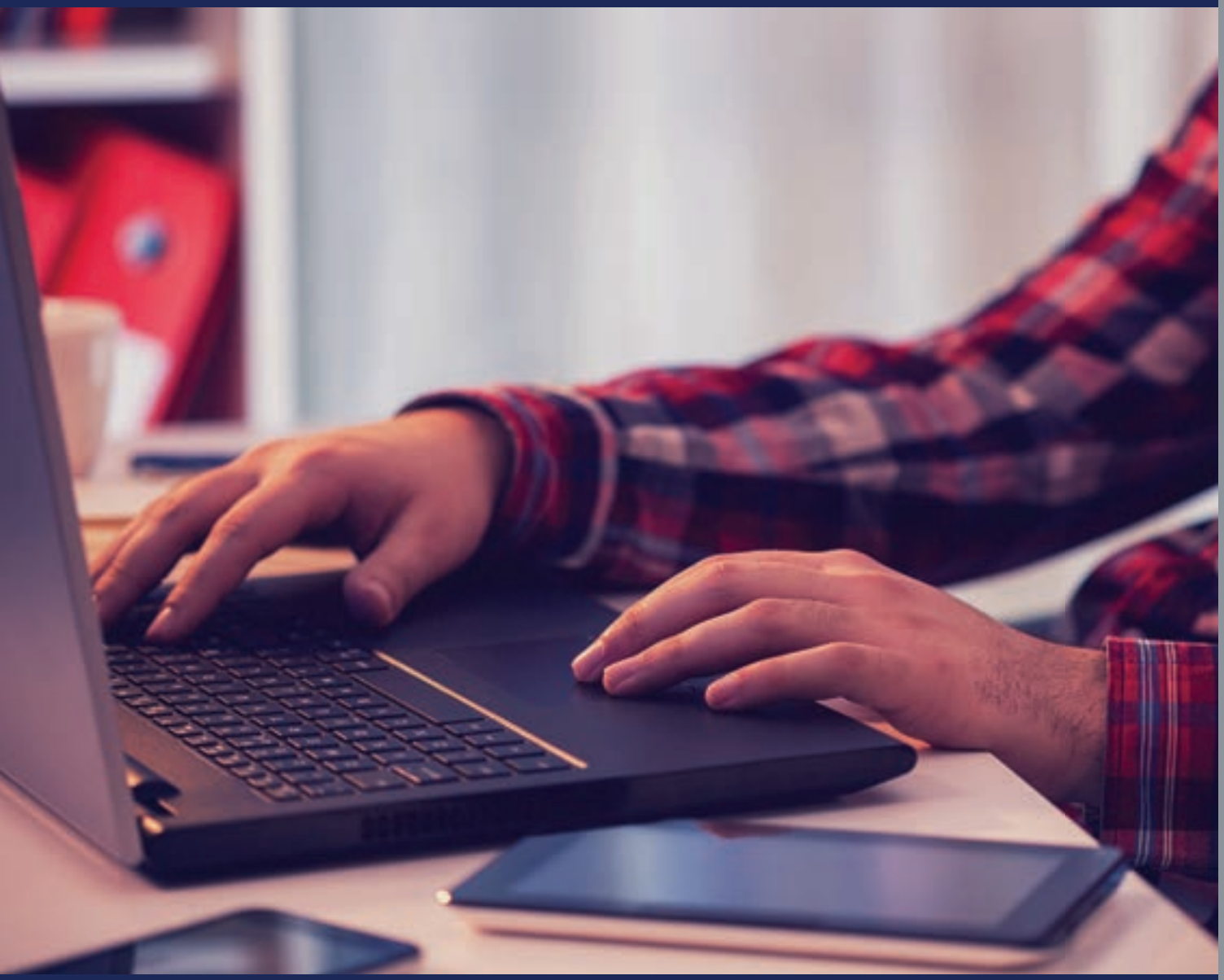
COVID-19
Remote Working Guide

Pulsant
Business Unlimited

Preparing for sustained remote working



Visit us at **pulsant.com** or call **0345 119 9911**

REMOTE WORKING GUIDE

Introduction

Since the COVID-19 pandemic reached the UK, many businesses have rapidly transitioned their teams to work from home successfully.

But now the transition phase is over, we are entering a period of sustainment; where the focus is no longer on just ensuring systems and processes work, but that they are optimised, secure and compliant. But what does this mean for your business?

This best practice guide explores the key challenges you're likely to face as a result of sustained remote working and provides advice on steps that can be taken to protect data, safeguard your business, and keep IT systems running efficiently for the duration of this crisis and beyond.

Importantly, it will pose questions about how a shift to remote working may impact the confidentiality, integrity and availability of your company's data, as well as the wider security and privacy risks that arise.

It might be a challenging time for IT teams, but get your strategy, systems and solutions right now and you can reap the benefits for years to come.

With more autonomy working from home, many employees find they perform better, producing a stronger output

Pulsant
Business Unlimited

The benefits of remote working

COVID-19 may have forced businesses into the widespread adoption of remote working, but the benefits of agile working are not new. Many organisations were embracing remote working long before the crisis, however, no one could have anticipated the need to shift to remote working on such a speed and scale.

The benefits for employees are obvious, but by embracing remote working for the long-term businesses also have much to gain, including:

Improved employee productivity

Many employees find they can do more work at home with less interruptions from colleagues. Some professions in particular require employees to focus for hours at a time and having a space with no distractions is vital. Plus, with no stressful commute, employees often use the travel time to work instead.

Better performance

With more autonomy working from home, many employees find they perform better, producing a stronger output.

Greater staff retention

Flexible working can be a critical factor in hiring and retaining the best people, with employees often choosing employers that can offer more flexibility. It also removes location as a barrier, meaning organisations can benefit from a wider talent pool.

Happier employees

With less time spent commuting, employees can benefit from more time to exercise, spend time with the family and focus on their wellbeing. This can help to reduce stress, making for a happier, more productive workforce.

Less absenteeism

If employees are able to work remotely, this can reduce the time they need to take out for appointments, particularly if they are not near the office, as well as any absenteeism as a result of travel disruption.

Lower costs

One of the most obvious benefits is a reduction in spend on office space, as well as supporting overheads such as heating, water and electricity bills.

Better for the environment

Enabling employees to work remotely has many environmental benefits, from the reduction in traffic pollution to conservation of office space.

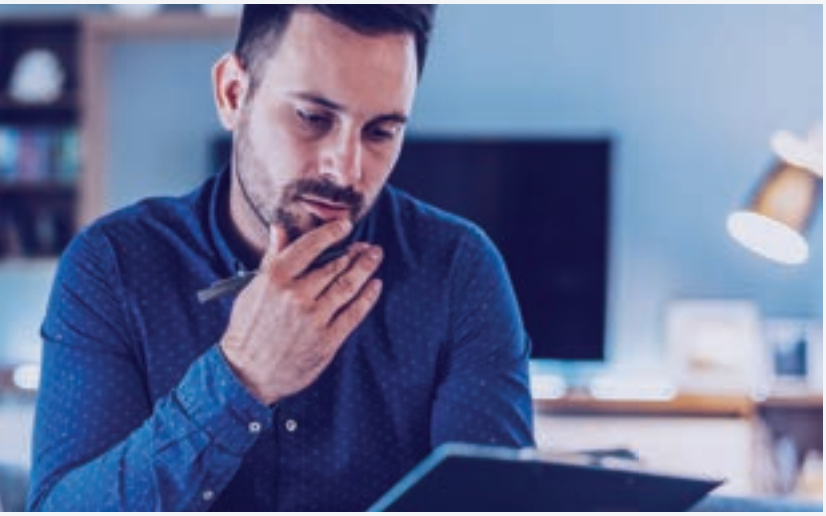
Flexible working can be a critical factor in hiring and retaining the best people, with employees often choosing employers that can offer more flexibility

Pulsant
Business Unlimited

Understanding the risks

Whilst remote working has many benefits for businesses, it also has risks. Employees are working from uncontrolled environments and, as a result, perimeters have expanded. Cyber security is a lot harder when your attack surface is bigger and you need to understand the full implications.

One of the most important things you need to consider is whether a move to remote working has implications on the confidentiality, integrity and availability of your data. While remote workers are still bound by the same policies, the measures to implement and control them are not present at home, so you're placing a lot of trust in employees to take the right precautions.



Cyber criminals are already seizing the opportunity presented by mass remote working to gain access to and breach systems and data

Added to this are the new risks that arise from a dispersed workforce, which for attackers is a lucrative target. Cyber criminals are already seizing the opportunity presented by mass remote working to gain access to and breach systems and data.

Some of the most common challenges that you are likely to face in this environment include:

Understanding the new risk profile and responding to it dynamically

One of the biggest challenges is just understanding how your risk profile has changed. And there's a lot to consider. For example, do your policies need updating to accommodate the change in working environment? Are your processes and practices robust enough? Do employees know how to protect themselves against increased risks?

Maintaining compliance in new working environment

The shift to home working introduces many considerations for GDPR compliance. With employees working remotely, your risk of data breaches increases.

Preventing data loss from employees

With employees now outside of your line of sight, there's a risk information could be misused or misplaced.

Pulsant
Business Unlimited

Reducing the risk of phishing and cyber-attacks

COVID-19 has provided the perfect opportunity for cyber criminals to increase phishing and cyber-attacks. Employees' emotions are high, defences are reduced and as a result, attacks are more likely to slip through the net.

Ensuring backups are sufficient and secured

In a remote environment, having a solid data backup plan is even more of a priority. With employees working in a variety of locations and conditions, your regular backup plan might not be sufficient.

Preventing unauthorised access

More employees working from home means more people accessing and processing information outside of your normal security perimeter. Furthermore, this might be via shared networks which introduce new risks.

Securing applications and data where employees are now working on home broadband and unsegregated networks

You no longer have control over the networks employees are using. Many home networks aren't password-protected, use easily guessed or default passwords, or may be configured without encryption, allowing attackers to easily compromise the network.

Maintaining visibility and control over corporate assets

You may have employees using new devices, or in some cases, their own. If you can't see and control user activity on all endpoints being used for work purposes, you might face problems like unauthorised access, malicious external sharing and data protection issues.

Ensuring data protection in a remote environment

While in the traditional office environment you have a number of in-built security measures to ensure that data is kept secure, this is not the case in a home environment. You need to understand where your data resides where employees are working remotely.

Securing the remote workforce

With the risks high and the dust now settled from the transition to remote working, it's time to start thinking about mid-term plans and moving beyond functionality to a focus on security.

The following steps can be implemented quickly to help you get your organisation back inside its risk comfort zone.

- Ensure all laptops are encrypted and require a password to boot
- Ensure complex passwords or biometric authentication is enabled for all mobile devices and additionally at application level if needed
- Develop Bring Your Own Device (BYOD) security policies and controls
- Use two-factor authentication to guarantee you know who is accessing data
- Implement device management to allow tracking, remote wipe or lock in case of theft or loss
- Use encrypted connections to prevent data leakage over unsecured networks
- Restrict access to removable media such as SD cards or USB sticks
- Keep antivirus services, software and firmware up-to-date
- Provide users with the right security education
- Implement solutions such as monitoring software for data leak prevention
- Control access to the network
- Replace home routers low / end firewall or VPN solutions
- Implement virtual desktops to help maintain the common operating environment and organisational security policies

Pulsant
Business Unlimited

Planning for the future

Looking further ahead, it is likely that as we eventually transition out of this period there will be large sections of industry where remote working becomes the new normal.

We may well end up moving back into our offices, but continuing to apply social distancing there, perhaps with half the team in the office and half working from home at any one time. Or you might consider accelerating existing plans to permanently scale down your office footprint.

With this in mind, you also need to consider the more significant or longer-term changes needed to support the entire workforce working remotely for a prolonged or indefinite period. This also means thinking about how you should be approaching bigger infrastructure projects that were planned.

You also need to consider the more significant or longer-term changes needed to support the entire workforce

Answering the following questions will help you prioritise where to focus your efforts:

- Does your IT strategy still stand up in the light of recent experience? Do you need to modify your objectives, the pace of change, or indeed the investment approach?
- For each project that contributes to your strategy, do the objectives still make sense? Will it still deliver what you want?
- Are your applications and data in the right place to achieve both performance and compliance requirements?
- You have probably been moving your key business applications to cloud over a period of time. Do you need to accelerate that?
- Do you have an application delivery model that supports your new working practices?
- To what extent can your project be implemented using remote resource? Would procuring a more packaged, standardised solution help mitigate this risk?
- Educating the workforce will change. Are you well placed to use the wide range of modern online learning tools?

Pulsant
Business Unlimited

Seize the remote working opportunity

The introduction of any new technology and working practices requires new security measures, but usually this risk is managed carefully, over a period of time.

With COVID-19, organisations have had to accelerate digital transformation plans with many forced to make the transition almost overnight, and in this scenario, achieving security best practices may not have been possible.

The problem is attackers are aware of this situation and are already taking steps to exploit the opportunity. So, with the new work setup likely to continue in some form or another, for at least the next few months, steps must be taken to improve security posture in this new working environment.

The technology has proven to work, so now is the time to take a step back and review security practices and posture. You need to think about mid-term plans, moving beyond functionality to a focus on security and must not neglect longer term changes and bigger infrastructure projects.

It is impossible to overstate the importance of protecting your organisation's data and ultimately its reputation. By implementing the correct controls, systems and processes now, your organisation can benefit from smarter, efficient, more effective ways of working not just now, but for years to come.

With the new work setup likely to continue in some form or another, for at least the next few months, steps must be taken to improve security posture in this new working environment.

Visit us at **pulsant.com** or call **0345 119 9911**

Pulsant
Business Unlimited