech's managed security services, Corstorphine & Wright has seen a significant improvement in its security posture. Jonathan highlights several key benefits:

- threats are identified and responded to within minutes, reducing risk of data breaches or downtime
- the IT team has more time to focus on strategic work rather than day to day fire fighting
- the organisation's board and investors have greater confidence in the security strategy
- the practice successfully achieved 'Secure by Design' accreditation, enhancing credibility with clients

Jonathan summed up the impact simply: "Constant monitoring has given us confidence and peace of mind. It means we can focus on what really matters, moving the business forward."

Stronger trust, stronger future

The strengthened security posture has already delivered measurable value. With 24 hour protection, greater visibility and specialist expertise on hand, the practice is better equipped to safeguard sensitive data and maintain smooth operations across all offices.

By partnering with Bistech, Corstorphine & Wright now has a futureproof security foundation that supports continued innovation, reinforces client trust and protects the business from the growing risk of cyber crime.

“ We needed specialists to fill the gaps we could not cover ourselves. I can now sleep well at night, knowing our systems are secure. ”

Jonathan Carthy
Head of IT

C&W

Law firms are making their networks AI ready: starting with managed SD-WAN.

By Stephen Dodge

AI is transforming legal work. It now powers smart tech, automated drafting and cloud-based collaboration. As a result, law firms are exploring new ways to improve productivity and client service. However, one question often gets overlooked: is the network ready for it?

AI needs low latency, strong security, and consistent availability. Without these fundamentals, tools slow down, risks increase, and fee earners become frustrated. Therefore, a modern network is essential for consistent performance. This is where Bistech SD-WAN, delivered as part of our Managed Network Services, provides the foundation for success.

The challenge with traditional networks

Legacy architectures struggle with today's cloud-first world. Firms face issues such as:

- increasing data flows to and from cloud platforms
- hybrid working across locations
- AI tools needing real-time access to large datasets
- rising security expectations around sensitive materials

Older networks introduce latency and limit visibility. This affects user experience and increases risk at the very moment firms need clarity and control.

What does an AI-ready network provide?

An AI-ready network delivers security by default, with encrypted traffic, zero-trust principles and consistent policy enforcement. It intelligently routes traffic using cloud and AI optimisation, prioritising legal tools and business-critical applications.

Centralised control combines with local enforcement to enable fast, safe rollout of new tools and access policies. You also gain real-time visibility, giving clear insights into performance, usage and anomalies. Together, these capabilities create a stable, predictable environment for modern legal work.

Why a managed service makes the difference

Deploying SD-WAN is one thing; managing it well is another. With Bistech, you benefit from:

- Proactive operations: continuous monitoring and swift resolution before users feel the impact
- Structured change control: safe updates as AI tools evolve
- Integrated security: alignment with Bistech Managed Security for end-to-end protection
- Performance accountability: regular reviews focused on user experience, resilience and risk
- One accountable partner: connectivity, hardware, configuration and troubleshooting handled by one expert team

This ensures the network performs consistently, not just on day one.

The opportunity for forward-thinking legal firms

AI offers significant advantages for legal practices. The firms that thrive will be those that strengthen the network behind these tools. Bistech managed SD-WAN provides the performance, resilience and security needed to maximise value from AI investments. As an example, it supports demanding tools such as eDiscovery, document automation, and Microsoft Copilot.

Talk to a Bistech expert

Every legal firm's environment is different, so understanding your current network readiness is the first step. If your firm is exploring AI or looking to improve the performance of tools already in use, now is the ideal moment to assess your network readiness.

About Bistech.

Founded in 1988 from a passion for great engineering and even better customer service, Bistech has grown into one of the UK's most trusted technology partners.

For more than 35 years, our focus has been on delivering secure, scalable and future-ready IT that helps organisations work smarter every day.

Today, our portfolio spans managed IT services, cyber security, cloud and data platforms, connectivity and modern communications. Everything we deliver is grounded in technical depth, a consultative mindset and long-term partnership. That approach has earned the confidence of hundreds of organisations across the UK, from household names to rapidly growing enterprises.

Our industry reach is broad and proven. One in three of the AM-Online Top 100 motor dealership groups now rely on us to underpin their operations. Beyond automotive, our customers include iconic brands such as The White Company, Lakeland, Toyota, White Stuff and Mizuno, along with many others across Finance, Accountancy, Legal, Manufacturing, Supply Chain, Property, Architecture, and Retail.

Behind it all is a simple ambition: to combine exceptional expertise with outstanding service, helping our customers build resilient, high-performing businesses ready for the future.



Retail



Automotive



Legal



Finance & Accountancy



Manufacturing & Supply Chain



Property & Architecture



Are you AI ready?

**Don't let hidden network issues hold
your company back.**

If your network is not performing at its best, it could already be slowing your organisation down. A complimentary Network Health Check gives you clarity on how your network is performing and where you can improve. There is no cost, no commitment and nothing to lose. You simply gain insight, confidence and a stronger foundation for what comes next. So why wait?

Book your complimentary discovery call today:

bistech.co.uk/network-health-check/



Get in contact

01202 33 22 00

E hello@bistech.co.uk W bistech.co.uk

