Talking Tech.

IS HYBRID IT SUPPORT THE FUTURE?

THE CHALLENGES FACING IT TEAMS IN 2025

From sophisticated cyber attacks to a rise in shadow IT, IT teams face pressures from all sides.

TECH TRENDS TO GET BEHIND THIS YEAR

How many are on your radar?

Edition 01 - June 2025

We're delighted that Arc are sponsors of the first "Talking Tech" magazine, shining a light on a better way for businesses to handle their internal and external IT functions.

With 2025 already proving to be a challenging year for UK businesses, this first edition is an opportunity to give senior executives the insights that they need to adjust their IT strategy to align to a rapidly changing competitive landscape.

IT support noticeably changed post-pandemic and with tightening budgets, and radical operational change opportunities, it will continue to do so over the coming years.

As AI and automation make technology more accessible and less complex for the average worker, the role of IT teams and third-party IT partners must adapt. More so than ever, businesses need to be laser-focused on the future in order to stay prepared.

In this edition, we'll be exploring everything from how to futureproof your business with an effective, actionable IT strategy to getting to grips with Microsoft's Azure, as well as a spotlight on the AI solution taking businesses by storm, Microsoft Copilot, which showcases the value of surfacing data through AI.

Geoff Wing
CRO at Arc

Must-know IT stats

34%
of UK businesses outsource their IT support

The UK MSP market has around
11,492
active providers

Outsourced IT Support can help reduce IT costs by
25-45%

82%
of IT helpdesk customers prefer to use phone calls as their main communication channel

52%
of businesses cite simplifying and consolidating IT as a driver for outsourcing their IT

30%
of IT leaders believe outsourced IT support provides better results

Contents

Futureproofing your business' IT

With the pace at which technology advances and with significant rises across both technology and staffing costs, you could argue that taking a strategic view of your IT infrastructure and roadmap has never been more important. It ensures that you can synchronise any investment you make with your strategic business goals. For example, if you're looking to scale over a short period, having a ringfenced budget will allow you to invest in new systems, adopt and onboard new processes or fund simple everyday items such as increased licensing. If, however, there are no budgeted funds in the bank to fund these items, a business-as-usual approach will falter.

Without a strategic plan, organisations may find themselves reacting to external changes rather than proactively leveraging technology to drive innovation and growth. In essence, an IT strategy is crucial for maintaining competitiveness and supporting both business resilience and continuity planning. Failure to have a strategy in place during a time of need can be detrimental to any organisation, with businesses known to have gone from healthy to ceasing trading within a matter of months due to being unprepared for a cyber attack.

Moreover, having a strategy in place helps with wider risk management, identifying potential technological vulnerabilities and establishing protocols to mitigate them.

Defining, discussing, and refining a business strategy fosters collaborative decision-making and provides a clear business roadmap for technology investments and implementations. Your business will naturally prioritise initiatives that deliver the most value, so you can ensure optimal use of resources and avoid the pitfalls of adhoc or redundant projects.

Aligning IT strategy and business objectives

As with any business strategy, aligning back to what you're trying to achieve at an organisational level ensures that you're investing in and contributing to the future success of your organisation.
When it comes to strategy, the IT lead should be involved in creating both the IT and business strategies. Neither should be developed in isolation, as both are somewhat intertwined, and neither can achieve optimum success without input from both business and IT leaders. By aligning IT strategy to business objectives and sharing ideas and complementary views, businesses can improve efficiency, reduce costs, and enhance customer experiences.

Bringing it back to the business needs

As we've already discussed, the foundation of any robust IT strategy lies in thoroughly identifying the organisation's needs. This involves assessing current capabilities, pinpointing gaps, and anticipating future requirements. A comprehensive IT needs analysis allows businesses to determine where improvements are necessary and how technology can be leveraged to address these areas.

A detailed assessment of business needs enables business leaders to identify specific pain points and opportunities for improvement. By engaging with various stakeholders to understand their needs and expectations, you can ensure that your IT strategy is comprehensive and inclusive of different teams and requirements as well as overarching business goals.

Allocating the right resources and budget

Budget can make or break the effectiveness of any strategy. Yet many businesses fail to allocate what they truly need to meet their ambitious goals, making budget planning an afterthought rather than something calculated and agreed upon throughout. By properly considering the budget and resources needed to meet your aims, you may identify the need to increase targets, hire more staff, or prioritise specific business areas to ensure that you can adequately fund the required investment. Beyond

that, locking in budget upfront helps to focus on the return of investment, ensuring that you've got the budget you need to deliver the outcome you want.

In addition to the cost of buying and implementing technology, business leaders need to consider additional indirect costs. For example, they must consider how they will ensure that they have the necessary skills and expertise to make the most of their investments. This might mean expanding their internal headcount or appointing a third-party provider to offer resilience.

Leveraging third-party expertise

While you may be able to develop and execute an IT strategy effectively with your existing resources and capability, there are considerable benefits to working with a third party. IT support providers and independent consultants are exposed to a large number of other businesses of all shapes and sizes, which gives them a unique perspective on how other businesses are approaching their IT strategy, investment, and broader IT roadmap.

This experience enables them to pass on learnings from others - including what has and hasn't worked well, as well as how to go from where you are now to where you want to be. They're also exposed to a much wider product set, offering insights into whether specific solutions are right for your business and whether they'll enable you to achieve the ROI you're hoping for.

Lastly, working with a third party to develop a strategy enables you to build rapport and trust, testing the waters on whether you could continue to work together long-term should any additional IT support needs arise. After all, these partners provide valuable support in areas including cybersecurity, data management and cloud services, which are critical to modern business operations.

IT strategy is not a one-time thing

You can't simply just create an IT strategy and then implement it. Instead – as with any strategy – you must regularly review effectiveness against business objectives and needs as they evolve. By doing so, you can ensure that you remain synchronised as buisness priorities change, as well as protected against new and emerging threats that were not around when the strategy was designed.

Businesses need to think of technology as part and parcel of what they do, not an afterthought. Those that do will drive the greatest ROI on their investment and reap the greatest rewards.

The essential components of an IT strategy

A comprehensive IT strategy should encompass several key components:

Vision and objectives
What is it you're trying to achieve? How does this align with business objectives?

Assessment of our current state of play
How capable is your existing infrastructure in helping you achieve our goals? Where are the gaps?

Needs analysis
What are our business and individual technological needs?

Resource allocation
What resource and budget do you need to allow for? What contingencies need to be in place to ensure you stay on track?

Measuring success
What will be monitored and how will you evaluate if your strategy is working?

The true value of outsourced IT support

As of 2025, the median salary of an IT manager in the UK is £55,000. When you take into consideration wider emplyment costs – including pension and National Insurance contributions - it's no surprise more and more businesses are turning to third-party partners to provide the IT support they need.

Third-party providers provide a much broader skill set than internal teams can recruit, with plenty of experience to support with the development of IT strategy or the delivery of IT support, which can overcome limitations relating to technology choice or skill set and experience.

Additionally, they can help you to understand where your business compares to others in the same or similar markets.

Driving cost savings and financial efficiency

One of the most compelling reasons for outsourcing IT support is the potential to make substantial cost savings. According to a report by **Deloitte**, 59% of businesses leverage outsourcing to reduce overall expenses. By outsourcing, they can avoid the high costs of hiring and training in-house IT staff. Outsourcing eliminates these expenses, allowing for more efficient resource allocation.

Moreover, outsourcing IT support can significantly reduce hardware and software costs as IT service providers often have established relationships with major vendors, enabling them to secure discounts and favourable client terms, which can result in lower licensing fees and reduced costs for software and hardware upgrades.

Accessing unrivalled knowledge and skills

Working with an external IT partner brings a wealth of knowledge and experiences far beyond what you will likely have among your internal teams. IT support partners hire the very best of the best, often at an inflated cost above what you can afford to pay your teams. These highly specialist individuals bring a wealth of solution experience within their areas of expertise – for example, cyber security, networking or cloud.

Enhancing user satisfaction and improving productivity

According to a survey from **HDI**, outsourced support led to improved user satisfaction in 84% of organisations. By partnering with a third-party, businesses can ensure that their employees can access timely and efficient technical assistance, minimising downtime and enhancing overall productivity.

Outsourced IT providers often offer round-the-clock support, ensuring that technical issues are resolved quickly, regardless of the time of day. This level of responsiveness is difficult to achieve with an in-house IT team, which may be limited by regular business hours and staff availability. As a result, employees can focus on their core responsibilities without being hindered by technical difficulties.

Additionally, outsourced support can contribute to a more productive work environment by implementing proactive maintenance and monitoring practices. These practices help to identify and address potential issues before they escalate, reducing the likelihood of system failures and data breaches.

> **"Businesses no longer want a reactive IT partner - they see the value in building a strategic relationship with a trusted advisor"**
>
> **Lee Harding, Service Director at Arc**

Supporting a strategic business focus

Outsourcing IT support allows internal IT teams to utilise their knowledge of the business to drive progress development and enhancement to support the delivery of an IT strategy. Instead of being bogged down by routine maintenance and troubleshooting, in-house IT staff can dedicate their time and expertise to projects that drive innovation and competitive advantage.

A **McKinsey** report highlights that businesses that outsource IT functions can redirect 40% of their IT workforce to strategic initiatives. This shift in focus can lead to the development of new products and services, improved customer experiences, and enhanced business agility.

Measuring the value of outsourced IT support

Every business that chooses to outsource some or all of its IT functions will have its reasons for doing so – but how do you know if you made the right decision? With any new business change, thinking about what good looks like before jumping in is essential. With IT support, that might be a monetary value saved, a reduction in the time it takes to resolve an IT issue or a decrease in downtime or outages.

Example metrics

Area	Measured by	Example metrics
Cost	Comparing previous or budgeted spend against actual	£spent
User satisfaction	Subjective employee assessment	Scale of 1-0
Productivity	Output and the time it takes to complete affected tasks	No. of tasks completed
Time to complete tasks	Time freed up to focus on more value-added tasks	Minutes made available
Capacity of IT resource	Time spent doing value-added tasks	Hours logged
Strategic focus	Ability to complete more strategic tasks	Progress against strategy

AI's evolving role in the workplace

AI can be found everywhere we look in our personal lives: from the recommendations we're given when we arrange an online food delivery to the ads we're shown when we browse the internet, the ANPR cameras we pass on the motorway, and much, much more.

In work? AI is even more prevalent. Businesses are implementing AI solutions at pace, often led by user adoption first; for example, an employee learning about a new piece of kit and doing a free trial on their own accord (referred to as shadow IT) before making a business case for implementation.

Leaders are aware of the benefits AI can bring to their businesses, from automating time-consuming task to improved data accuracy. AI is helping them make more effective decisions at a quicker pace than ever before.

Of course, AI needs data in order to learn and develop; the larget the data set, the better the learning. Therefore, larger organisations with larger data sets tend to drive more value from their use of AI.

Got a problem? There's an AI solution for that

There are thousands of AI-first solutions on the market for businesses to take advantage of, and thousands more that now have AI embedded within them. The solutions that businesses have come to rely on have evolved, introducing AI features and functionality to stay relevant and prevent customer churn.

Irrespective of role, company size or even sector, there are AI solutions that can support what it is you're doing or trying to achieve. Take manufacturing, for example, whereby businesses have been using AI-powered robots to perform tasks such as assembly line work with precision and speed, reducing human error and increasing productivity.

Additionally, sector-agnostic, those in administrative roles can use AI to handle scheduling, email sorting, and document management, freeing up value time to focus on higher-value tasks.

Can everybody use AI?

On paper, AI is a valuable tool for everybody. However, AI's output is only as good as the data and information is has available. For example, a small business might not find predictive analytics as reliable or useful as a larger multi-national corporation that processes thousands or more records each day. Why? Simply, a much larger organisation is likely to process more information, which means predictive analytics can be more accurate, reliable and save more time.

In a similar vein, generative AI tools like ChatGPT, Copilot and Gemini are only as good as the prompt used. The more information you can provide AI, the better the end output.

AI architects argue that a good prompt should:

- **Be clear and specific**: Clearly state what you need help with.
- **Provide context**: Give background information or context to help it to better understand your request.
- **Ask direct questions**: Direct questions help AI tools to focus on providing the information you need.
- **Break down complex requests**: If your request is complex, break it down into smaller parts.
- **Specify the format**: If you need the information in a specific format, mention it.

Even the most experienced AI users end up following up on their original prompt, providing more context or being more specific in what they're asking.

Becoming a generative AI expert can take time!

The universal business benefits of AI

Anybody can gain from AI. However, the more time and effort you put into making AI implementation a success (for example, coaching or formal or on-the-job training), the more rewards you're reap.

Businesses implementing AI can expect to access the following benefits:

- **Time savings**: AI can process vast quantities of information at lightning speed.
- **Improved accuracy**: AI removes human error from basic reporting.
- **Real-time decision-making**: AI empowers business leaders to make informed decisions based on rapidly processed data.
- **Future-proofing**: AI can make recommendations on future budgets, resource needs or customer demand.
- **Consistent experiences**: AI supports teams by automating and streamlining mundane and complex business processes.
- **Personalisation**: AI enables personalisation at scale across the end-to-end customer lifecycle.

Everyday AI solutions

There are AI use cases for every single role, function and team. Here are just some of them – and how they can support businesses.

ChatGPT & Gemini

Both ChatGPT (Open AI) and Gemini (Google) can be used to find answers, create content and provide ideas, great for tasks such as brainstorming and content creation.

Chatbots

Chatbots enable businesses to handle general enquiries where content already exists, for example returns policies, open hours or pricing, perfect for providing customer support.

Microsoft Copilot

Microsoft's Copilot works in two ways: searching the web for content that already exists and searching your internal Microsoft environments to find organisation-specific information, such as what was discussed at a meeting or when an employee started with the business. The latter way of using Copilot is perfect for any role!

How different industries are utilising AI

Healthcare

Healthcare organisations can utilise AI within diagnostic tools and when managing patient data, as well as improving accuracy and efficiency in patient care.

Supply chain

Businesses involved in a supply chain can benefit from stock management and optimisation, preventing over-ordering, which boosts profitability and supports sustainability.

Retail

Retail businesses can use AI to analyse consumer purchasing habits, as well as stock ordering and replenishment through greater demand forecasting.

Manufacturing

Manufacturing businesses can use AI-powered robots to carry out precision-necessary functions, as well as accessing AI-driven predictive maintenance to foresee equipment failures and minimise downtime.

Education

Schools, colleges and universities can use AI to personalise learning experiences by adapting content to individual student needs, which can lead to improved educational outcomes.

Legal

The legal field benefits from AI's ability to review documents and conduct legal research more efficiently, saving time and resources.

"AI has the potential to revolutionise how even the smallest businesses operate. However, we're seeing two common trends: some businesses are diving in and making significant investments without a clear AI strategy, proper data governance or adequate end-user training, often leading to poor adoption and wasted investment. Others are hesitant to adopt AI at all, uncertain about how it fits within their environment, what it's truly capable of, or what a successful implementation strategy looks like."

Gemma Meggitt
New Business Sales Lead,
Perspicuity

Getting to grips with Microsoft Azure

The last couple of years has seen cloud computing advance at a remarkable pace. Unlike a decade ago, fewer organisations are using on-premises servers for their daily operations, with the cloud now hosting most personal and considerable professional data.

Most businesses operating partly or fully in the cloud are likely to be using Azure, AWS or Google. For years, AWS has been the frontrunner, dominating cloud computing market share globally. However, the tides are beginning to turn, with Microsoft beginning to close the gap with their land-and-expand approach from a foundation of Microsoft 365, articulating the value of integration with applications already in use and encouraging cloud migration – with a simple singular vendor approach.

Technology is expensive, and by consolidating vendors and solutions, businesses can access significant cost savings, with Microsoft's business solutions offering affordable and access step benefits at small incremental per-license costs.

What you don't know about Azure

Many consider it simply as a place to migrate existing applications or build new ones. But Microsoft Azure is much more than that. In fact, it boasts over 200 individual solutions.

Azure solutions that your businesses can implement include:

- **Azure Fabric** – breaking down business silos and providing rich, decision-ready analytics that foster a culture of innovation.
- **Azure AI Vision** – a suite of tools and services, which allow businesses to integrate advanced visual intelligence into their own applications.
- **Azure Virtual Desktop** – a full Windows experience on any device, managed centrally by your IT team or third-party partner. With AVD, you can guarantee all uses have the same secure experience irrespective of device or location.
- **Azure Backup** – Azure's answer to the automatic backup of data and applications, including those stored on-premises and in the cloud. With centralised monitoring and management, you'll never lose data again.
- **Azure Site Recovery** – complete protection in the event of an outage. Your workloads are replicated in real-time to a secondary location, allowing you to continue on business as usual around-the-clock. Supports cloud and on-premises infrastructure.
- **Azure SQL Database** – a fully managed PaaS (Platform-as-a-Service) database engine, which handles simple and complex functions – from upgrading and patching to backup and monitoring. A power database management solution.
- **Azure AI Foundry Models** - a catalog of over 11,000 AI models developed by leading AI providers and open-sources communities.

On-premises, cloud or hybrid

Which approach is right for you?

There is no easy answer and no one-size-fits-all approach to storing business data. Some choose the cloud for ease of everywhere access. Some choose on-premises because of the nature of their business operations. Others prefer a blended, hybrid cloud approach.

But no business should jump to a decision on a whim. Instead, you should consider your needs and budget, as cost is essential. Operational efficiency will be directly impacted by how and where you store your data… choose carefully.

It's important to think about where the data will reside and whether it will need to interact with other systems that may or may not be compatible with a specific approach.

The storage options available to you

Cloud

The cloud leverages the internet to store data, which can be both public or private. Public cloud storage uses third-party providers to house data on shared servers, making it cost-effective and scalable, and is always charged for operationally, which is suitable for businesses with variable storage demands. It is highly appropriate for "testing" with little up-front investment. Private cloud storage, on the other hand, is dedicated to a single organisation, offering greater security and control but at a higher cost, often with upfront charges associated. As a result, it can be more valuable for a business to transfer existing workloads rather than set up a new instance to test.

Providers of public cloud are now wrapping their services with exceptionally easy API integrations into AI capabilities (for example, number, text recognition, dictation and chatbots), which will only grow over time. This is enabling forward-thinking organisations to easily introduce AI into their existing workflows and applications.

Additionally, public cloud providers are now enabling specialist AI computing (Graphic Processing Units or GPUs) farms that can be drawn down as needed.

On-premises

Operating on-premises involves keeping data within on-site servers, enabling complete control over the service provided. This is often the least expensive long-term cost for the actual equipment, but often comes with considerable upfront costs.

Businesses maintain on-premises capability for several reasons:

- They need to tightly manage every aspect of the service they offer.
- They require very low latency for data processing.
- They already have internal staff managing infrastructure.
- They have previously paid for these services via capital.
- They need to sweat existing capital investments.

Despite benefits, on-premises services often come with greater internal staffing requirements for securing and maintaining. In the long term, they often become challenging to support fully as technology and skill sets to support become outdated.

Over a cycle (typically 5-7 years) when on-premises services reach end of life, organisations typically conduct a full review of their requirements in an attempt to measure and forecast all the above factors for a comparative perspective.

Hybrid cloud

The hybrid approach combines cloud and on-premises capabilities, offering a flexible and adaptive solution. It allows businesses to store critical data on-premises for enhanced security and use cloud storage for less sensitive information or to manage data surges.

Trying to decide which option is right for you?
Some factors to consider:

Cost - Cloud infrastructure is subscription model charged, whereas on-premises servers may require substantial initial investment and ongoing expenses.

Scalability - Cloud solutions offer easy scalability while scaling on-premises servers is complex and costly and has significant implementation costs.

Flexibility - Hybrid cloud solutions combine on-premises and cloud capabilities, offering the flexibility to perform critical activities locally, while leveraging the cloud for less critical services.

Data Accessibility - Cloud storage enables remote access, facilitating collaboration and remote work. On-premises storage requires users to be nearby.

Expertise and Resources - Cloud providers handle most maintenance, reducing the burden on in-house IT teams, whereas on-premises solutions require skilled IT personnel.

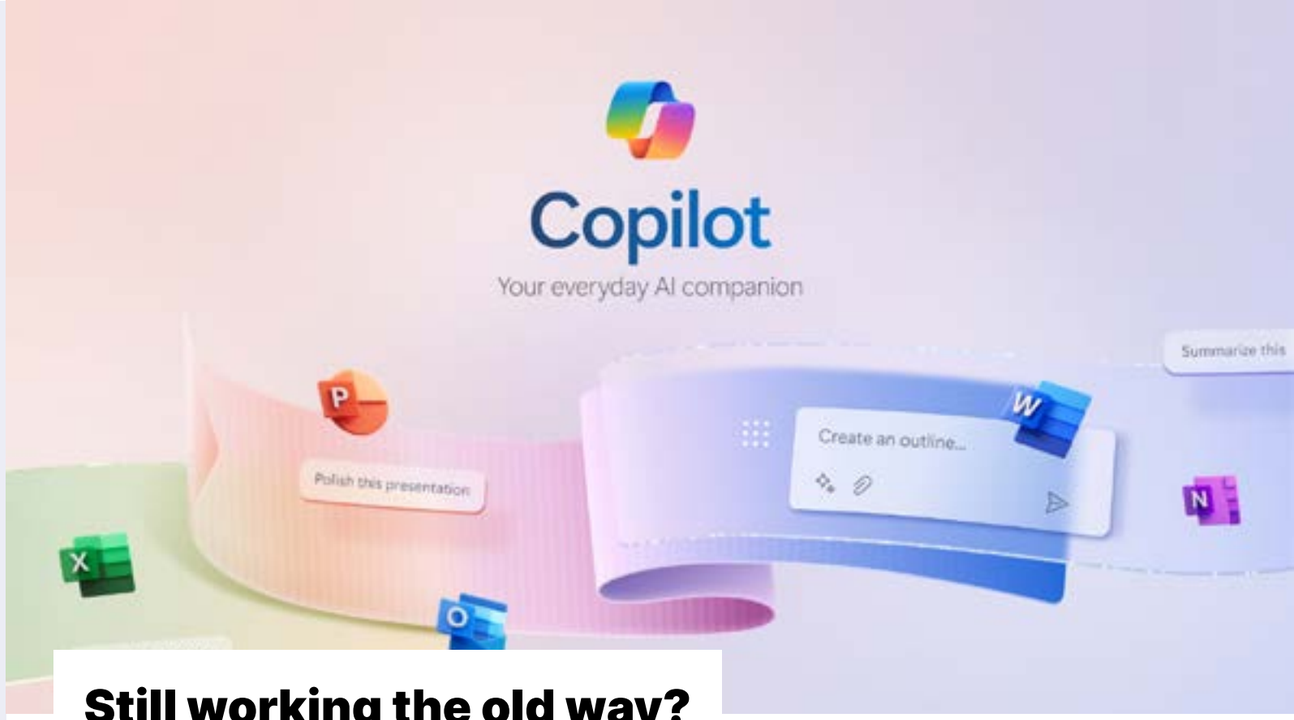
Environmental Impact - On-premises servers consume significant energy, while cloud providers often invest in energy-efficient data centres.

Data Governance - On-premises services offer more control over your data, whereas hybrid or cloud environments are bound by local data sovereignty laws.

Integrations - Cloud or hybrid cloud infrastructures allow for much easier integration with a broader set of readily available solutions.

Security and compliance considerations

On-premises servers allow businesses to implement custom security protocols, while cloud providers offer out-of-the-box security features with regular updates. Compliance with industry-specific regulations is crucial, and cloud providers often meet various regulatory standards but require thorough due diligence. Consider whether you can manage these yourself.



Still working the old way?
There's a Copilot for that.

Microsoft has changed the way organisations work with what we now know to be Microsoft Copilot – or Copilots, your "AI assistant for work".

What exactly is Microsoft Copilot?

It might be easier to ask the question, "What isn't Copilot?" because its sheer capability and sophistication put most other SaaS-based AI solutions to shame. According to Microsoft, Copilot is your AI assistant, on hand to help you supercharge your work. And it does just that.

Copilot acts as your very own workplace copilot, supporting you with many of the mundane tasks you hate doing, as well as several tasks you wish you knew how to do.

The core Copilot solutions

Microsoft 365 Copilot

Enhances the user experience across the full Microsoft 365 suite. By leveraging its built-in AI, Copilot assists users in drafting documents, creating presentations, analysing data, and managing emails, to name a few use cases.

Dynamics 365 Copilot

Extends AI capabilities to Microsoft's suite of business applications, including Dynamics 365 and Business Central. It also analyses customer interactions, predicts trends, and automates routine tasks such as financial reporting, freeing up valuable time to focus on strategic work.

Security Copilot

Leverages advanced algorithms to enhance cybersecurity measures. With real-time threat detection, automated response actions and comprehensive risk assessments, businesses can safeguard their digital assets with continuously monitoring network activities that look for potential vulnerabilities.

Copilot Studio

Enables businesses to create and integrate their own AI agents into their own existing applications, tailoring Copilot-level AI to their unique workflows and processes.

Is Copilot worth the investment?

We certainly think it is – perhaps the following benefits will entice you to give Copilot a go?

Enhanced productivity - Employees complete more tasks in less time, allowing them to focus on high-value activities that drive business growth.

Improved decision-making - Copilot helps businesses identify trends, uncover opportunities, and mitigate risks by analysing large volumes of data and providing predictive insights.

Streamlined operations - Copilot streamlines business operations by automating repetitive tasks and optimising existing workflows, reducing the burden on employees and minimising the risk of errors.

Enhanced customer interactions - Copilot analyses customer interactions and behaviours, suggesting ways to personalise your marketing strategies, identify cross-selling opportunities, and predict customer needs.

Robust security like never before - Security Copilot helps businesses stay ahead of threats by proactively addressing security risks and protecting digital assets, enabling businesses to maintain a secure environment for their operations.

You get out what you put in

Investing in Copilot is not cheap, but the potential it unlocks is limitless. If you invest the time and effort in understanding its capabilities, you'll agree that it's the best thing your business has ever implemented—and that it more than pays for itself in boosting business productivity.

It's all about the prompt

With its no-code functionality, Copilot is fit for every type of worker, irrespective of their technical know-how. Using Copilot is less about using technology and more about how you use it. Based on prompts, the output of Copilot is only as good as the input.

A poor prompt might be vague or lack context, leading to suboptimal results. On the other hand, a good prompt is specific and detailed.

A poor prompt

"Generate a report"

A good prompt

"Generate a sales report for the last quarter including revenue, profit margins, and top-performing products."

Are you interested in exploring Copilot more before you make the jump?

Take advantage of a **free** Copilot demo or find out more about our Copilot readiness workshop by scanning the QR code below.

Addressing cyber security threats in 2025

According to the UK Home Office's Cyber Security Breaches Survey, published April 2025, 43% of UK businesses and 30% of charities reported cyber incidents in the past year. The cyber security risks to businesses have never been more serious and we expect this to only increase throughout the remainder of 2025 and beyond. Cybercriminals are relentless in their pursuit of gain – at your expense. The likelihood that you will fall victim to an attack is increasing every day, so if you're not currently thinking about building resilience and protecting against threats – known and unknown – then it's time you did.

The cyber threat landscape in 2025

The opportunity for cybercriminals is significant: there are an infinite number of gains to be made, from selling data on the dark web to ransoms and theft of money and assets from business accounts. All it takes is one weakness in your infrastructure, and your entire business is at risk.

In 2025, businesses are likely to be on the receiving end of several key types of cyber threats:

Ransomware attacks

A ransomware attack occurs when attackers gain unauthorised access to critical business data, locking users out of their systems. The attackers then demand a ransom, typically in cryptocurrency, in exchange for the decryption key needed to restore access to the data.

This kind of attack can have devastating consequences for businesses, resulting in significant financial losses and severe reputational damage. Implementing robust cyber security measures, such as regular data backups (ideally automated), employee training on recognising phishing attempts, and implementing or activating solutions with advanced security, is the key to mitigating the risk of ransomware attacks.

Phishing scams

A phishing scam involves using deceptive emails, messages, or websites to trick individuals into divulging sensitive information such as usernames, passwords, or financial details. This type of threat continues to be popular amongst low-level cyber criminals and is believed to cost UK victims an average of £1,169 per person, with the 55+ age bracket being most affected. Sadly, it's not just consumers who are victims. In fact, advanced phishing techniques, including spear-phishing and whaling, are targeting high-level executives to gain access to valuable data.

Did you know...

Spear-phishing is where the attacker customises a deceptive message to a specific individual or organisation, often using information gleaned from social media or other sources to make the message appear legitimate, increasing the likelihood of the recipient falling for the scam and divulging sensitive information.

Whaling is a variant of spear-phishing that specifically targets high-level executives such as CEOs or CFOs.

Malware

Malware is the creation of malicious software designed to infiltrate, damage, or disable computers and networks. It typically involves viruses, worms, trojans, ransomware, spyware, or adware, which disrupt normal operations, steal sensitive information, or gain unauthorised access to critical business systems. The presence of malware within a network can provide an easy gateway for further malicious attacks, potentially allowing cybercriminals to establish long-term control over business systems.

Insider threats

Insider threats are among the most dangerous to a business. They occur when employees with access to sensitive information accidentally or deliberately compromise security, resulting in a serious data breach.

Advanced persistent threats (APTs)

APTs are long-term targeted attacks where an intruder establishes a foothold in a business network and continuously extracts data over extended periods. Given the nature of this “small and often” approach to data theft, they can be particularly challenging to detect and mitigate.

Antivirus

Installing an anti-virus onto a business machine is no longer deemed effective in protecting against the sophistication of modern-day threats. Instead, businesses must adopt a multi-layered approach to cyber security.

The 7 layers of cyber security

Layer 01 - Human layer

Today, most businesses do educate employees. They provide a view of best practices, enforce a policy of firm and regularly updated passwords, implement multi-factor authentication for accessing sensitive data, and conduct frequent unannounced audits to identify and rectify gaps in security practices. If you are not doing this – you really are just leaving the door open.

Layer 02 - Perimeter Security layer

Adequate perimeter security involves establishing robust firewall configurations, deploying intrusion detection and prevention systems (IDPS), using virtual private networks (VPNs) for secure remote access, and implementing network segmentation to isolate sensitive areas and limit the spread of potential breaches. This is a 100% necessary for every business with external access – most businesses have this.

Layer 03 - Network Security layer

Businesses should utilise intrusion detection systems (IDS) to monitor network traffic, restrict access via network access control (NAC), design a secure network architecture with redundancy and failover mechanisms, and conduct regular vulnerability scans and penetration testing to identify and address potential weaknesses.

Layer 04 - Application Security layer

Web application firewalls (WAF) help protect websites against database threats like SQL injection, and where organisations have their own bespoke software, they should adhere to security best practises, utilising tools such as application security testing (AST) to identify vulnerabilities.

Layer 05 - Endpoint Security layer

Antivirus and anti-malware software should be installed and updated regularly to detect and remove threats, while endpoint detection and response (EDR) solutions provide continuous monitoring and threat response. Keeping on top of regular patch management ensures software is current with security updates, and device encryption protects data from unauthorised access in case of loss or theft. This is all easy to say – but practically – poses quite a problem for many organisations. The sheer scale of the work required to maintain this if often overwhelming.

Layer 06 - Data Security layer

Businesses can reinforce data security by encrypting sensitive information during transit and storage, implementing data loss prevention (DLP) solutions, enforcing role-based access controls, and scheduling regular automated data backups to ensure data integrity and availability.

Layer 07 - Mission-critical assets

Policies and procedures help businesses protect mission-critical assets. These include, but are not limited to, robust risk assessments, developing and optimising incident response plans, and business continuity plans.

Helping A1 Pharmaceuticals to keep their data and infrastructure safe after a series of cyber attacks

The challenge

Operating in a sector that is both highly regulated and frequently targeted by cyber threats, A1 Pharmaceuticals experienced a number of cyber security incidents over several years.

The first major breach occurred approximately five years ago when a ransomware attack encrypted critical files, resulting in three days of lost business. Despite recovery through existing backups, the breach exposed vulnerabilities in their IT infrastructure.

The most critical incident came during the busy Christmas season, when the company was compromised in a coordinated attack targeting multiple pharmaceutical businesses. The timing – during a period of reduced staffing and increased demand – amplified the impact. The company had to cut off external connectivity to protect its core operations, resulting in significant disruption and a financial loss exceeding £50,000.

The solution

Following the attacks, A1 Pharmaceuticals deepened its partnership with Arc. Working collaboratively, a full-scale cyber protection strategy was implemented, including:

- Deployment of Managed Detection and Response, multi-factor authentication across all systems
- Upgraded firewall and antivirus protection, including enhanced features from Sophos
- Regular penetration testing and proactive threat monitoring
- Staff training programs, including bi-weekly cyber awareness emails
- Real-time monitoring and response plans for suspicious activity

This comprehensive approach not only restored A1 Pharmaceuticals' systems but also built a robust defence against future threats.

The results

Since implementing these changes, A1 Pharmaceuticals has successfully thwarted further attempted attacks.

In one notable instance, the new protocols prevented a financial fraud attempt by detecting compromised credentials before funds were transferred. Additionally, regular meetings with Arc and system monitoring have led to the early detection of several other threats, preventing potential disruptions.

The company's investment in cyber resilience has translated into tangible protection, increased employee awareness, and restored confidence in their digital operations.

"Thanks to the support of Arc, the changes we've made have genuinely paid off"

Chris Dancer, Managing Director at A1 Pharmaceuticals

Maximising efficiencies with a hybrid approach to IT support

Gone are the days when it was all or nothing - you had to hire a full IT team or outsource every element. Nowadays, egos aside, internal and external teams work in harmony. At the end of the day, both can exist and even prosper by delivering against organisational objectives.

The hybrid IT support model typically combines internal IT strategists and external IT practitioners. The former delivering on big-ticket items, sometimes supported by external parties, while the latter handles the day-to-day, more time-consuming, and less strategic work.

By working together, businesses can leverage top IT skills, strategically plan for future growth, and create a robust and future-proofed IT environment that can reach and adapt to evolving needs.

The hybrid approach: best of breed?

Many businesses are choosing a hybrid approach because it allows them to bring internal teams and an outsourced IT support provider together to deliver exceptional IT support.

Here's a flavour of what you can take advantage of...

Diverse skills

One primary benefit of hybrid IT support is the ability to access a wide range of technical skills. Internal IT teams often possess deep knowledge of the company's people, systems and processes, while external experts bring specialised skills and up-to-date industry insights. This ensures comprehensive IT coverage, addressing routine maintenance, maintaining face to face relationships, as well as dealing with complex technical challenges.

Flexibility

A hybrid model guarantees flexibility. External IT partners can be engaged on an as-needed basis, allowing businesses to scale their support resources in response to fluctuating demands or budgets, which can be particularly valuable during peak periods or when tackling projects that require specific expertise.

Robust security – the most expensive resource

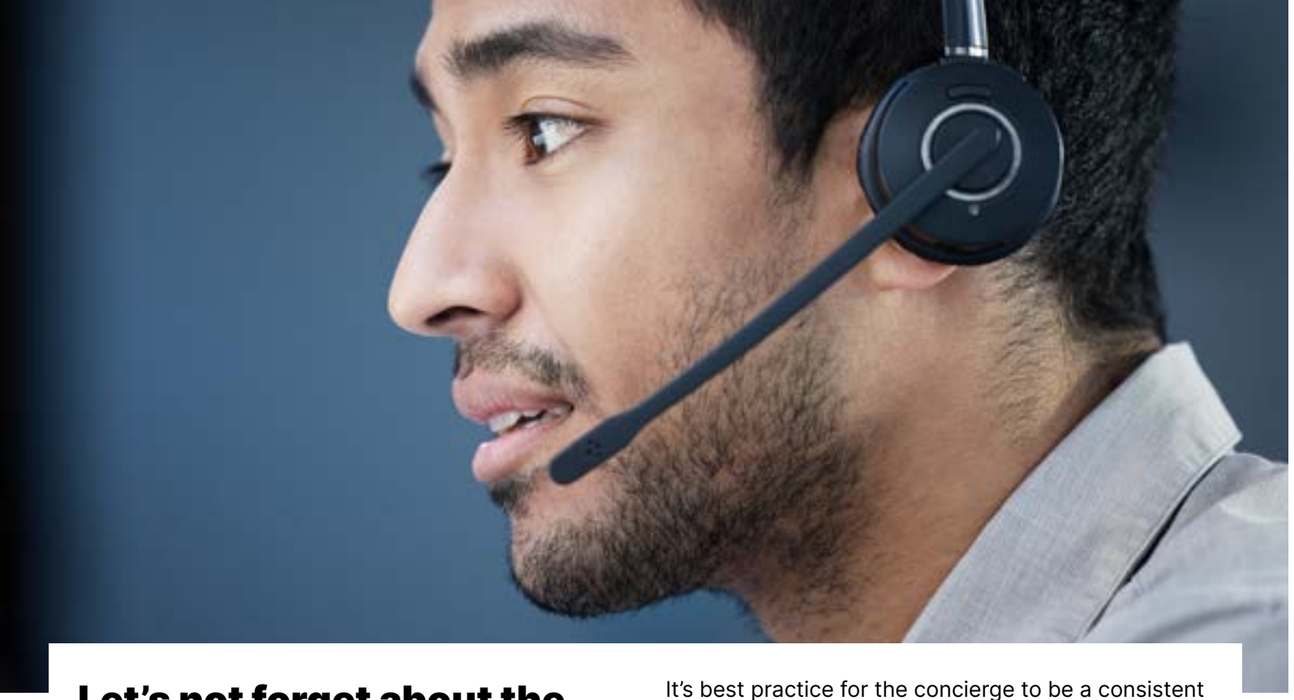
Internal teams are only as good as the pace they keep up with technological advancements, which can be time-consuming. External teams can add value by staying up to date with the latest security solutions and providing insights into new and emerging cyber threats. Models now exist where SME businesses can adopt proactive management by the very best leading industry experts with fractional costs of 24/7/365 staffing whom are already trained and tooled to the highest standards.

An always-on approach to support

Working together makes around-the-clock support more possible, with internal teams handling traditional hours and external support covering out-of-hours. This blended approach helps ensure that day-to-day operations run without disruption. Cyber security is not Monday to Friday, it is often Saturday at 3am. Businesses often need this level of cover.

Strategic success becomes a reality

Bringing all the best minds together makes creating an ambitious strategy much easier. You get the right brains around the table, which results in a better strategy that can be delivered across both teams. Moreover, an external party can more easily objectively identify opportunities for improvement and innovation (without feeling exposure), with internal teams implementing these strategies in alignment with the company's goals and objectives.



Let’s not forget about the role of the concierge

Despite many organisations encouraging people to return to the office five days a week, remote work looks set to endure for the long term.

Whilst that provides flexibility for businesses and workers - from reduced rents and rates - to fitting work in around individual lifestyles, it provides a headache for businesses without flexible IT support. When people work at home, often with diverse working patterns, how do you provide an effective and efficient IT support service?

The secret lies in the art of the concierge: consistent, scheduled office days when IT support is onsite and can resolve any of your non-emergency issues. Can’t connect to the office printer? Do you sometimes struggle to get applications to open first time? Your dedicated IT support concierge can help.

How should the concierge work?

Sometimes referred to as fractional on-site IT support, the concierge requires a commitment to being onsite for a specific period – for example, Monday and Thursday mornings. The concierge member simply walks the floor, assisting team members with whatever IT-related queries they have. This hands-on approach builds rapport and trust between IT support as a function and the wider business. It also helps ensure that ad-hoc IT problems are addressed promptly and effectively, reducing the likelihood of business downtime.

It’s best practice for the concierge to be a consistent figure, somebody individuals can get to know. It may be silly to say, but if you know somebody on a 1-1 basis, you’re more likely to go to them for help. That means that as a business, you’re driving the best possible ROI from your investment in a concierge function, as well as supporting a business and individual desire for more personalised IT support.

Whatever your view, the hybrid approach is here to stay

The hybrid IT support model represents a strategic approach to managing a company’s IT needs. By combining the strengths of internal and external IT experts, businesses get the IT support they need.

As technology continues to evolve, the importance of a robust and adaptable IT support system cannot be overstated. By embracing a hybrid approach to IT support, companies can build a resilient IT infrastructure that supports their current needs and anticipates future challenges.

In summary, hybrid IT support is more than just a trend - it’s a comprehensive solution that empowers businesses to leverage the best of both worlds. With the right combination of internal and external IT resources, they can achieve a higher level of operational excellence and stay ahead of both the competition and changing landscapes, including unforeseen market changes.

The link between IT support, enhanced monitoring, compliance and data governance

As businesses, we are storing more data than ever before. In fact, a report by **Cybersecurity Ventures** reports that the total global data storage is projected to exceed 200 zettabytes by 2025. As well as a wealth of internal company data, such as financial records, applications, and everyday documents, we’re storing an incredible volume of data relating to our people and customers. Consequently, businesses have a moral and legal duty to ensure that the data they hold is secure and compliant with regulations such as the General Data Protection Regulation (GDPR).

As compliance and regulations become more stringent and far-reaching, many businesses find themselves struggling with the technical aspects of data security. While they may have data protection officers and policies in place, enacting these measures can be challenging, leading to vulnerabilities in their infrastructure security. This is where external IT support partners really come into their own. With their expertise and makeup, they can often provide more measurable performance metrics than internal equivalents and are more likely to be ahead of the curve when it comes to supporting businesses through the complexity of compliance while ensuring business infrastructure is protected at the same time.

Highlighting persistent problems: The importance of effective performance monitoring

One key advantage of engaging external IT support is their ability to measure and report on meaningful performance metrics. Unlike some internal teams, reporting performance is a contractual obligation for an IT partner.

Performance metrics - such as response times, resolution times, and system uptime - are consistently tracked and reported accurately, providing valuable insights into the efficiency and effectiveness of their IT operations. For example, an external IT support provider can offer detailed reports on how quickly issues are resolved, highlighting areas for improvement and identifying trends that may indicate underlying problems.

Additionally, external IT support partners regularly use proactive advanced monitoring and reporting tools that provide transparent, real-time visibility into system performance. Using proactive tools allows businesses to address potential issues before they escalate into significant problems, thereby minimising downtime and ensuring seamless operations.

How do you stay focused with a target on the move?

One of the greatest a business challenges (and ultimately distractions) is the ever-changing compliance and regulation landscape. With new standards popping up all the time, it can be difficult to understand what you’re supposed to be doing. Not to mention that it can provide an inconvenient distraction from day-to-day tasks, taking focus away from cyber security and potentially exposing your infrastructure to an unforeseen attack.

External support organisations are often better equipped to handle these changes, thanks to their specialised knowledge and the resources they have available to them. Complying with UK standards is second nature to them, making it easier for small to medium businesses to meet requirements such as GDPR, ISO, and Cyber Essentials Plus.

Implementing comprehensive security measures

Strong governance is essential for identifying, managing, and reducing cybersecurity risks. Even the smallest business must commit to reviewing its foundational cyber security protocols. Things such as:

- Patch management and software updates
- Virus and malware protection
- Security measures for email and web browsers
- Data backup, recovery, and restoration
- Access controls
- Mobile device management: Recording, monitoring, and updates
- Clear policies and procedures for these management tasks

Dropping the ball on even one of these areas exposes your organisation to risk, and articulating the weight of that risk is sometimes not easy.

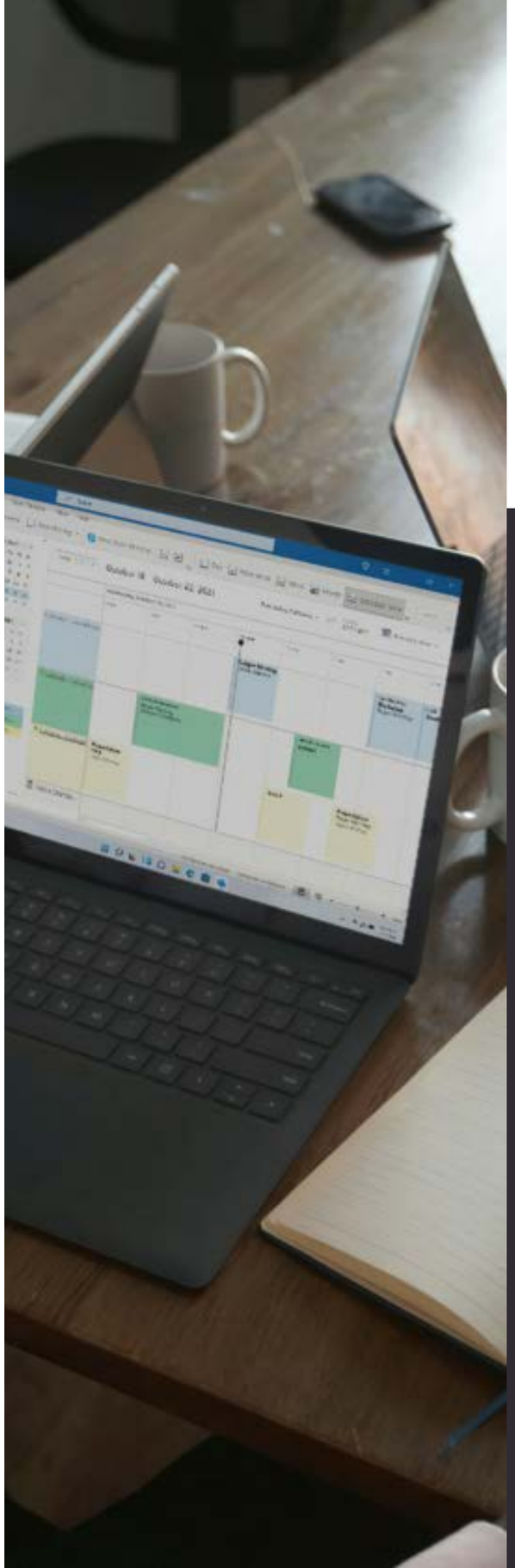
Knowing where you are, and how big your gap is, is the very first step. An external party will deliver an objective unbiased view. Alongside manual surveys, third parties can audit your infrastructure, conduct penetration testing both internally and externally, and even define future vulnerabilities. They can also create the necessary board level governance to ensure the risk you carry is fully understood.

The bane of every business: legacy systems

While many businesses have invested in migrating legacy systems, many also remain using them for business-critical activities. The fear of migration is just too great. Other organisations simply do not understand how exposed they are.

Legacy systems cause headaches for both internal and external teams. Due to an inability to change them, some legacy systems can be cumbersome to use, with lengthy processes working around what should be simple tasks. Additionally, there is a daunting fear of how systems will be maintained if skilled team members leave the business.

The good news: managed service providers can help you maintain legacy systems, secure the edges, and often have the skill set scale to ensure your availability for the long term.



Procuring IT support services

Given how important technology is to businesses today, senior leaders must be concerned about getting the procurement process right.

Gone are the days when IT only touched email, phone lines and servers. Now, IT touches – or powers – everything we do in business. From creating and hosting documents to building and managing applications and the growing beast of cyber security.

Many find it challenging to know what to go to market for and how to manage the procurement process. In this article, we aim to make procuring IT support services sensible, providing plenty of best-practice guidance along the way.

The typical procurement process

01 Initial scoping

The initial scope should be created at the start of every procurement process. This list should include what the procurement lead believes the business needs at a top level, such as someone to manage cloud computing or cyber security.

02 Broader requirement gathering

Once a baseline list of services is established, the procurement lead should discuss individual and team needs across the business and create a more comprehensive list of requirements based on particular tasks and team functions.

03 Needs refinement

Now it's time for the long list to be prioritised, removing duplicate and similar tasks and removing anything that is not business critical (or that can be picked up internally).

04 Brief building

The refined list details what the company needs from an IT support partner, forms the foundation for the brief and details the scope of services required.

05 Objective setting

The business now needs to define what good looks like and the metrics for how they'll measure success from their new IT partner. Remember to link this back to the overarching business objectives.

06 RFP

The Request for Proposal is created and distributed or promoted, inviting potential IT support providers to submit a response.

07 Shortlisting

Now that you have your responses, it's time to evaluate them and shortlist your top 3 to 5, whom you will invite to interview. Remember to cross check back the evaluation to the criteria you shared in the RFP process. Be sure to consider case studies and references at this point.

08 Negotiation & appointment

With your chosen partner now selected, it's time to negotiate the finer details of the contract, including pricing, SLAs and any additional services you may want to procure (that were not part of the original RFP).

Tips for a smooth procurement process

01 Communicate openly and transparently with all stakeholders throughout the process. This helps manage all parties' expectations and sets the relationship up for long-term success.

02 Ensure transparency by sharing any information that has material value to the process (during or after). You may miss something crucial out of the process, which later incurs an additional cost. Similarly, you might appoint the wrong partner (either expertise or cultural or business fit).

03 Keep accurate records of all communications, proposals, evaluations, and decisions made so that you can refer to them at any point.

What makes a good Request for Proposal (RFP)?

A good, robust RFP should include all of the following:

- A detailed brief – where you are now and where you want to be
- Your specific service requirements
- What you're looking to achieve
- How you'll measure success
- Your indicative IT support budget
- How you will evaluate responses

Moving beyond money

It's easy for a business to base a procurement decision on price alone. From experience, we see too many take this approach only to hit numerous stumbling blocks. When it comes to IT support and the security of your business's IT infrastructure, it's important that you make decisions on the best fit: who can provide the best service to your business? After all, the price to pay for a security breach or leaving a contract early to restart the procurement process can be substantial. It's important to get it right the first time.

What does IT support look like in 2025 and beyond?

In 2025, AI is set to continue significantly influencing how we work. People are beginning to see the benefits of solutions like Copilot and ChatGPT, which make their working days easier and enable them to work smarter, not harder. But AI is only an enabler and is only as good as its user. IT support will develop in many other ways, with users expecting more without necessarily putting in the work themselves. So, how do IT support teams react? Towards the end of 2024, we were already beginning to see changes in users' habits and needs. But there are generational contrasts, and as IT support teams, how do you be all things to all people?

More so than ever - 2025 is a year of listening, understanding, learning and responding. People want more from life and more from work, so technical teams will undoubtedly be busy.

Our predictions for IT support in 2025 and beyond

The acceleration of automation

IT support teams already know the power of automation and many use it in their day-to-day operations. In 2025, we see this intensifying, with costs and pressures forcing teams towards greater efficiencies. Stored business information will start to create value, and automation will begin to bring searching to an end. Pertinent predictive valuable insight information will be displayed within context, in real time. A users need will be predicted, and the typical source information surfaced as a user needs it.

As AI becomes more accurate and sophisticated, AI-powered chatbots and virtual assistants will become commonplace, and users will spend less time engaging with humans and more time engaging with technology.

Our prediction: Users will not mind if they can still swiftly access a human if the chatbot or VA is unable to resolve their query. Time will be of the essence.

Personalised experiences will take centre stage

The traditional one-size-fits-all approach to delivering support is no longer fit for purpose. The technology gap is widening, and IT support teams will need to be able to cater to all needs, those who embrace technology and those who struggle to understand it.

Our prediction: User satisfaction with IT will drop whilst businesses struggle to adapt to these new expectations.

Where's the data?

Decisions will be made less based on subjectivity and more on hard facts. Businesses will begin to use the data they have had available for many years to inform decisions. Those decisions will also be augmented with guidance from AI.

Our prediction: There will be a greater expectation for accountability within teams and departments as more insight and informed decisions can be made. Greater focus will be given to alignment of IT strategy and overall business strategy. As a result, more people will look to third parties to support filling recognised gaps.

The generational gap provides a real challenge

Different generations have distinct expectations when it comes to IT support and we're seeing a widening of the space between AI comfortable and traditional use. Older workers (i.e., Baby Boomers) who did not have the luxury of growing up with technology will continue to need more support than younger generations (Zoomer, Gen Z) who grew up with mobile phones and computers from an early age.

IT support teams will implement automation to accommodate younger workers while spending more human, one-on-one time with those who are less comfortable with technology.

How different generations might access support

Zoomers (GenZ)	
Expects	Instant support
Prefers	Self-service tools and AI chatbots
Values	Efficiency

Baby Boomers	
Expects	To speak to a human
Prefers	1-1 support via a telephone call
Values	Clear communication & guidance

We said upfront in this article that it's going to be a year of listening, and if you've read this far, we're sure you agree. Individual employees will have more say in how IT is delivered and become more vocal when it doesn't quite meet their needs.

The upside? IT budgets will continue to increase, with businesses understanding that the ROI benefits, such as user satisfaction, productivity, and efficiency, outweigh the cost - assuming they can afford to keep up with the pace of technology advancement.

Advanced business needs require advanced IT services

With rising costs, increased competition and technology's renewed role in powering much of what we do, businesses are being forced to rethink their business models and make difficult decisions about where to invest. Having a solid proposition is no longer enough. Instead, they need to operate lean businesses to afford the sorts of budgets that enable them to be competitive.

With that, the same old BAU approach to IT support is changing, too. Businesses need more than basic troubleshooting; they demand a comprehensive, proactive approach to managing and maintaining their IT infrastructure. One that is forward-thinking and has innovation and proactivity at its heart.

What businesses need from IT support has changed

Support has primarily focused on resolving issues as they arise - everyday BAU troubleshooting. For years, this was a sufficient approach to delivering and receiving support. But with the pace of change and the rising risks, it's no longer adequate.

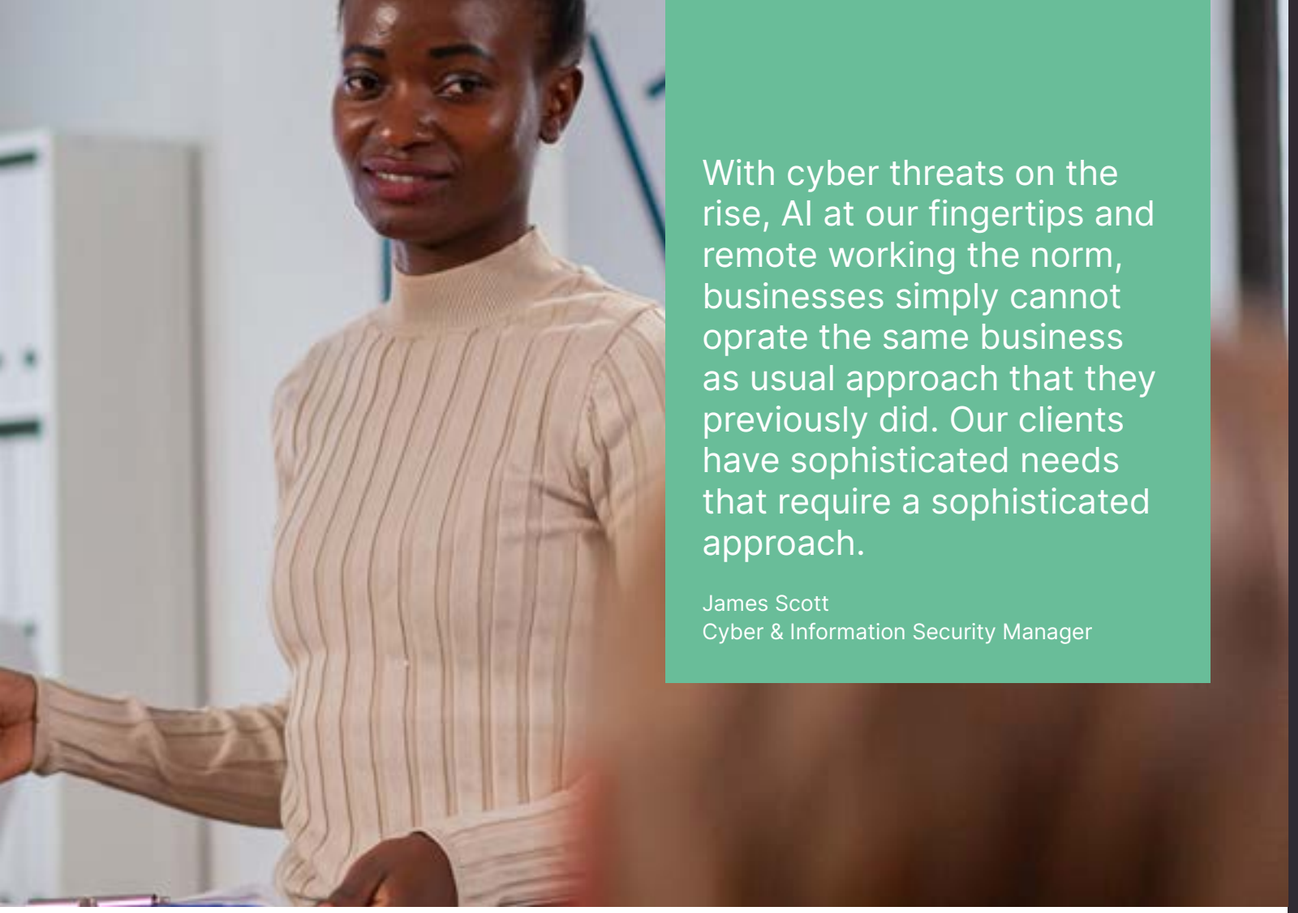
Nowadays, every minute a business experiences downtime is a loss that directly hits the bottom line. What's more, in addition to a drop in revenues, there's reputational risk. Consumers are fickler than ever; if they have even the tiniest of poor experiences, they'll go elsewhere.

Proactivity as standard

With this change in needs comes an increasing business need for proactive services. That means proactive monitoring of end-to-end infrastructure and proactive maintenance. In effect, businesses want to know their risks are minimised before the event, not as it happened. Conversations have turned from "this is an issue; here's what we recommend" to "this could have been an issue; here is how we prevented it from happening."

Advanced threat protection

With threats advancing and becoming more sophisticated, the need for more robust protection is clear. Traditional antivirus software and firewalls are no longer sufficient to safeguard against modern cyberattacks. Instead, businesses require advanced security measures to detect, prevent, and respond to a wide range



> With cyber threats on the rise, AI at our fingertips and remote working the norm, businesses simply cannot oprate the same business as usual approach that they previously did. Our clients have sophisticated needs that require a sophisticated approach.
>
> James Scott
> Cyber & Information Security Manager

of threats in real time, with well-defined incident response plans in place to ensure the quick and effective mitigation of the threats, minimising damage and reducing recovery time.

Additionally, businesses are now looking for IT support to assist in employee training, educating individuals about cybersecurity best practices to strengthen their frontline of defence: people. After all, if businesses can reduce the likelihood of accidental incidents, they can limit their overall risk profile.

The power of virtualisation

Virtualisation has opened up a new way of managing IT resources while minimising costs. By creating virtual versions of hardware, software, and storage, virtualisation allows for more highly efficient resource use and singular IT management.

Embracing the scalability of the cloud

Cloud computing has transformed IT support by offering a flexible, scalable and cost-effective way to access business data and applications from anywhere, anytime. It enables businesses to quickly implement solutions that help them to overcome everyday challenges, whatever they may be.

Advanced needs require advanced relationships

When dealing with complex situations, you need a partner who understands what you're going through. This partnership should be built on trust, transparency, and mutual understanding, underpinned by genuine experience and expertise in a sector, solution, or challenge - or all three.

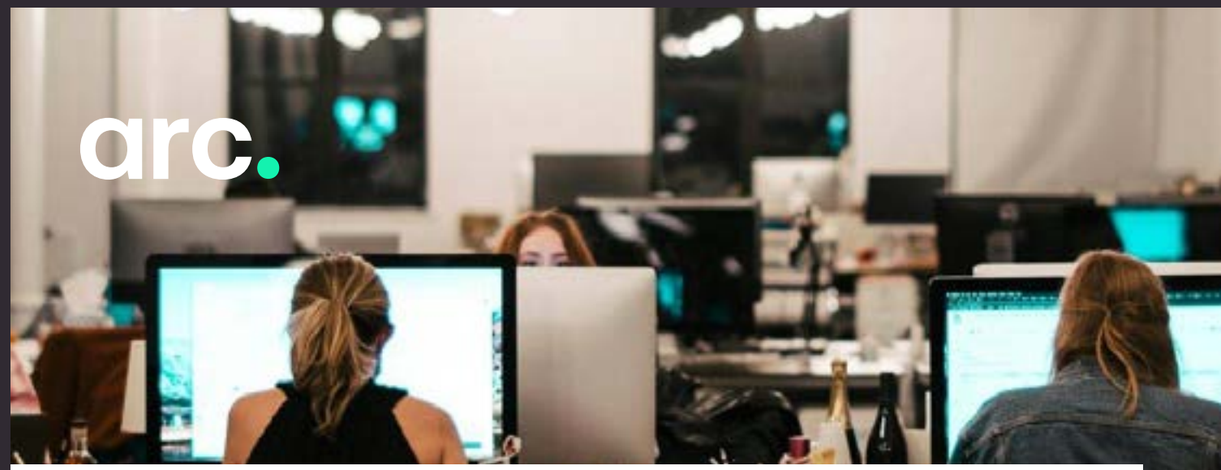
Further, you need a partner in it for the long run, not somebody who will turn their back on you at the first possibility.

Advanced relationships mean challenging each other where appropriate, making proactive recommendations for improving things and striving for innovative excellence.

By combining advanced solutions with a long-term, experienced and strategic partner, you truly set yourself up for sustained success.

If there's an extra mile, we'll go there.

We're tech experts. But we won't blind you with science – we show up and get things done, helping you to stay ahead of the challenges rather than simply reacting to them. And if there's an extra mile when it comes to keeping your tech running, we always go there.



Our numbers always add up.

Numbers, as they say, never lie. Here are some that all add up to why you should be using Arc when it comes to managed IT support.

25400+
helpdesk tickets logged across 2024

99.8%
first response SLA met across 2024

33
years experience delivering cutting edge IT solutions

600+
active customers

Get in touch with Arc.

Visit arcsystems.co.uk **Call** 01268 288100

Talking Tech.