



# UK SME Cybersecurity Threat Report 2025

# UK SME Cybersecurity Threat Report 2025


## Contents

• Introduction: Why UK SMEs Are Under Siege from Cybercriminals	3
<b>Part One: The Top Cybersecurity Threats Facing UK SMEs in 2025</b>	<b>4</b>
• Ransomware: Holding SMEs Hostage in a Digital Lockdown	4
• Phishing & Social Engineering: Cybercriminals Preying on Human Nature	5
• AI-Driven Cyber Attacks: The Next Frontier of Digital Crime	6
• Insider Threats: When the Danger Comes from Within	7
• Supply Chain Vulnerabilities: The Hidden Risks in Your Business Network	8
<b>Part Two: Why SMEs Are Prime Targets – And How to Fight Back</b>	<b>9</b>
• Weaker Defences: Why SMEs Are Easy Prey for Hackers	10
• Cyber Awareness & Training: Your First Line of Defence	11
• High Trust, Low Oversight: Why SMEs Need Tighter Security Controls	12
• Regulatory & Customer Pressures: Compliance Isn't Optional Anymore	13
<b>The Role of Policies in Strengthening Cyber Defences</b>	<b>14-15</b>
<b>Industry Leadership &amp; Best Practices</b>	<b>16</b>





# Introduction: Why UK SMEs Are Under Siege from Cybercriminals

A large circular image on the left side of the page shows a man with dark skin and curly hair, wearing a yellow shirt and a blue lanyard with the ramsac logo. He is sitting at a desk, looking at a laptop screen. In the background, another person is partially visible, also working at a desk.

Small and medium-sized enterprises (SMEs) form the backbone of the UK economy and are therefore increasingly in the sights of cybercriminals. UK businesses faced **a relentless barrage of cyber attacks** in 2024, in fact, half of UK businesses experienced some form of cyber breach or attack. Fraud and cybercrime are taking a heavy toll on this sector with 41% of UK SMEs having suffered financial losses due to fraud, with an average loss of **£4,000 per incident**.

As SMEs embrace the ever-changing digital landscape with new digital tools and remote work, they find themselves **faced with increased threats** ranging from sophisticated ransomware gangs to everyday phishing scams.

This report provides a structured analysis of the top cybersecurity threats confronting UK SMEs in 2025, and explores why these businesses are increasingly targeted by cybercriminals. It also offers **practical guidance on how SMEs can strengthen their defences**, improve cyber awareness, and meet rising regulatory and customer expectations.

# Part One: The Top Cybersecurity Threats Facing UK SMEs in 2025

## Ransomware: Holding SMEs Hostage in a Digital Lockdown

Ransomware remains one of the most prevalent and devastating cyber threats to UK organisations. In 2023, the UK saw a **70% surge in ransomware attacks** compared to the prior year, with criminals increasingly hitting SMEs, making it essential that SMEs prepare for ransomware campaigns as aggressively as larger firms do.

Ransomware attacks involve criminals infiltrating a company's infrastructure, **encrypting critical data** or systems, and demanding a ransom (often in cryptocurrency) for restoration. Modern ransomware gangs often engage in "double extortion" stealing sensitive data before encryption, then threatening to publish the data unless paid. Ransomware groups are constantly evolving their tactics, and this threat is expected to continue growing into and beyond 2025.

Attackers assume that a small firm will be more likely to pay to quickly resume operations making them a more likely target. A single ransomware incident can **paralyse business operations**, cause permanent data loss, and **incur hefty recovery costs**. Many SME victims also suffer reputational damage if customer or partner data is leaked. Unfortunately, SMEs often lack the robust systems which are fundamental to recover from attacks like these without paying the ransom.

A mid-sized UK logistics company fell victim to a ransomware attack in June 2023. They infiltrated the company's network and left a note on screens: "If you're reading this, it means the internal infrastructure of your company is fully or partially dead." The attackers had encrypted the firm's files and threatened to leak confidential data, essentially holding the business hostage.

[Ransomware Gangs' Merciless Attacks Bleed Small Companies Dry](#)

## Phishing & Social Engineering: Cybercriminals Preying on Human Nature

Phishing is by far the most common cyber threat facing businesses. With **84% of businesses** that experienced a cyber incident in 2024 identifying phishing as the cause. Phishing persists as the top threat, because the people working at an organisation are often the first line of defence when it comes to cyber security. No security tool can perfectly filter out every convincing phishing email, and staff are so busy they are not noticing the tell-tale signs.

Phishing emails often impersonate trusted contacts or organisations, **coaxing employees into clicking malicious links**, entering credentials on fake login pages or opening infected attachments. Attackers also use psychological pressure (urgent deadlines, authority figures, fear of missing out) to prompt impulsive actions. Closely related are impersonation and business email compromise scams, where fraudsters pose as a company CEO or vendor to request fraudulent payments. These tactics are forms of **social engineering** that prey on trust and human error. For example, “invoice redirection” scams where a scammer hacks or spoofs a supplier’s email to

inform the business of “new bank account details”. The SME unwittingly updates the payee information and later sends a legitimate payment straight to the fraudster’s account. Such scams typically go unnoticed until the real supplier asks about a missing payment, by which time the funds have vanished.

A small manufacturing firm in England received an email that appeared to be from a long-time supplier, informing them of new bank account details for future payments. The email was convincing and even included the supplier’s letterhead. The next legitimate invoice was paid to the fraudster’s account. By the time the SME realised something was wrong tens of thousands of pounds had been lost.

[SMEs lost €10m through email-related scams last year - Brophy Gillespie](#)

For SMEs, phishing is especially dangerous because **a single click by an employee can bypass whatever defences are in place.**

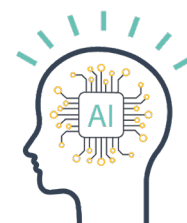
SMEs without extensive cybersecurity training programs are seen as prime targets. Social engineering attacks are highly targeted, criminals often research small companies’ LinkedIn accounts and impersonate key personnel or suppliers to maximise credibility.

Social engineering ploys exploit the fact that SMEs might not have strict verification processes for payments or may have a small finance team under pressure to act quickly.



## AI-Driven Cyber Attacks: The Next Frontier of Digital Crime

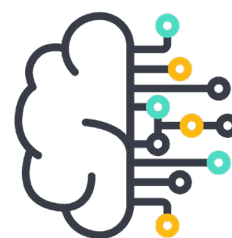
Artificial intelligence (AI) is a double-edged sword in cybersecurity. On one hand, AI technologies can help defenders by **automating threat detection** and analysing anomalies. On the other, cybercriminals are leveraging AI to launch more sophisticated attacks. UK SMEs rank AI-driven attacks as their top emerging concern in 2025.



AI driven attacks include the use of generative AI to craft convincing phishing emails, deepfake technology for impersonation, and AI powered malware that can adapt or evade detection. For instance, AI can quickly scrape an SME's public online footprint (website text, social media) to generate **spear-phishing** messages that are uniquely tailored to the business and its employees, increasing the likelihood of success. Attackers have even begun using AI chatbots to engage targets in real-time social engineering, and AI tools can assist in discovering vulnerabilities or automating the search for weak passwords.



In one survey, over a third of UK SMEs voiced worry that **AI-enabled attacks** pose a significant new threat to their operations. Cybersecurity experts advise that for now AI is mostly an "enabler for existing threats" rather than a completely new category of attack. AI raises the volume of attacks an SME might face. Compounding the issue, many SMEs are still unfamiliar with AI's implications and they may not have the expertise to distinguish an AI-generated scam from a real communication.



## Insider Threats: When the Danger Comes from Within

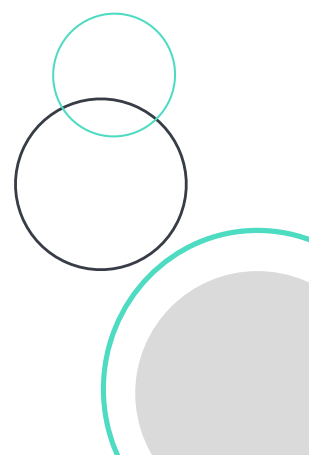
Not all threats come from anonymous external hackers; sometimes the danger is on the inside. Insider threats involve security risks posed by a company's own employees or other insiders (contractors, partners with access). The NCSC estimates that about **one in four data breaches** in the UK are caused by human error (often insiders making mistakes).



This can be malicious, such as a disgruntled employee stealing data or sabotaging systems, or inadvertent, such as an employee **accidentally leaking sensitive information** or falling for a scam that compromises the network. A well-meaning staff member might misconfigure a cloud storage bucket, leaving customer data exposed, or use weak passwords that get cracked, providing an entry point. There have also been cases where former employees retain access to systems after leaving – if their account is not promptly revoked this can become a way in to the systems.



While insider threats did not rank in the very top tier of SME concerns in surveys, they still present a significant danger. For SMEs, every employee typically has broad access and wears multiple hats, which can increase insider risk. **SMEs can be particularly vulnerable** because they often operate on high trust with less formal security oversight. SMEs are advised to follow the principle of least privilege where each employee has only the minimum access necessary for their role.



## Supply Chain Vulnerabilities: The Hidden Risks in Your Business Network

In today's interconnected economy, SMEs rarely operate in isolation – they rely on vendors, cloud providers, software suppliers, and partners. This interconnectedness introduces supply chain vulnerabilities, where a weakness in one link of the chain can compromise the entire network of businesses.

Attackers have learned that instead of directly targeting a well-defended company, it can be **easier to breach a smaller supplier** or service provider and use that as a foothold to infiltrate the larger target.

From an SME perspective, being that weaker link is a serious concern: cybercriminals view small firms as “soft targets” and potential gateways into bigger organisations. **77% of UK SMEs do not maintain any in-house cybersecurity personnel** and often these SMEs enjoy trusted network connections with their enterprise clients – a combination that attackers find attractive.

Many SMEs lack the capacity to thoroughly vet the security of each third-party service or to apply patches immediately, which leaves them exposed.

**SMEs must scrutinise the security of their partners** and providers. A

vulnerability in a third-party can quickly become an incident for the SME. Likewise, larger organisations are increasingly demanding that their SME suppliers adhere to certain cybersecurity standards.

A large retail breach in 2013 occurred when attackers compromised a small HVAC subcontractor (with far weaker IT security) and used those credentials to penetrate the larger corporate network. That attack led to the theft of millions of customer card details and tens of millions of dollars in damages – all traced back to a third-party SME vendor being hacked via a phishing email.

[Target attack with long lasting consequences.](#)



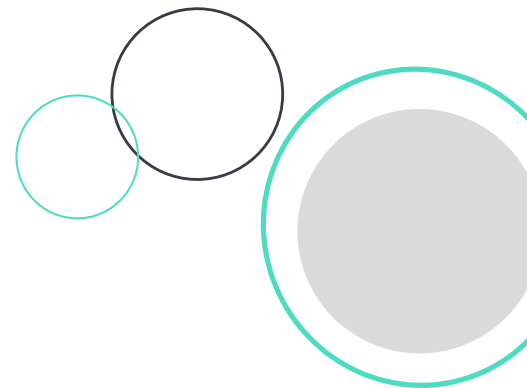
## Part Two: Why SMEs Are Prime Targets, And How to Fight Back

While facing the breadth of threats, SMEs often have **inherent disadvantages in cybersecurity** that make them more vulnerable than large enterprises. Smaller companies rarely have dedicated cybersecurity teams. It's common to have just a handful of IT generalists, or to entirely outsource IT support. This leads to a lack of skills and resources to adequately address all cyber threats. Without expertise, they may not stay current on emerging threats or best practices.

SMEs face enterprise-grade threats with far fewer defences. Cybercriminals are aware of this mismatch, which is why they have been intensifying their focus on small and mid-sized targets. **No SME is too small for a big attack**, quick and informed response is crucial, and preventative measures (whether technical controls or employee training) often spell the difference between a close call and a catastrophe.

By being aware of, and implementing changes around the areas discussed in the next part of this report, **SMEs can prevent or blunt most common attacks**. Investing in the right tools and configurations can significantly reduce an SME's exposure to cyber attacks however having tools alone is not sufficient, they must be supported by sound operational practices.

This is where a high quality Managed Service Provider (MSP) comes in, by outsourcing your IT to the right MSP you get a **full team of cybersecurity experts** who keep your IT estate secure, ensuring that all vulnerabilities are reduced and issues are picked up quickly.



## Weaker Defences: Why SMEs Are Easy Prey for Hackers

Budget constraints mean SMEs might not invest in the latest security tools or infrastructure. Basic protections like up-to-date firewalls, intrusion detection, and endpoint monitoring may be missing or outdated. A recent study suggests that **69% of UK SMEs do not have a formal cybersecurity policy** in place. This patchy “cyber hygiene” leaves holes that attackers can exploit. By investing in the basics and taking the time to consistently review your systems you will be more likely to catch any weaknesses and resolve those weaknesses before they become a threat.



Ensure that a business-grade firewall is installed and properly configured to block unauthorised access. **Use reputable anti-virus/anti-malware software** on all computers and servers, and keep it updated. SMEs should also consider segmenting their internal networks, separating critical servers or sensitive data networks from general workstations, means that even if an attacker breaches one segment, they cannot freely roam the entire IT environment.



**Use encryption to protect sensitive data** at rest and in transit. Full-disk encryption (e.g. BitLocker on Windows, FileVault on Mac) ensures that if a laptop is lost or stolen, the data remains unintelligible to anyone without the key. Encryption of databases or at least specific fields (like customer personal data) adds safety even if an adversary gains access.



Implement MFA for email, remote logins, and any critical systems. Stolen or weak passwords are behind many breaches. **MFA adds an extra verification step** (like an app code or SMS text) that drastically reduces the chance that a compromised password alone leads to a breach.



Deploy logging and monitoring solutions to **catch suspicious activity early**. Even if an SME can't have a 24/7 security operations centre, there are managed detection and response (MDR) services or simpler log alerting tools that will notify administrators of red flags.



Keep all software and systems updated with the latest security patches. Many attacks (including ransomware and supply chain breaches) exploit known vulnerabilities in unpatched systems. SMEs should **turn on automatic updates** wherever possible and where automatic update isn't feasible, establish a routine to apply patches. Remember it's not just Windows that needs updating – third party software, network devices such as firewalls, router and switches, all need to be part of your weekly maintenance plan.

By having the right MSP in place these processes should be taken care of, meaning you will not have to worry about holes in your defences being exposed to criminals.



## Cyber Awareness & Training: Your First Line of Defence

Many small business owners and employees underestimate cyber risks with a third of SME CEOs feeling confident that a cyber-attack wouldn't disrupt their business. Half of SMEs say they would not know how to respond if an attack occurred. **Untrained staff are prone to click on phishing emails or use poor passwords**, inadvertently opening the door to attackers. In smaller companies, employees often juggle roles and may not prioritise security amidst other duties. Cyber awareness tends to be informal at best, which is not enough given the sophisticated social engineering tactics in play. Employee training is arguably one of the most critical elements of an organisation's defence. Training staff once does not provide enough protection against cybercrime.



The Information Commissions Office issued guidance in 2021 saying that they expected that all staff and volunteers that have access to data, should receive cyber awareness training as part of their induction, **within 30 days of starting** and before the employee is granted access to any databases containing personal or sensitive data.



SMEs should conduct **regular cybersecurity awareness training** for all employees, at least annually, with brief refreshers or updates more frequently.



Training should cover how to **recognise phishing emails**, proper handling of sensitive information, use of strong passwords and password managers, and policies on acceptable use of work devices.



**Interactive phishing simulations** can be very effective: employees receive fake phishing emails sent by an internal test system, and those who click can be gently coached on what warning signs they missed.

Human error is a leading cause of breaches, so educating staff is arguably the single most important operational defence. The aim is to create a culture where employees **"stop and think"** before clicking unknown links or divulging information and feel responsible for the company's security. An MSP will be able to provide you with comprehensive, ongoing training scaled up or down as your business needs.



## High Trust, Low Oversight: Why SMEs Need Tighter Security Controls

SMEs often operate with a **tight-knit culture of trust**. They may not enforce strict access controls or separation of duties the way a bank or large corporate would. For example, an SME might have a single employee who can approve large payments, administer user accounts, and handle IT support – a convenience that unfortunately also creates a single point of failure if that account is compromised.

Many small firms also allow wide access to data across the company for efficiency's sake, which means if any user is breached, a hacker could pivot to sensitive systems easily. This "flat" network structure (versus segmented networks) **magnifies the damage from intrusions**. By being vigilant about locking down systems and only allowing access as necessary you have a better chance of keeping your data and your systems safe.

Regularly review staff's access especially if they change roles or departments. When staff members leave ensure their access to your systems is removed immediately.

Each quarter, SMEs should audit which employees have admin rights, remote access, or access to sensitive data, and revoke any access that is not necessary for their job role.

Use the principle of least privilege by reviewing user access rights regularly. Use separate accounts for admin tasks versus regular work, even for IT staff, to reduce risk.

A security focussed MSP will be able to handle the back office admin of permissions, set up and shut down access easily and ensure that new starters, movers and leavers have their access adjusted as needed.





## Regulatory & Customer Pressures: Compliance Isn't Optional

While not exactly a vulnerability, it's worth noting SMEs are increasingly subject to the same data protection regulations as big firms (e.g. UK GDPR). Many struggle to comply due to limited knowledge, which **can lead to fines** or mandated corrective actions after a breach, adding an extra financial hit after an incident.



Cyber insurance, which could be a safety net, is often not carried by SMEs; over half of UK SMEs have **no cyber insurance in place**. The absence of insurance may also reflect that some SMEs haven't taken baseline steps needed to qualify for affordable coverage.



While obtaining cyber insurance is a policy/financial decision, operationally it requires meeting certain criteria and having an **appropriate incident response plan**. Cyber insurance can provide access to incident response experts, legal advice, and financial coverage for losses.



Carrying certificates like Cyber Essentials can be a helping hand in securing reliable, affordable cyber insurance. The main objective of the **Cyber Essentials assessment** is to determine that your organisation has effectively implemented the controls required by the Scheme, in order to defend against the most common and unsophisticated forms of cyber-attack.

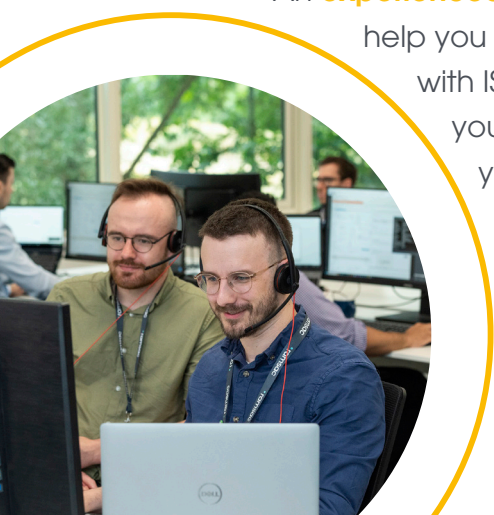


Develop and maintain an incident response (IR) plan that outlines the steps to take if a cyber incident is suspected. This plan should designate roles such as who calls the IT provider? Who communicates with customers if data is compromised? Who has authority to shut down systems to contain an attack? and provide a checklist of actions for various scenarios. **Practice the plan regularly** to ensure everyone knows their roles and the details are constantly kept up to date.



ISO 27001 is a globally recognised standard for managing information security. It helps SMEs create structured security policies and procedures, reducing risk and improving data protection. Achieving **ISO 27001 certification** shows clients and insurers that robust cybersecurity practices are in place.

An **experienced MSP** will be able to assist you to draft an Incident Response Plan, help you reach Cyber Essentials or Cyber Essentials Plus and support you with ISO 27001 implementation and compliance, which can help you to gain the right level of Cyber Insurance coverage for your business. Giving you a little more comfort that you are protected if you were the subject of a cyber threat.



## The Role of Policies in Strengthening Cyber Defences

Policy-based measures set the framework within which technical and operational controls operate. They ensure that cybersecurity is embedded in the organisation's governance and that the company meets **legal and regulatory obligations**. For SMEs, developing clear security policies and aligning with industry standards can significantly improve resilience and build trust with customers and partners. Key policy-based checks include:

**Cybersecurity Policy:** Every SME should have a formal written cybersecurity policy (or a set of policies) that outline how the company manages and protects information. Shockingly, **69% of UK SMEs have no formal cybersecurity policy** at all, often resulting in ad hoc and inconsistent practices. A cybersecurity policy doesn't need to be hundreds of pages; it can be a concise document covering areas like acceptable use of company devices, password requirements, data handling procedures, incident reporting, and so on.



The process of writing a policy itself often reveals gaps and helps set expectations for employees. Once established, ensure all staff read and acknowledge the policy. Update it at least annually or whenever significant changes occur.

### Compliance with Regulations (e.g. UK GDPR, Data Protection Act)

SMEs must comply with data protection laws if they handle personal data. The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 mandate **safeguarding personal identifiable information** and reporting breaches to authorities within 72 hours if they pose risk to individuals' rights. Compliance means knowing what personal data you hold, ensuring its security (both technical and organisational measures), and not retaining data longer than necessary. SMEs should conduct basic data mapping and risk assessments for the personal data they process. Non-compliance can result in hefty fines – but beyond avoiding penalties, following these regulations inherently guides a company to better security practices.



### Governance and Leadership

**Involvement:** Cybersecurity should have leadership oversight, not just be an IT afterthought. In practice, this means someone at the management level should be responsible for cybersecurity strategy and risk, even if they're not a technical expert. It could be an executive or the business owner themselves. Regularly include cybersecurity as an agenda item in management meetings – discussing recent incidents, needed investments, or policy approvals. Some SMEs create a role of **"Security Champion"** – not a full-time position, but an existing staff member with an extra duty to liaise on security matters and keep momentum. The tone from the top matters: if leadership emphasises security, employees are more likely to follow suit.



## The Role of Policies in Strengthening Cyber Defences (cont)

### Third-Party/Supply Chain

**Security Policy:** Develop policies or guidelines about engaging with third-party vendors from a security standpoint. This could involve requiring contracts to include data protection agreements, setting up Non-Disclosure Agreements (NDAs) when giving contractors access to sensitive info, and having criteria for selecting tech suppliers. In sectors like defence or critical infrastructure, formal supplier vetting is required; even if not mandated for your SME, adopting a scaled-down **vetting for your key suppliers** is wise. Essentially, treat your suppliers as an extension of your enterprise and insist on certain standards, even if it's just verbal confirmations.



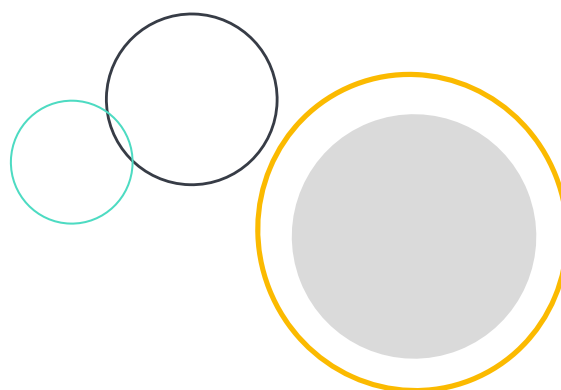
### Data Breach Response and

**Notification Policy:** Hand-in-hand with the incident response plan, have a clear policy on how to handle data breaches, especially regarding notification. Under UK law (GDPR), if a personal data breach occurs that risks people's rights/freedoms, you must notify the Information Commissioner's Office (ICO) within 72 hours and possibly affected individuals. The policy should define what constitutes a notifiable breach and assign responsibility for making that decision and drafting notifications. Many SMEs are unsure of legal requirements and delay breach reporting, which can **worsen penalties and reputational damage**. Being prepared with a policy and even template notifications accelerates the response.



Implementing these policy-based measures creates a strong foundation for cybersecurity. They ensure that there is organisational clarity and commitment to security. In an environment where cybersecurity is increasingly a factor in B2B relationships, having these governance pieces in place can be a competitive advantage for an SME. Cyber threats evolve quickly, so policies should not be static. SMEs should periodically assess their cyber risks and update policies accordingly. **Treating cybersecurity as an ongoing business risk** similar to market or financial risks will help you to stay ahead of the cyber criminals and be prepared.

If you have an MSP in place they may be able to support you in writing Cyber based policies to ensure all the important points are hit and you have coverage for all possible eventualities.





## Industry Leadership & Best Practices:

The SME community in the UK is slowly but surely raising its cybersecurity game, aided by guidance and tools from both government and private sector leaders. Best practices such as implementing layered defences, fostering a security-aware culture, leveraging managed services, and continuously testing oneself are becoming more commonplace. Many UK SMEs now recognise that **cybersecurity is a business enabler**. By protecting themselves, they not only avoid losses but also gain credibility and trust in the marketplace. The proactive stance of these leading SMEs serves as a blueprint for others to follow, ensuring that being “small” does not equal being “soft” on security.

Partnering with a Managed Service Provider (MSP) offers SMEs access to expert cybersecurity services, including proactive monitoring, threat detection, and **rapid response to incidents** which will help keep them ahead of the curve. MSPs provide tailored solutions that align with the specific needs and budget of SMEs, ensuring robust protection without the need for extensive in-house resources. By leveraging the expertise of an MSP, SMEs can focus on their core business activities while maintaining confidence in their cybersecurity posture.





# About ramsac

## ramsac: The secure choice for IT & cybersecurity

ramsac is the secure choice for organisations that want reliable, proactive IT support and robust cyber protection — all delivered with clarity, care, and a personal touch.

We help businesses and charities stay safe, productive, and focused on what they do best, by taking the stress out of managing technology. Our services include fully managed IT support, Microsoft 365 expertise, cloud infrastructure, and strategic IT leadership — underpinned by cutting-edge cybersecurity solutions.

With round-the-clock monitoring, real-time threat response, and 24/7 protection from cyber breaches, our clients trust us to keep their systems secure and their data safe. We don't just react — we predict, prevent, and protect.

**At ramsac, we believe technology should empower, not overwhelm. That's why we deliver IT that's secure, simple, and always on your side.**



## ● Get in touch

For information on **cybersecurity services from ramsac** please contact us on **01483 412040**, email **info@ramsac.com** or visit **ramsac.com**

ramzac Limited

[www.ramsac.com](http://www.ramsac.com)

01483 412 040

  
the secure choice