Supporting Hybrid Work Securely: A UK SME Guide

why hybrid work changes IT risk

- Hybrid work has become normal for the small and medium-sized enterprises (SMEs) located throughout the UK.
- The security assumptions that were made about office-based work environments will not work any more.
- Devices, data, and users are not all located in the same area.
- Risk is no longer measured only by the "internal" versus "external" security.
- The goal will be to enable flexibility while minimising risk where possible.
- What the guide will offer you is something very useful (a way to put the guidelines into action) versus, just talking about them.

What “hybrid work” really means in practice

From an IT and security perspective, hybrid work comprises:

- Accessing company systems (email, files, applications) via multiple locations and devices (e.g. office, home, public places).
- Variable usage of company-owned and personal devices (i.e. work laptops and phones, and BYOD devices).
- Cloud-based tools (Microsoft 365, Google Workspace) replacing or adding to the on-premises servers.
- Increasing dependency on different forms of internet connections which have diverse levels of security.
- An increased need for verification of identity and control/access to devices and sensitive data away from the physical office itself.

It’s much more than just occasionally ‘working from home’ when you think about security; it is a considerably more distributed environment where security needs to follow the user.

The 10 biggest hybrid work security risks for UK SMEs

According to analysis that incorporates 2025-26 data compiled by NCC and other government/corporate experts and reports, and from all other incidents in this area:

1. Phishing attacks on home workers have increased due to use of AI, making them seem more realistic than they did previously (although human factors will still contribute).
2. Employees accessing the web from insecure home networks/public Wi-Fi, as well as accessing logins and other sensitive data via those networks;
3. Lost/stolen unencrypted/full disk-protected devices;
4. Work email accounts/files being accessed from shared/generic family/home devices;
5. Use of weak/recycled passwords, especially when MFA is not being used;

6. Out of date software/patches on work laptop/phones that are located outside of the physical office.
7. These may include accidentally sharing data through personal accounts such as personal Dropbox accounts.
8. The lack of direct supervision allows for increased potential for errors (misconfiguration)* and shadow IT.
9. Third-party applications used remotely may subject to the risk of supply chain attacks from those vendors or their subsequent suppliers.
10. Failure to promptly remove access by removing accounts of former employees, leaves them with unfettered access.

Core pillars of secure hybrid working

1) Identity & Access Management

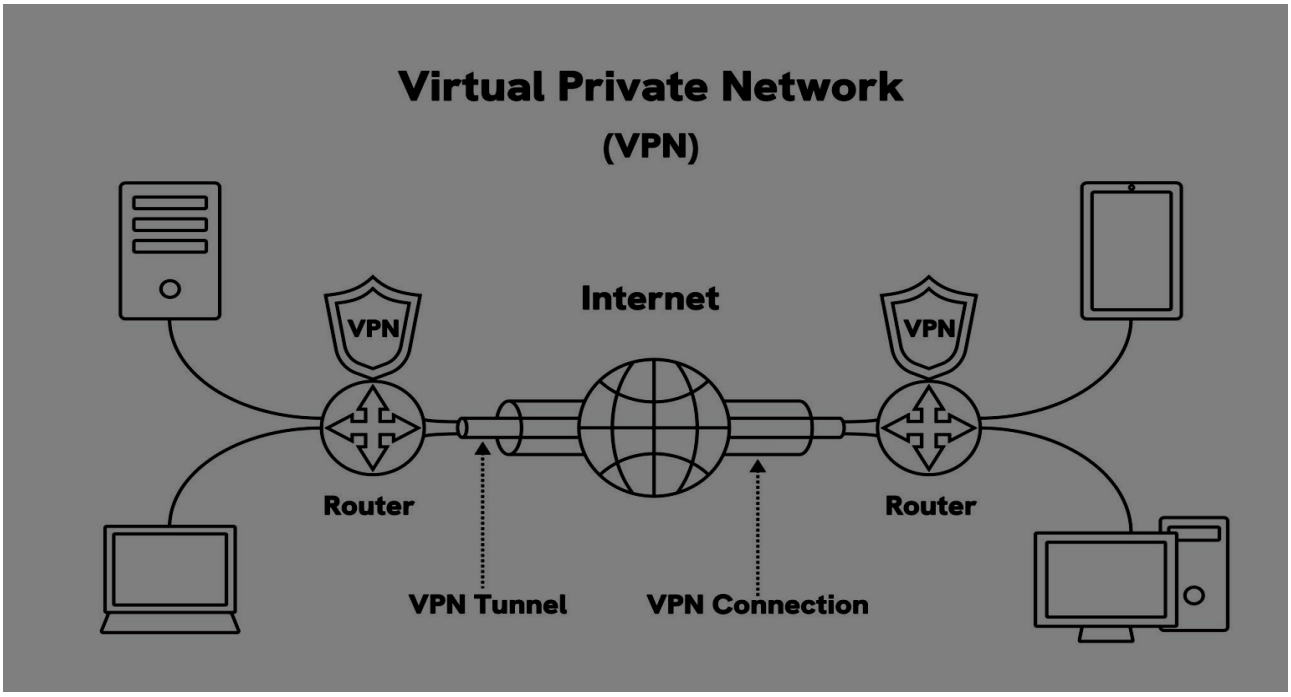
- Multi-Factor Authentication (MFA) Across All Cloud Services
- Strong policies on passwords
- Principle of Least Privilege
- Basics of Conditional Access
- Link to Cyber Essentials

2) Device Security

- Devices Issued From The Company Vs Personal Devices
- Disk Encryption
- Screen Locks
- Mobile Device Management - Basic Definition
- Ability To Remotely Wipe Data From Devices

3) Secure Connections

- Using VPNs -Traditional Use -When Do You Need A VPN?
- Re-Building Using A Cloud-First Method-Explanation of Zero Trust in Normal Terms
- When Do You Use A VPN
- Using open wireless Network



4) Endpoint Monitoring & Patching

- Mandatory Automatic Updates
- Endpoint Security Software
- Remote Device Monitoring
- Importance Visibility

5) Email & Phishing Protection

- Email Is Still Number One Attack Vector

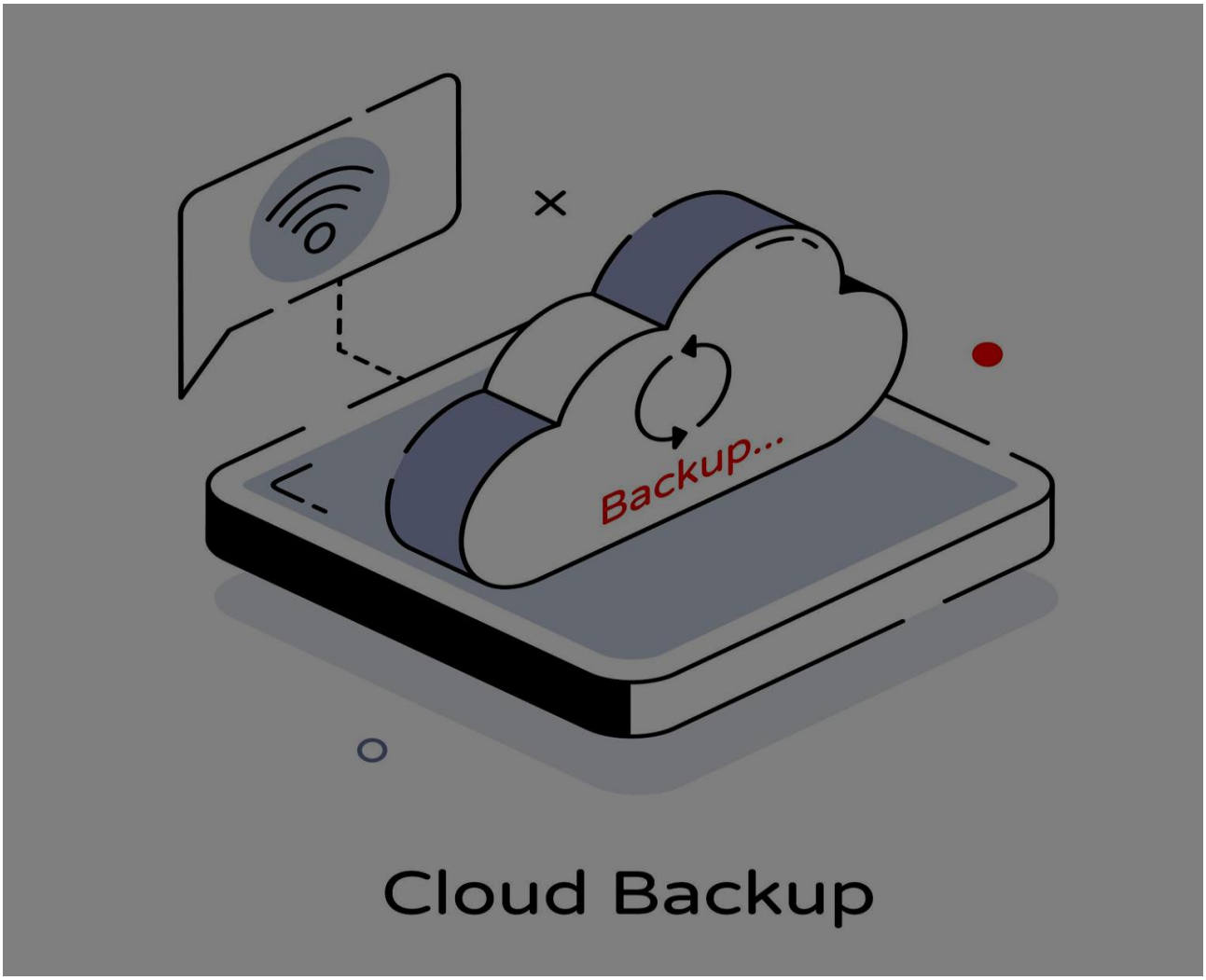
- Email Filtering
- Creating User Awareness
- Establishing A Simple Process For Users To Report Phishing

6) File Sharing & Data Protection

- SharePoint Vs Personal File Storage
- Link Expiration
- Periodic Audit Of Access
- GDPR Accountability

7) Resilience Against Data Backup & Ransomware

- Backup Of All Company Data With Cloud Providers
- Backup Data That Cannot Be Altered Once Created
- Testing Recovery Process Reported Every 6 Months
- Expectations For Cyber Insurance



8) Acceptable Use Policy & Remote Working Guidelines

- Clear Instructions For Staff On Their Responsibilities
- Expectations Around Employee Devices
- General Information About Employment Law For All Employees Based In The UK
- Transparent Policies.

Technology checklist

Director-Level Security Technologies Checklist

- Is Multi-Factor Authentication applied?
- Is there device encryption in place?
- Have backups been tested?
- Is there a leaver process in existence?
- Are you compliant with Cyber Essentials?

Technical Checklists for IT Departments

- Are endpoints monitored?
- Has patch management compliance been tracked?
- Have backup logs been checked?
- Are there scheduled access audits?
- Have you set up conditional access?

Policy and People Considerations

- Do you have proper training for your Hybrid staff?
- Do all staff have a remote working policy outlined?
- Is there an acceptable use policy established?
- Are there BYOD considerations?
- Is there clarity in reporting for incidents?
- Is there an annual review process for agreements?

Monitoring and privacy (UK-compliant overview)

Monitoring activities (for example: logging of endpoint and log-in activity) can continue on a proportional, transparent and lawful basis (legitimate interests of GDPR).

- Advise staff what is being monitored and why (update your privacy notice/policy).
- Do not conduct excessive intrusions (for example: routinely capturing webcams/screenshots).
- Perform a DPIA for any tools you consider to be intrusive.

- Consult with staff and minimise the privacy impact, following guidance from ACAS.
- Only monitor security events rather than monitoring performance.

Practical implementation roadmap (30-60-90 days)

1-30 days (Simple victories)

- Multi-factor authentication should be enabled everywhere.
- Conduct Phishing Training Seminars.
- Revise your Remote Work Policies and Acceptable Use.
- Ensure that all company laptops have encryption.
- Analyse the Joiners/Leavers Process.

31-60 days (Build the foundation)

- Develop Centralised Device Management.
- Transfer Shared Data to Teams/SharePoint.
- Enforce Conditional Access Policies.
- Verify Backups and Perform One Restore.
- Develop Documentation for Privacy Notices for Employee Monitoring.

61-90 days (Strengthen & Train)

- Implement Automated Third Party Patching.
- Conduct Three Full Staff Training Sessions.
- Deploy Phishing Simulations and Analyse Data.
- Obtain Cyber Essentials Certification (if not obtained already).
- Review Schedule Quarterly.

FAQs

➢ **Does a VPN still have to be used?**

A VPN's need depends on the underlying access technology and security requirements. For example, a user accessing Microsoft 365 through a zero trust or cloud-based method would not require a VPN, while someone accessing legacy systems or high-risk connections does.

➢ **Are home networks considered "trustworthy?"**

Home networks can generally be considered untrustworthy (i.e., do not trust them). User education and awareness is important (use multi-factor authentication (MFA), implement conditional access, and do not conduct sensitive work from a public/open network).

➢ **How do you monitor your employees without violating their privacy?**

Transparency (explain privacy monitoring), proportionality (monitor based on security not based on individual's life), and consultation with employees (ACAS) are the key principles of monitoring an employee's use of work-related technology. Ensure you have documented your privacy monitoring efforts in your employee's privacy notice.

- **What is the minimum security technology required?**

Monthly security review of the following items: MFA, encryption, access to company files, patch updates, daily backups, and user training.

- **Is hybrid working more expensive to support?**

Yes; initially, yes (technology purchases such as MDM) but typically has long-term benefits (such as lower overall facility costs and increased resilience). Most SMEs can effectively operate within the standard Microsoft 365 plan.

About This Guide

The **Computer Support Centre** is a UK-based IT and Cyber Security Consultancy that helps small and medium businesses with secure infrastructures, Microsoft 365 environments, and practical Governance Frameworks. This guide has been developed from real experience of helping organisations move to hybrid and remote working and to comply with their UK GDPR obligations, as well as to meet Cyber Essentials control requirements. The document provides directors and managers with clear, straightforward advice in non-technical language. The contents of the document are for education only and do not constitute legal or regulatory advice. For further details about our services or how we work, please visit our website at https://computersupportcentre.com.

Conclusion

Enabling hybrid working within a secure manner isn't primarily about limiting flexibility; it's about having appropriate measures in place so that flexibility can continue and does not result in additional risk. Since employees (as well as their devices and the data they access) will no longer only be accessing an office network, therefore, the focus of security will change from location controls to identity, device and data protection. The good news being that many of the basic security controls (i.e. multi-factor authentication, encrypted devices, regulated file sharing as well as reliable backups) are fairly easy and inexpensive for any small to medium sized enterprise (SME) to implement. By applying a structured and proportional approach along with regularly reviewing their security controls; businesses can implement flexibility in working from home confidently whilst still meeting their obligations under data privacy legislation and ensuring they remain operationally resilient.