Common IT Mistakes UK Small Businesses Make

Why UK SMEs Keep Getting IT Wrong

- The majority of small and medium-sized enterprises in the UK view IT as a transaction, but not a priority as the day-to-day business activities take precedence.
- Because of a lack of time and attention, many small and medium-sized enterprises (SMEs) make mistakes that are costly in terms of time, money and reputation.
- SMEs also typically have very limited budgets for IT (5% or less of overall revenue) and do not have dedicated IT professionals.
- Many SMEs typically only address IT problems after they have occurred, and not before.
- As of 2025, 43% of UK businesses have experienced at least one cyber-attack, making it vital to have preventative measures taken regarding IT.
- In the event of a small data error, fines can be issued under GDPR regulations, starting at £1,000; this imposes additional risk for SMEs.
- If an employee's laptop is unpatched, this small neglect could lead to an infection by ransomware, halting business operations.
- 95% of all IT errors can be solved with straight forward, inexpensive adjustments.
- This document will help companies track and enforce confident, strong IT practices.

1. Weak Passwords and Password Reuse

What it looks like

- Staff using their same password for different accounts on different platforms. Ex: Email, Payroll, CRM, etc.
- Using a password like “Summer2026!”
- Using shared passwords on an Excel sheet.

Why it’s a problem

Password reuse is the primary point of entry used by an attacker to compromise accounts. If a single site is compromised, a thief will attempt to reuse that password to access other sites Microsoft 365 being the most common.

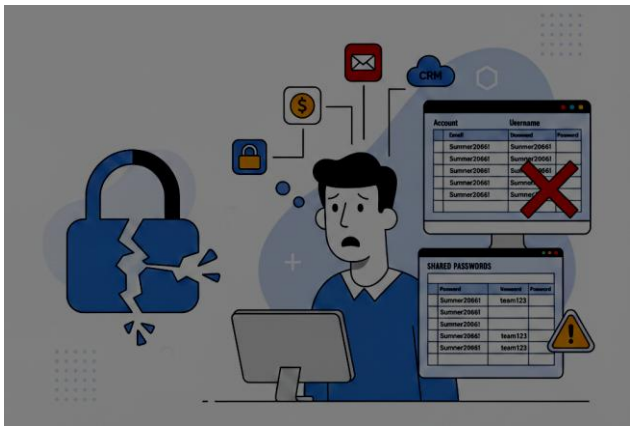
UK GDPR defines careless failure to prevent the compromise of your account as having insufficient protection of your account.

How to fix it

- Implement a corporate password manager.
- Implement long pass-phrases (3 random words).
- Have a strict "No password sharing" policy.
- Implement role-based access instead of shared logins.

UK Scenario:

A 12-person consulting company reused the same password for their LinkedIn and Microsoft 365 accounts. LinkedIn was breached. Their email was compromised. The company suffered an invoice redirection fraud loss of £18,000.



2. No Multi-Factor Authentication (MFA)

What it looks like

- Microsoft 365 accounts secured with only a password.
- Directors refusing multi-factor authentication due to it being, "annoying."

Why it’s a problem

Without MFA, a thief can instantly access all of your accounts if they have your password.

More and more, cyber insurance policies are requiring you to have MFA in place for:

- Email accounts
- Remote access
- Administrative accounts

MFA is also mandated under the Cyber Essentials Scheme.

How to fix it

- Your organisation should enforce MFA for ALL users.
- Whenever possible, use an App-Based Authentication system rather than an SMS.
- Implement stricter controls around Administrative Accounts.

MFA reduces the risk of account compromise by more than 90%.

3. Outdated or Unpatched Systems

What it looks like

- Windows devices months behind on updates.

- Old on-premise servers never rebooted.
- “We can’t update because the software might break.”

Why it’s a problem

Most ransomware exploits known vulnerabilities with available patches.

Unpatched systems are considered negligence in many breach investigations.

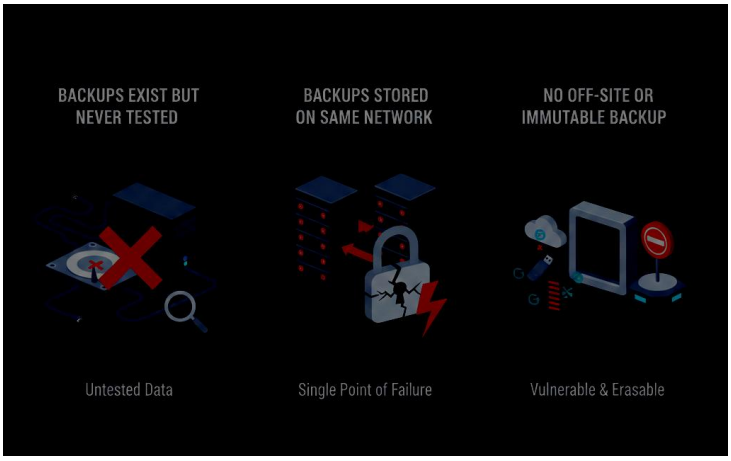
How to fix it

- Enable automatic updates.
- Schedule monthly patch reviews.
- Replace unsupported hardware.

4. Poor Backup Practices

What it looks like

- Backups exist but are never tested.
- Backups stored on the same network.
- No off-site or immutable backup.



Why it’s a problem

Many SMEs only discover backup failure during a ransomware attack.

If backups are encrypted too, recovery becomes impossible.

How to fix it

Follow the 3-2-1 rule:

- 3 copies of data
- 2 different media
- 1 off-site

Test backups quarterly.

UK Scenario:

A 25-person construction firm believed their NAS was backing up daily. It hadn’t worked in six months. A server failure meant permanent loss of project drawings.

5. Misconfigured Microsoft 365 or Cloud Settings

What it looks like

- There are no Conditional Access Policies
- Individuals posses Global Admin permissions
- Shared files have "Anyone with a link" access permission

Why it’s a problem

Cloud-based services provide a secure platform. However if not correctly configured they can become a liability.

Default settings are generally not set up for the SME company's level of risk associated with security.

How to fix it

- Limit the number of Admin accounts
- Implement Security Baselines
- Review the Company Policy for shared files
- Review Sign-In logs

6. Ignoring Cybersecurity Training

What it looks like

- No awareness training on Phishing
- Staff are not trained on how to report suspicious emails received

Why it’s a problem

Humans are the most common means of being hacked into.

Training on Cyber Security is required when applying for Cyber Essentials and helps support compliance with GDPR.

How to fix it

- Provide mandatory annual training
- Create phishing simulation tests for users
- Simple reporting process for employees to report suspicious emails

7. BYOD Without Policy

What it looks like

- Employee's Are Using Their Own Laptops For Work
- No Encryption On Devices Used For Work
- No ability to remotely Wipe Data Off Of Devices

Why it’s a problem

A lost device is a data breach.

Underneath the UK GDPR, personal data must be protected from being lost regardless of who owns the device.

How to fix it

- Adopt Company BYOD Policy
- Utilise Mobile Device Management
- Have Encryption Turned On for Devices and Require all Devices to have a Screen Lock Enabled.

8. No Business Continuity or Disaster Recovery Plan

What it looks like

- No documented response plan exists
- No recovery time objective defined
- No communication templates

Why it’s a problem

Recovery delays result in lost revenue and damage to your reputation.

IT recovery alone does not constitute business continuity.

How to fix it

- Create a streamlined Business Continuity Plan.
- Identify all mission-critical functions.
- Define Recovery Objectives.
- Test annually.

9. Insecure Home Working Setups

What it looks like

- Employees using unapproved Wi-Fi networks at home without appropriate security configured on their router
- No VPN or email-based conditional access

Why it’s a problem

The hybrid work environment expands your surface area of potential attack.

How to fix it

- Enforce 2-factor (or multi-factor) authentication.
- Provide secure laptops to employees.
- Use encrypted connections.
- Educate employees on router security basics.

10. Using Unlicensed or Pirated Software

What it looks like

- "I got a copy for free on the internet."
- Use of shared licence keys.

Why it’s a problem

Legal liability, security liability and lack of security updates.

How to fix it

- Conduct a software review across your business.
- Remove unauthorised software immediately.
- Maintain records of software licenses in perpetuity.

11. Ignoring Software End-of-Life

What it looks like

- Outdated Windows Server 2012.
- Unsupported Accounting Software.

Why it’s a problem

Your Software will not receive any Security Updates.

Your Insurer may refuse claims.

How to fix it

- Monitor the life cycles of your Software.
- Plan to budget for updating.
- Replace Software by or before the End Of Support Date.

12. Poor Vendor Security Management

What it looks like

- Not undertaking due diligence on your IT Suppliers.

- Not having Data Processing Agreements with your Suppliers.

Why it's a problem

Under The UK GDPR regulations, you still have responsibility for any actions of your Processors.

How to fix it

- Undertake Supplier Risk Assessments.
- Maintain Contracts with your Suppliers.
- Request copies of their Cyber Essentials certification or equivalent.

13. No Monitoring of Network or Endpoints

What it looks like

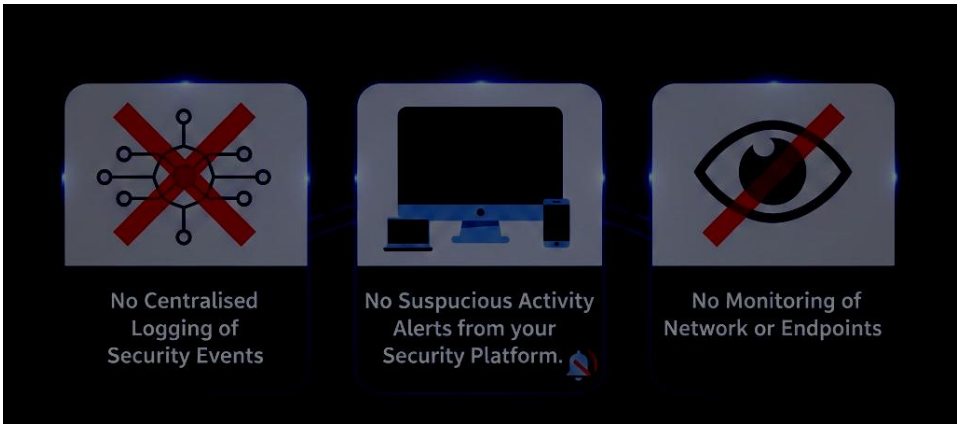
- No Suspicious Activity Alerts from your Security Platform.
- No Centralised Logging of Security Events.

Why it's a problem

A cyber attack can remain undetected for weeks.

How to fix it

- Implement Managed Detection and Response (MDR).
- Enable Security Alerts and Notifications.
- Review Logs on a regular basis.



14. Overlooking UK GDPR Compliance

What it looks like

- No Data Mapping Document.
- No Documented Policies on the length of time data will be retained.
- No Data Breach Response Plan.

Why it’s a problem

The Information Commissioner's Office (ICO) requires you to provide evidence that you have put in place safeguards for the data you hold.

In addition to Financial Penalties, the investigation into your company will be disruptive to your Business.

How to fix it

- Create Data Flow Documentation.
- Create a Data Breach Response Procedure.
- Review Data Retention Policy Annually.

15. Treating IT as a Cost, Not a Risk Area

What it looks like

- Making decisions for IT only based on cheapest option to purchase.
- No planning oversight from a senior management level for what is being purchased/done.

Why it’s a problem

Taking short term savings from cheaper option will create much greater long term exposure to a risk.

How to fix it

- Perform yearly IT risk assessment.
- Align IT systems / processes with overall business objectives.
- Appoint senior management individual responsible for overseeing any and all aspects of company(s) Information Technology Environment.

Business Owner Checklist (2026)

SECURITY:

☐ MFA utilised & enforced

☐ Passwords stored in Password Manager

☐ Devices patched on a Monthly basis

BACKUP/RECOVERY:

☐ Off-site Backups tested Monthly

☐ Defined RTO/RPO established

☐ Detailed plan to recover from a Disaster

COMPLIANCE:

☐ GDPR review level's are competed

☐ Data Processing Agreements are properly stored

☐ Breach Procedures created

GOVERNANCE:

☐ IT Owner has been assigned

☐ Supplier Risks have been assessed

☐ Annual review of IT Function established

HOME WORKING

☐ Secure Remote Access has been implemented

☐ PC's & Laptops are encrypted

☐ Staff have been trained All staff.

FAQs

1. **Do small businesses have any risk?**

Yes. Automated attacks occur regardless of how big a business is. Small businesses or SMEs tend to be targeted more than larger businesses because they generally have weaker controls in place.

2. **What is the cost of these mistakes?**

Costs can vary widely, but some common costs of incidents experienced by SMEs are:

- Invoice Fraud: £5K - £25K
- Ransomware Recovery, Downtime, Legal: £10K - £100K+

Reputationally, you may experience a loss that lasts longer.

3. **Can a business fix this without an IT department?**

Yes, many of the basic items can be done with the proper guidance. However, monitoring and configuring will typically benefit from the use of a specialist.

4. **Which mistakes, when working to fix, should be at the top of the list?**

- No MFA (Multi-Factor Authentication)
- No or untested back-ups
- Unsupported systems/software
- No monitoring or reporting

These are the most pressing priorities for you to work on fixing first.

5. **How often should I review my IT environment?**

You should review your IT environment at least once a year and anytime there is a significant business development, a major growth/change in systems employed, a new regulation, or an IT insecurity/event.

About This Guide

The **Computer Support Centre**, a Managed IT Services provider based in the UK that provides support to small/medium-sized business, has produced this Guide.

We work with organisations throughout the UK, providing a range of services designed to:

- Enhance IT security and resilience
- Assist compliance with the UK GDPR and Cyber Essentials
- Reduce operational risk
- Improve backup and disaster recovery processes
- Enable secure hybrid/remote working

The information in this Guide is based on our experience of the working environments of UK SMEs to help them avoid preventable IT-related problems which can cost them time, money and affect their reputation.

Our goal is very straightforward; we want to provide you with practical, simple and easy to follow information that has no technical language or unnecessary complexity.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
 https://computersupportcentre.com

Conclusion

Small businesses in the UK face most IT issues due to simple, all-too-frequent mistakes, as opposed to significant technical failures. On a day-to-day basis, misunderstandings of weak passwords, missing backups, unpatched systems, and unclear policies deliver nominal impacts; however, over an extended period of time, each can produce a real impact on a small business' overall financial performance, operational effectiveness, and compliance with regulations.

Fortunately, all of the errors listed above can be resolved through processes and/or methods which can be implemented without requiring substantial capital outlays. Written policies that are regularly reviewed, properly enforced security controls, and a reasonable amount of thorough planning can have a dramatic effect. By being proactive today, you are reducing your potential for interruptions and protecting your data while providing the requisite stability for your business to expand with peace of mind.