

BUILDING A **SMARTER** **IT STRATEGY** FOR SUSTAINABLE GROWTH

An Essential Guide to Driving Innovation & Efficiency
in SME Engineering and Manufacturing Firms



**Speak to our
expert team**

Our office is
open between
9:00AM – 5:30PM
weekdays.



01604 879330



info@moon.co.it



INTRODUCTION:

In an economy defined by rapid technological change, engineering and manufacturing firms are under growing pressure to innovate, adapt and deliver at speed. From adopting Industry 4.0 technologies to meeting increasingly stringent regulatory requirements and customer expectations, the stakes are higher than ever.

These pressures are particularly acute in the manufacturing industry. Operating with lean teams and constrained budgets, SME engineering and manufacturing businesses must balance the demands of day-to-day operations with a strategic imperative to modernise.

The challenges of managing legacy systems, fragmented infrastructure, manual processes and complex compliance obligations can expose firms to cyber threats, hinder productivity and impede growth.

At the same time, the digital landscape offers unprecedented opportunity. Cloud computing, IoT, data analytics and AI can transform operations, enhance decision-making and accelerate innovation.

But realising this incredible potential to optimise, innovate and grow, demands IT foundations that are robust, scalable and secure.

This is where managed IT services play a vital role. By partnering with a trusted IT provider, SMEs can offload the day-to-day management of their digital environment, freeing internal resources to focus on core operations and innovation.

CONTENTS

Introduction	02
Why IT modernisation matters	04
The challenges you're facing	05
How do managed IT services make my life easier?	07
Highlight: cybersecurity in manufacturing	08
How can I build a smarter IT strategy?	09
What do I need to do?	10
Case study: Rulmeca UK	11
Why choose Mooncomputers?	13

WHY IT MODERNISATION MATTERS

Stay ahead of competitors

Firms that embrace automation, smart factory systems, and Industry 4.0 practices can dramatically improve productivity and responsiveness – critical in today's fast-moving markets.

Strengthen cyber resilience

Cyberattacks are on the rise in manufacturing, with ransomware, IP theft, and supply chain breaches now common. Modern IT architectures and managed services provide essential protection.

Prove your quality & compliance

Regulatory frameworks (ISO 9001, ISO 27001, GDPR, Cyber Essentials, export controls) require robust IT processes. Demonstrating compliance also strengthens customer trust and unlocks high-value supply chains.

Control costs & improve scalability

Modern IT turns unpredictable CAPEX into manageable OPEX, delivering enterprise-grade tools and infrastructure on SME-friendly terms. Scalability enables you to grow without heavy reinvestment.

Enable innovation & agility

Smart IT strategies free internal teams from firefighting and enable focus on innovation – critical for differentiating products and services in competitive global markets.

In this guide, we explore how engineering and manufacturing firms can leverage modern IT strategies and outsourced services to:

- Enhance productivity through automation, streamlined workflows, and reliable infrastructure
- Protect critical data from evolving cyber threats and ensure regulatory compliance
- Control costs by converting unpredictable capital expenditure into manageable operational spend
- Prepare for the future by adopting scalable technologies that support agility and innovation
- Adopting a smarter, security-first approach to IT enables manufacturers like you to gain resilience, agility, and competitive edge in a fast-moving digital-first world.



THE CHALLENGES YOU'RE FACING

The Engineering and Manufacturing industry is a driving force of innovation and a critical pillar of the UK economy. Yet they face a series of deeply interrelated challenges that can constrain growth and competitiveness – especially as they strive to compete in an increasingly global, digital marketplace.

1 Skills shortages

The skills gap in engineering and manufacturing is well documented. As experienced engineers retire, SMEs struggle to attract new talent with the digital and technical competencies required in modern manufacturing – from CAD/CAM design to automation and control systems. Limited budgets often constrain investment in upskilling existing teams, leaving firms exposed and slow at adopting Industry 4.0 practices.

2 Financial constraints

Operating with tight margins and limited access to capital, you must manage rising costs across energy, raw materials, transportation, and compliance – all while maintaining profitability. Investing in transformative technology or automation can seem risky or out of reach, making reactive spending more common than proactive IT modernisation.

3 Cybersecurity risks

As firms digitise and adopt cloud-based solutions or connected machinery, cyber risk escalates. Manufacturing SMEs are increasingly targeted by ransomware, phishing, and Intellectual Property theft. Without dedicated security resources or robust incident response plans, the business impact of a breach – from operational downtime to reputational damage – can be devastating.

4 Legacy IT and fragmented infrastructure

Outdated ERP systems, isolated shop floor machinery and manual processes create data silos and hinder agility. Many SMEs recognise the need to modernise but are held back by perceived complexity, cost and operational risk.

5 Limited ability to adopt advanced technologies

Emerging technologies such as IoT, AI, automation and robotics offer tremendous potential. But SMEs often lack the capital and expertise to deploy them effectively. Without clear ROI and strategic guidance, firms risk being caught in a cycle of reactive rather than transformative technology investment.

6 Regulatory burden

Navigating complex regulatory landscapes – from health and safety and environmental compliance to standards like ISO 9001, ISO 14001, ISO 27001, Cyber Essentials and GDPR – places an additional strain on internal resources. Post-Brexit trade complexity further exacerbates compliance challenges.

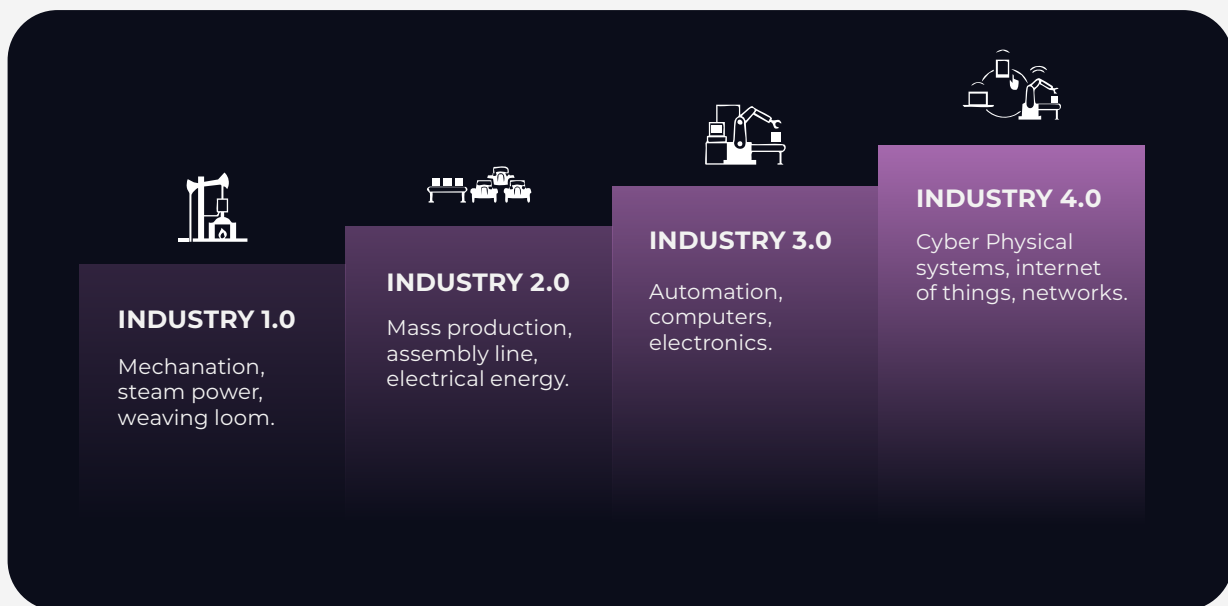
7 Supply chain fragility

Recent global disruptions have exposed vulnerabilities in lean supply chains. Many are re-evaluating their supply chain strategies – yet without modern IT systems to support visibility, agility and resilience they remain exposed.

8 Digital transformation uncertainty

The path to Industry 4.0 is clear – but how to get there is less so. Many lack confidence in how to plan and execute a digital transformation journey. Cultural resistance, operational risk and unclear ROI can slow or stall progress.

These challenges are highly interconnected. Cyber risk often stems from outdated systems; automation is constrained by skills gaps; underinvestment in IT traces back to financial uncertainty. Addressing them requires a strategic, holistic approach.



HOW DO OUTSOURCED IT SERVICES MAKE MY LIFE EASIER?

For most engineering and manufacturing SMEs, the traditional reactive, internally managed approach to IT is no longer fit for purpose. The demands of a modern digital infrastructure – and the associated risks – exceed what most internal teams can manage alone.

Managed IT services, delivered by an experienced MSP (Managed Services Provider), offer a practical, cost-effective way to transform IT capabilities and position the business for growth.

Access to expertise

Outsourced IT provides instant access to a wide pool of specialists in cybersecurity, cloud infrastructure, data protection, networking, and compliance – without the overhead of building an in-house team. This ensures IT decisions are informed by best practice and aligned with strategic goals.

Cost control

Managed services convert unpredictable capital expenses into stable, predictable operational spend. You can access enterprise-grade solutions – from cloud platforms to advanced cybersecurity – on terms that fit your budget and growth trajectory.

Stronger cybersecurity

With 24/7 system monitoring, proactive threat detection, automated patching and rapid incident response, MSPs help you dramatically strengthen your cyber resilience. Tailored to the risks of the manufacturing sector, this protection minimises business disruption and safeguards intellectual property.

Support for digital transformation

An MSP can assess legacy infrastructure, guide technology upgrades and ensure new solutions integrate seamlessly into existing workflows. Whether migrating to cloud-based ERP, enabling smart factory operations or deploying IoT sensors, the MSP delivers expertise and project leadership – accelerating transformation and reducing risk.

Simplified compliance

By aligning IT systems with standards like GDPR, ISO 27001 and Cyber Essentials, managed IT services simplify compliance and audit processes. This reduces legal exposure and builds trust with partners and customers.

Enhanced supply chain resilience

Modern IT enables secure data sharing, real-time visibility and improved collaboration with supply chain partners – increasing agility and responsiveness in a volatile global environment.

Scalability and flexibility

As business needs evolve – whether through new product development, market expansion or digital innovation – MSPs provide scalable IT infrastructure and flexible support. Meaning you can grow without the need for major reinvestment or internal reorganisation.

In short, managed IT services enable you to operate with the resilience, agility and innovation capacity of a much larger enterprise – without the associated cost or complexity.

HIGHLIGHT: CYBERSECURITY IN MANUFACTURING

SME manufacturers are prime targets for cyberattacks. Intellectual property, just-in-time production, and interconnected supply chains all increase cyber risks.

Common gaps:

- Legacy equipment with unpatched vulnerabilities
- Limited staff awareness and training
- Insecure remote access
- Lack of incident response plans

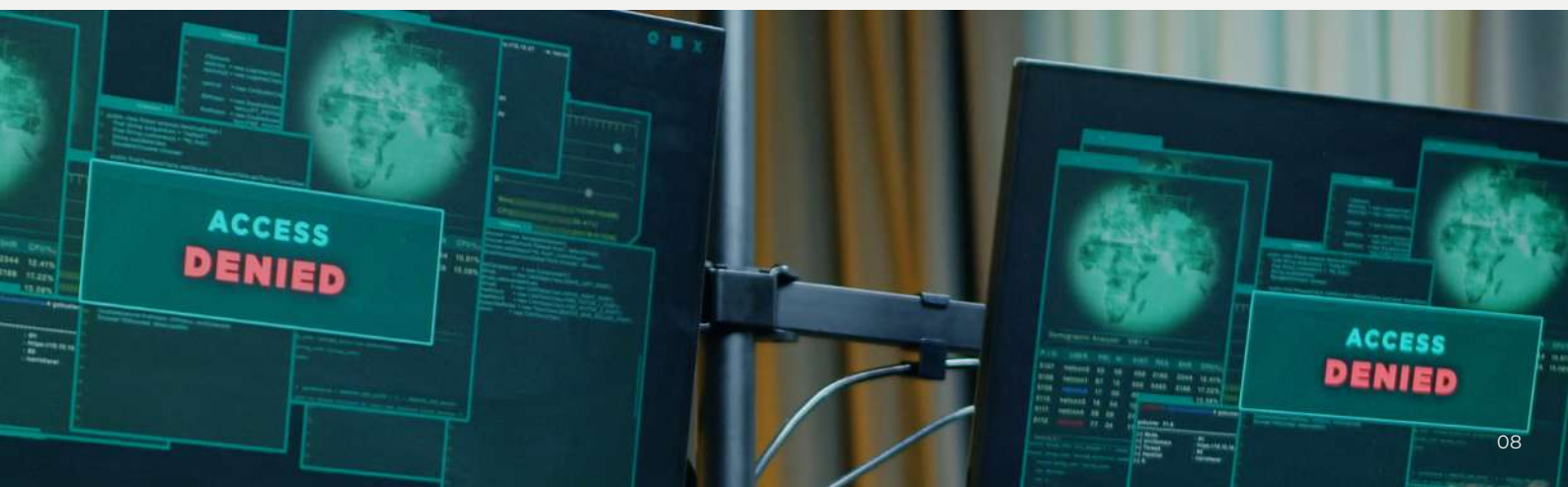
Managed IT services mitigate these risks through:

- Endpoint protection and network monitoring
- Secure remote access solutions
- Vulnerability scanning and patch management
- Proactive incident detection and response
- Backup and disaster recovery planning
- Employee cybersecurity awareness training

Unfortunately, many SME manufacturers remain vulnerable. Legacy systems, unsupported software, and limited in-house security expertise create an ideal environment for attackers. Phishing, ransomware, and supply chain breaches are no longer rare occurrences—they are daily realities. Even relatively unsophisticated attacks can bring production lines to a halt, compromise confidential designs, or expose customer data, leading to downtime, reputational damage, and regulatory penalties.

“Businesses with proactive IT support see 40% less downtime.”

CYBER SECURITY BREACHES SURVEY 2024



HOW CAN I BUILD A SMARTER IT STRATEGY?

1 Assess current state

Conduct a full IT audit of your organisation's infrastructure, processes, data handling, security posture and operational risks.

Go beyond a simple hardware inventory – map software dependencies, evaluate network architecture and identify potential compliance gaps. Document opportunities for efficiency gains, automation and integration.

2 Align IT with business goals

Clarify your core business objectives: Is your priority faster production cycles? Improved quality control? Enhanced compliance reporting? Entry into new markets or customer segments? Translate these goals into measurable IT outcomes.

For example, if reducing lead times is a target, prioritise investments in shop-floor automation and real-time data visibility. If compliance is key, focus on systems that support audit trails and document control. This ensures IT investments drive tangible business value.

3 Choose the right IT partner

Selecting the right managed services provider is a strategic decision. Look for a partner with proven experience in the engineering and manufacturing sectors—someone who understands machine-to-cloud connectivity, shop-floor system integration and the importance of uptime.

4 Develop an IT roadmap

Create a phased roadmap for IT improvement that balances short-term wins with long-term strategy. Identify quick wins such as upgrading endpoint protection, enhancing remote access security or migrating key applications to the cloud.

5 Foster internal digital culture

Digital transformation is as much about people as technology. Start with mandatory cybersecurity awareness training for all employees. Encourage teams to identify and champion process improvements and as staff confidence grows, more advanced initiatives like IoT data analysis and quality control will become easier to implement.

6 Monitor & review

IT is not a one-time project – it must evolve continuously. Establish regular review cycles for leadership and IT partners to jointly assess performance against KPIs. Monitor system uptime, security incident trends, user satisfaction and alignment with business goals. Conduct regular cybersecurity testing and compliance audits. Use these insights to refine the IT roadmap for informed future investment decisions. Continuous improvement ensures that IT remains a driver of innovation, not a source of friction.



WHAT DO I NEED TO DO?

Preparing your IT environment for the future requires a structured and comprehensive approach. This checklist provides a practical starting point to enhance your resilience, security and operational agility:

Conduct a full security and risk assessment

A comprehensive security assessment identifies vulnerabilities, evaluates existing controls and ensures alignment with current regulatory and business requirements. This proactive step is crucial for safeguarding sensitive data and ensuring operational continuity.

Audit current infrastructure and identify bottlenecks

An infrastructure audit reveals inefficiencies, compatibility issues, and performance constraints that can hinder productivity and scalability. Addressing these bottlenecks with an experienced partner to guide you will optimise resource utilisation and improve agility.

Create or update your disaster recovery plan

A robust disaster recovery plan ensures that your organisation can quickly recover from unforeseen disruptions. Regularly updating this plan guarantees business continuity and minimises downtime in the face of cyberattacks or hardware failures.

Assess remote work capabilities and security gaps

With hybrid working models here to stay, it's essential to ensure that remote access solutions are secure, scalable and efficient. Identifying and closing security gaps in remote work infrastructure helps protect both corporate and client data.

Build an IT strategy roadmap for the next 3 years

A forward-looking IT strategy roadmap aligns technology investments with business goals. It provides a clear path for modernisation, ensures readiness for emerging technologies and supports sustainable growth.

Partner with an MSP that understands engineering-specific needs

Choosing a provider with deep industry knowledge ensures that IT solutions are tailored to the unique challenges of engineering and manufacturing. The right partner can deliver operational resilience, compliance assurance and innovation support.

By systematically addressing each element of this checklist, you lay the foundations for a robust, future-proof IT environment that empowers your business to thrive in an increasingly digital world.



CASE STUDY: RULMECA®

Rulmeca UK Ltd, based in Corby, is a key part of Rulmeca Group, globally renowned for manufacturing high-quality rollers, motorised pulleys and conveyor components. Serving industries such as mining, quarrying and logistics, the UK branch is a vital part of the company's mission to deliver reliable and innovative materials handling solutions.

The Challenge

As Rulmeca UK expanded its production capacity and embraced international collaboration, it started facing complex IT challenges. In 2004, they needed to establish a centralised system for sharing data seamlessly across multiple international sites.

Over time, this evolved into a broader requirement for robust cybersecurity, reliable server infrastructure and support for new ways of working—including secure remote access and digital factory workflows.

By 2020, the shift toward remote work and smart manufacturing made these challenges even more urgent. Rulmeca needed to support employees working from home, safeguard against rising cyber threats and equip their growing facilities with fast, secure connectivity and modernised systems.

Our Approach

Mooncomputers IT Services partnered closely with Rulmeca UK to deliver a long-term, scalable IT transformation strategy. Our journey began with centralising their data infrastructure, enabling smooth communication between international branches.

Over the following years, we upgraded servers, introduced resilient firewall protection using WatchGuard technology, and ensured failover systems were in place to maintain continuous connectivity with headquarters in Italy.

As part of ongoing improvements, we implemented Office 365 to streamline communication and cloud collaboration. We also rolled out Bitdefender anti-virus software across the company's systems, thanks to its industry-leading threat detection capabilities.

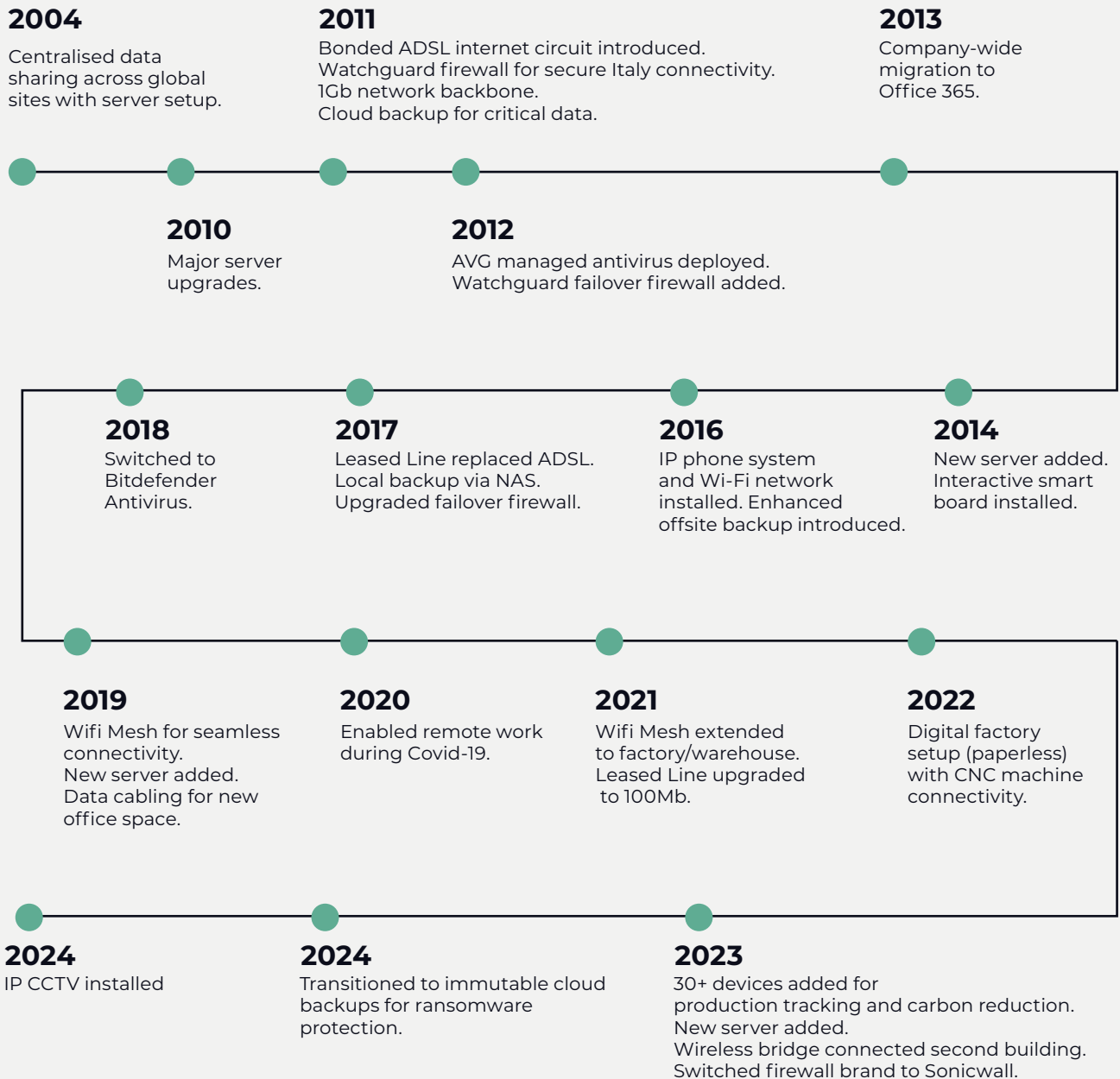
When the pandemic hit in 2020, we helped Rulmeca adapt quickly—enabling secure remote access for 20 staff members. In 2022, we supported the company's move toward a digital factory model by introducing Wi-Fi-enabled servers and station-based systems, reducing paper usage and increasing production efficiency.

Most recently, as Rulmeca UK expanded into a second building, we established a high-speed point-to-point Wi-Fi bridge to ensure seamless internet access between both sites. Additional upgrades included modern IP phone systems, immutable offsite backups, Wi-Fi mesh networks, and the integration of networked CNC machines into their production floor.



The Outcome

The transformation has delivered measurable results across all areas of Rulmeca UK's operations. Collaboration has become more fluid and efficient thanks to the cloud-first setup.



“Mooncomputers IT Services has been instrumental in transforming our IT infrastructure. Their expertise and proactive approach have enabled us to enhance security, improve collaboration, and support our digital transformation journey.”

– Management Team, Rulmeca UK Ltd

WHY CHOOSE MOONCOMPUTERS?

Mooncomputers is a trusted IT partner for engineering SMEs across the UK.

We understand the nuances of the sector and deliver future-ready solutions tailored to your operational goals. Our people-focused approach and technical excellence are grounded in a commitment to long-term client success.

Our mission is simple: to deliver friendly, high-quality, and consistent IT services that enable our clients to thrive. We believe in making complex IT challenges simple to manage, so you can focus on driving your business forward.

Our Services Include:

- ✓ **Managed IT Support and Helpdesk:**
Proactive monitoring, maintenance, and expert assistance to ensure systems run smoothly and end users are fully supported.
- ✓ **Cybersecurity Protection and Compliance Consulting:**
Comprehensive security frameworks, ongoing threat monitoring, and guidance to achieve and maintain industry certifications.
- ✓ **Cloud and Hybrid Infrastructure Solutions:**
Scalable, resilient cloud services and hybrid environments tailored to your operational needs.
- ✓ **Strategic IT Planning and Road-mapping:**
In-depth consulting to align IT investments with long-term business strategy, including digital transformation support.
- ✓ **Onsite and Remote Support across the region:**
Responsive, localised support backed by a nationwide team, ensuring seamless IT performance wherever your people are located.

At Mooncomputers, our core values include accountability, transparency and continuous improvement. We partner with you to provide a resilient, secure and future-proof IT environment – empowering your teams and strengthening your competitive edge.

Let us help you modernise with confidence.

SPEAK TO OUR EXPERT TEAM

Please don't hesitate to contact us, our staff are always happy to lend a hand however we can.

Our office is open between 9:00AM – 5:30PM weekdays.



01604 879330



sales@moon.co.it

Where we are

Mooncomputers Ltd
7 Prospect Court
Courteenhall Road
Blisworth, Northants
NN7 3DG