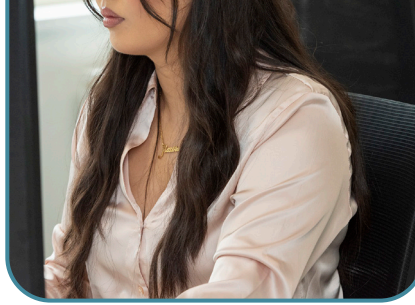




# UK Cybersecurity Threat Report 2026

Real-world threat insight and the security basics that protect modern organisations

# UK Cybersecurity Threat Report 2026

## Contents

|                                                    |           |
|----------------------------------------------------|-----------|
| • Executive summary                                | 3         |
| <b>Part one: The risk facing UK SMEs in 2026</b>   | <b>4</b>  |
| • Cybersecurity as a business risk in 2026         | 4         |
| • The cyber threat landscape facing UK SMEs        | 5         |
| • Why SMEs are prime targets                       | 6         |
| <b>Part two: The fundamentals that reduce risk</b> | <b>7</b>  |
| • Cybersecurity fundamentals that still matter     | 7         |
| • People, culture, and awareness                   | 7         |
| • Creating and improving your cybersecurity policy | 8         |
| • Practical cybersecurity tips for UK SMEs         | 9-10      |
| <b>Part three: Incident response and recovery</b>  | <b>11</b> |
| • What to do if you have been breached             | 11        |
| • Looking ahead: Building resilience beyond 2026   | 12        |
| • Bringing it all together with totalIT secure     | 12        |

## Executive summary

Cybersecurity is now a critical business issue for UK small and medium-sized enterprises. As organisations adopt cloud services, remote working, and digital supply chains, cybercriminals are increasingly targeting SMEs as attractive, low-resistance entry points. Key findings shaping the 2026 cybersecurity landscape include:

- Around half of UK businesses have experienced a cyber breach or attack in the past year.
- Phishing and social engineering remain the most common causes of incidents, exploiting time pressure and human trust.
- Ransomware continues to cause severe operational disruption, with attackers increasingly stealing data before encryption.
- AI-driven attacks are increasing the volume, speed, and realism of cybercrime, making scams harder to detect.
- Customers, regulators, and insurers now expect demonstrable cybersecurity controls as a condition of doing business.

This white paper combines current threat intelligence with practical guidance to help UK SMEs understand today's risks and apply proven cybersecurity fundamentals to reduce exposure in 2026 and beyond.



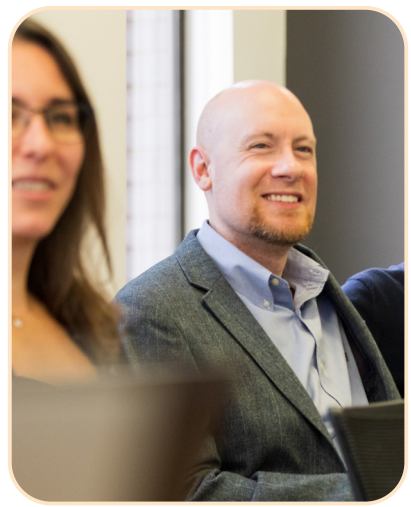
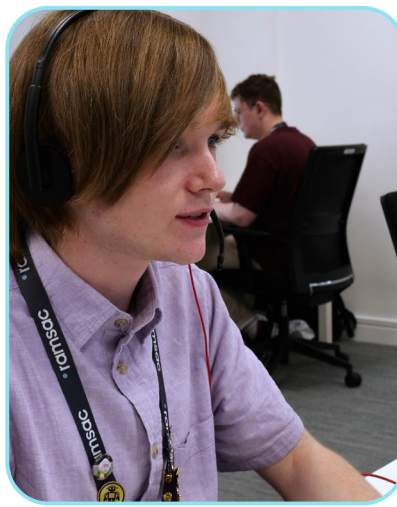
# Part One: The Risk Facing UK SMEs in 2026

## Cybersecurity as a business risk in 2026

Small and medium-sized enterprises form the backbone of the UK economy, but this also makes them a prime target for cybercriminals. In recent years, attackers have shifted focus away from only large enterprises and towards SMEs that often lack specialist security resources yet hold valuable data and trusted connections.

Cyber attacks are no longer rare or hypothetical events. They routinely disrupt operations, halt productivity, and damage customer confidence. For many organisations, the financial and reputational consequences of a serious incident can outweigh the cost of preventative security measures.

In 2026, cybersecurity should be viewed as a core component of business resilience. This white paper explores the threats UK SMEs face today and explains how focusing on strong fundamentals across people, process, and technology can significantly reduce risk.



## The cyber threat landscape facing UK SMEs

The threat landscape confronting SMEs has grown more complex and aggressive. Attacks are faster, more targeted, and increasingly automated.

Ransomware remains one of the most damaging threats to UK businesses. Modern ransomware attacks often involve so-called “double extortion”, where attackers steal sensitive data before encrypting systems. This places organisations under pressure not only to restore operations, but also to prevent confidential information from being leaked.

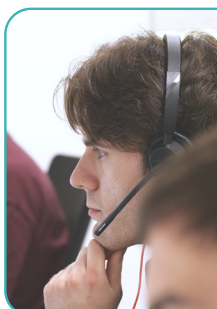
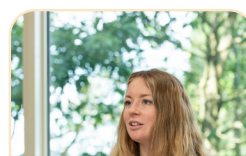
Phishing and social engineering continue to be the most common entry points for attackers. Emails impersonating suppliers, colleagues, or senior leaders are designed to trigger urgent action, such as approving payments or sharing login details. For SMEs with lean teams and informal processes, a single convincing message can bypass technical controls.

Artificial intelligence is amplifying these risks. AI is being used to generate highly realistic phishing messages, automate reconnaissance, and even impersonate individuals using deepfake technology. While AI also benefits defenders, its use by criminals significantly increases the volume and sophistication of attacks faced by SMEs.

Insider threats, both accidental and malicious, remain a significant concern. Human error, misconfiguration of systems, and excessive access privileges can expose data or create opportunities for compromise. Supply chain attacks further compound this risk, as attackers increasingly target smaller suppliers to gain access to larger organisations.

### Key takeaways for SMEs

- Most attacks exploit common weaknesses rather than advanced technical flaws.
- Human behaviour and identity compromise are central to many incidents.
- Third-party and supply chain risk is now a mainstream threat, not an edge case.



# Why SMEs are prime targets

SMEs face enterprise-grade threats with far fewer resources.

Many SMEs operate without dedicated cybersecurity specialists, relying on small IT teams or outsourced support. This can limit visibility into emerging threats and delay response when incidents occur.

High levels of internal trust, while beneficial for culture and efficiency, can also increase risk. Broad access permissions, limited segregation of duties, and informal approval processes make it easier for attackers to move laterally once a single account is compromised.

At the same time, regulatory and customer expectations continue to rise. Data protection obligations under UK GDPR apply equally to SMEs, and many customers now require evidence of cybersecurity controls as part of supplier onboarding. Cyber insurance providers are also raising baseline requirements, making security maturity a commercial necessity.

## Key takeaways for SMEs

- Being small does not reduce your attractiveness as a target.
- Trust-based operating models must be balanced with appropriate controls.
- Cybersecurity is increasingly linked to compliance, insurance, and revenue protection.



# Part two: The fundamentals that reduce risk

## Cybersecurity fundamentals that still matter

Despite the changing threat landscape, the fundamentals of effective cybersecurity remain consistent. Organisations that focus on these core principles are far better placed to prevent incidents and recover quickly when issues occur.

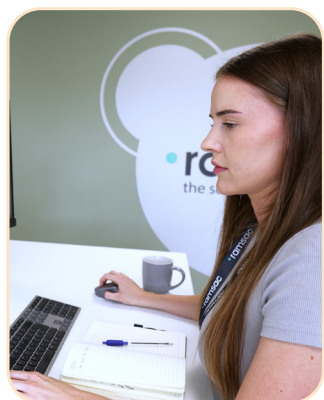
**Strong governance** ensures that cybersecurity is actively managed rather than left to chance. Clear policies, defined responsibilities, and regular risk reviews create accountability and consistency.

**Understanding what assets need protection** is equally important. This includes devices, users, data, cloud services, and third-party connections. Without this visibility, security controls are inevitably incomplete.

**Protective controls** should focus on reducing the most common attack paths. In 2026, this typically includes strong identity and access management, multi-factor authentication, secure system configuration, timely patching, and reliable backups.

**Detection capabilities** allow organisations to identify suspicious activity early. Centralised monitoring across endpoints and cloud platforms improves response times and limits damage.

Finally, no organisation can prevent every incident. Having a tested response and recovery plan ensures that systems can be restored quickly, regulatory obligations are met, and lessons are learned.



### Key takeaways for SMEs

- Fundamentals reduce risk more effectively than isolated security tools.
- Identity, visibility, and recovery planning are critical focus areas.
- Preparation significantly limits the impact of inevitable incidents.

## People, culture, and awareness

Human behaviour remains one of the most influential factors in cybersecurity. Untrained or overconfident employees are more likely to fall victim to phishing, reuse passwords, or mishandle sensitive information.

Effective security awareness training in 2026 must be ongoing, relevant, and practical. Employees should understand how attacks present themselves in real scenarios and feel confident reporting concerns early.

Creating a culture where cybersecurity is seen as a shared responsibility improves both prevention and response. Organisations that invest in people as well as technology consistently experience fewer and less severe incidents.

# Creating and improving your cybersecurity policy

A clear, well-maintained cybersecurity policy provides the foundation for consistent, effective security across the organisation. For many SMEs, policies are either missing, outdated, or overly technical, which reduces their effectiveness.

A good cybersecurity policy should be practical, proportionate, and clearly understood by staff. It does not need to be lengthy, but it does need to be relevant to how your organisation actually operates.

## What a strong cybersecurity policy should cover



**Roles and responsibilities** - who is accountable for decision-making, cybersecurity, and incident escalation.



**Remote and mobile working** - expectations for securing laptops, home networks, and mobile devices.



**Acceptable use** - how company devices, systems, and data should (and should not) be used.



**Third-party and supplier access** - how external access is approved, reviewed, and removed.



**Password and authentication standards** - including the use of strong passwords and multi-factor authentication.



**Incident reporting** - how staff should report suspected security issues or breaches



**Data handling and protection** - how sensitive and personal data is stored, shared, and disposed of.

## Tips for improving your cybersecurity policy

When developing or refining a cybersecurity policy, it is important to keep the language clear and non-technical so it can be easily understood by all staff, not just IT specialists. The policy should be aligned with recognised frameworks such as Cyber Essentials or ISO/IEC 27001 to ensure it reflects established good practice. Policies should be reviewed and updated at least annually, and whenever there is a significant incident or material change to the business, to ensure they remain relevant. All employees should be required to read and formally acknowledge the policy as part of onboarding and through regular refreshers, reinforcing its importance. **Above all, the policy should be treated as a living document, supported by ongoing training and visible leadership engagement, rather than a one-off compliance exercise.**



# Practical cybersecurity tips for UK SMEs

For most organisations, improving cybersecurity does not require complex technology or specialist knowledge. Small, consistent actions taken by individuals and teams can significantly reduce risk. The guidance below consolidates practical, everyday steps into three key areas that are most relevant to UK SMEs.

## Online security and safe behaviour



**Many cyber incidents begin with a deceptive website, email, or message. Developing cautious online habits is one of the most effective ways to prevent attacks.**

- ✓ Be cautious of emails from unfamiliar senders, messages requesting personal or financial information, or communications that create urgency or fear to prompt quick action.
- ✓ Check for “https” when visiting unfamiliar websites to confirm the connection is secure.
- ✓ Learn how to recognise spoofed or impersonated emails and remain alert to subtle warning signs.
- ✓ Avoid clicking on pop-ups or entering personal details into them.
- ✓ Trust your instincts when browsing or reading emails. If something feels wrong, avoid interacting with it and report it where appropriate.
- ✓ Use strong, unique passwords and consider using a reputable password management tool to reduce password reuse.
- ✓ Keep web browsers, operating systems, and applications up to date, installing security updates as soon as they are available.

## Securing devices and equipment



**Laptops, mobile phones, tablets, and removable media can all introduce risk if they are lost, stolen, or poorly secured. Whether devices are company-owned or personally owned, basic precautions make a significant difference.**

- ✓ Only take work devices with you when travelling if necessary, and keep them with you whenever possible.
- ✓ Lock devices with a strong PIN or password and enable features that allow devices to be located or wiped remotely if lost or stolen.
- ✓ Clear all data securely before disposing of, selling, or reusing devices.
- ✓ Avoid rooting or jailbreaking devices, as this weakens built-in security controls.
- ✓ Only install software and apps from trusted, legitimate sources.
- ✓ Back up data regularly to protect against loss or ransomware.
- ✓ Avoid using public Wi-Fi where possible. If it must be used, connect through a VPN and limit access to sensitive systems.
- ✓ Never connect unknown USB devices to company equipment without approval from IT.

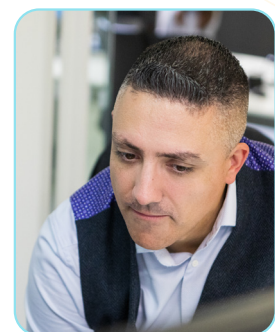
# Physical security and ways of working



Cybersecurity is closely linked to physical security and everyday working practices. Simple behaviours in the office and when working remotely can prevent data loss and unauthorised access.

- ✓ Be aware of who is entering and leaving your workplace, and challenge unfamiliar individuals politely where appropriate.
- ✓ Use visitor sign-in procedures and identification badges where possible.
- ✓ Lock screens whenever you leave your desk and avoid leaving devices unattended.
- ✓ Keep valuables and sensitive information out of sight and stored securely.
- ✓ Do not share access cards, keys, or login credentials.
- ✓ Clear meeting rooms after use, including whiteboards and flipcharts that may contain sensitive information.
- ✓ When working remotely, only connect to trusted networks, minimise sensitive data stored locally, and use full disk encryption where possible.

By embedding these simple practices into daily routines, SMEs can significantly reduce their exposure to common cyber threats without adding unnecessary complexity.



# Part three: Incident response and recovery

## What to do if you have been breached

Even with strong controls in place, no organisation can guarantee it will never experience a cyber incident. Having a clear, rehearsed response plan can significantly reduce the impact of a breach.

If you suspect your organisation has been compromised:



**Act quickly but calmly** – do not ignore early warning signs or attempt to hide the issue.



**Contain the incident** – isolate affected systems or accounts by disconnecting them from the network/internet to prevent further spread (do not turn off the machine).



**Preserve evidence** – avoid wiping systems unless advised, as logs and data may be needed for investigation.



**Notify the right people** – escalate internally and contact your IT or cybersecurity provider immediately.



**Assess data impact** – determine whether personal or sensitive data has been accessed or exfiltrated.



**Meet regulatory obligations** – if personal data is involved, UK GDPR may require notification to the ICO within 72 hours.



**Communicate carefully** – ensure any internal or external communications are accurate and consistent.

### Learning from incidents

- Conduct a post-incident review to understand what happened and why.
- Update policies, controls, and training based on lessons learned.
- Test and refine your incident response plan regularly.

# Looking ahead: Building resilience beyond 2026

Cybersecurity is not a one-off project or a compliance exercise. Threats will continue to evolve, and organisations must adapt accordingly.

By combining an understanding of the threat landscape with strong cybersecurity fundamentals, UK SMEs can reduce risk, protect their reputation, and operate with greater confidence. In an environment where trust and resilience increasingly influence commercial decisions, cybersecurity has become a business enabler rather than a barrier.

## Bringing it all together with totalIT secure

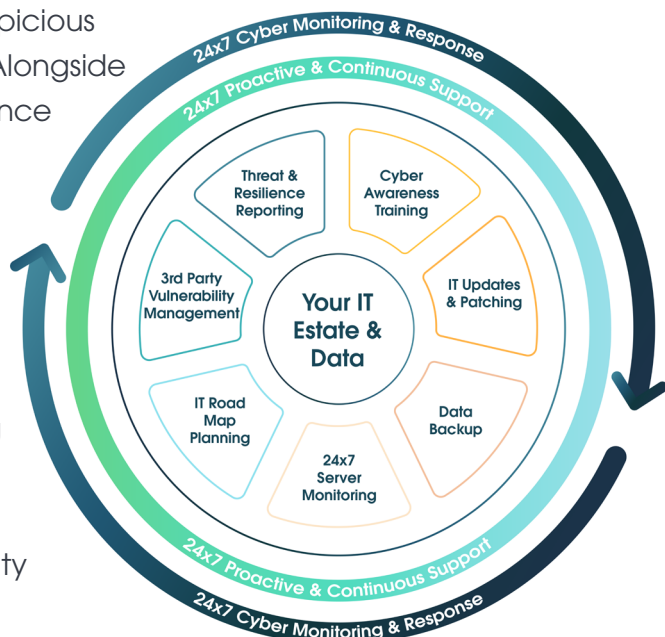


**totalIT secure** is ramsac's managed cybersecurity framework designed to help UK SMEs put the principles outlined in this white paper into practice. Rather than relying on disconnected tools or ad-hoc processes, totalIT secure brings together people, process, and technology into a structured, continuously managed approach.

The service focuses on reducing real-world risk by addressing the most common attack paths facing SMEs. This includes strengthening identity and access controls, maintaining secure system configuration and patching, monitoring for suspicious activity, and ensuring reliable backup and recovery. Alongside the technical controls, **totalIT secure** supports governance through policy development, user awareness training, and regular review of cybersecurity posture.

**totalIT secure** is designed to be proportionate and practical. It recognises that most SMEs do not need enterprise-scale security teams, but they do need clarity, consistency, and expert oversight. By providing ongoing monitoring, guidance, and support, **totalIT secure** helps organisations move away from reactive firefighting towards a more resilient, predictable security posture.

For organisations looking to strengthen their cybersecurity in line with evolving threats and expectations, **totalIT secure** provides a clear path from understanding risk to actively managing it.



# About ramsac

Since 1992, ramsac has been helping organisations thrive with secure, reliable technology.

We are proud to be different. We are a people-first business, committed to making IT simple, jargon-free and friendly. We are independent consultants, offering advice based on your needs, not on sales targets. And we are focused on long-term relationships, with many clients trusting us for over 20 years.

Our commitment to quality is backed by ISO 9001, ISO 27001 and Cyber Essentials Plus certifications, and we are proud winners of multiple national and regional business awards. Most importantly, we have been recognised as a Best Companies 3 Star World Class Employer, proof that our team love what they do, and that passion shows in the service we deliver.



## ● Your Technology. Our Responsibility

If you would like support reviewing your cybersecurity posture or strengthening your resilience for 2026 and beyond, the ramsac team is here to help.

Speak to us about your organisation's cybersecurity.

Call **01483 412040**, email **[info@ramsac.com](mailto:info@ramsac.com)** or visit **[www.ramsac.com](http://www.ramsac.com)**