HOW PREPARED IS YOUR BUSINESS FOR PROLONGED REMOTE WORKING?

InfosecPartners
CYBERSECURITY

REMOTE WORKING GUIDE

Since the outbreak of the COVID-19 pandemic, businesses of all sizes have successfully transitioned their teams to work from home effectively

Now that the initial transition phase is over, we are beginning to enter a period of sustainment; where the focus is no longer just ensuring that IT systems and processes work, but that they are optimised, secure and remain compliant with data privacy and protection regulations.

WHAT DOES THIS MEAN FOR YOU, YOUR STAFF AND YOUR BUSINESS?

This remote working guide is designed to help with key challenges your business is likely to face as a result of prolonged remote working and provides useful advice on the steps that should be taken to protect data, safeguard your business, and keep in line with the General Data Protection Regulations (GDPR). Organisations must ensure the personal data they collect and process is kept safe and secure.

This can all be a very daunting challenge for IT teams but getting the strategy, systems and solutions correct from the offset will provide huge benefits for many years to come.

Remote working not only benefits employees by eliminating daily commutes, it can also greatly increase performance, productivity and even lead to healthier lifestyles.

InfosecPartners
CYBERSECURITY

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 with such speed and scale.

The benefits for employees is clear, but by adopting remote working strategies for the longer term, businesses have much to gain, including:

IMPROVED 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 will often choose to use the travel time to work.

HAPPIER EMPLOYEES

With less time spent on the daily commute, staff can benefit from having more time to exercise, have more time with their families and can focus more on their wellbeing. This can dramatically reduce stress, which in turn creates a happier and more productive workforce.

LESS ABSENTEEISM

As ironic as it might sound remote working can significantly decrease employee absenteeism. Working from home enables staff to look after sick kids, make appointments or run errands, without having to take time off work. If employees can work remotely it removes the possibility of lateness and absenteeism due to travel disruption.

GREATER STAFF RETENTION

A more flexible approach to work has been proven to be an influential factor when hiring and retaining the best staff, with employees often choosing positions where employers offer greater flexibility.

Geographical location is no longer seen as a barrier, meaning businesses can benefit from a much wider talent pool.

INCREASED PERFORMANCE

With more freedom working from home, many employees find they are more spontaneous and as a result perform better and produce a stronger output.

LOWER OPERATING COSTS

If a business can successfully operate remotely significant savings can be made. As every business owner will know, whether they rent or own office space, the cost of such overheads can equate to a significant percentage of business outgoings. Anything saved on overheads is something that can then be reinvested into the future growth of the business .

InfosecPartners
CYBERSECURITY

The risks and rewards of remote working

Remote working provides huge benefits for business, but it also has huge risks. Employees are effectively working from an uncontrolled environment with expanded perimeters and risks.

It is essential to establish whether the move to remote working has increased implications on the confidentiality, integrity and availability of your data.

While remote workers are bound by the same company policies, the measures to implement and control these policies has become slightly more complex.

Your workforce, customers, supply and distribution chains and the constantly shifting threat landscape need to be protected to the same or even higher levels of security than what is used in the office.

Cyber criminals have already begun seizing the growing opportunity presented by mass remote working to gain access to and breach corporate systems and their data.

It is of huge importance with these new risks from this shift to a remote working environment, that security is assessed properly and that all technology and resulting risks are surveyed and secured.

84% of IT leaders reported that DLP is more challenging with a remote workforce.

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

UNDERSTANDING THE NEW RISK PROFILE

The biggest challenge is understanding how your risk profile has changed. Do your policies need updating to accommodate the change in working environment? Are your processes and practices robust? Do your employees know how to protect themselves against these increased risks?

MAINTAINING COMPLIANCE

The shift to remote working has introduced many considerations for GDPR compliance. With employees working remotely, the risk of data breaches increases significantly.

PREVENTING DATA LOSS

Data leak issues, like misdirected emails or malicious insiders, can put companies at risk of noncompliance with GDPR regulations.
This “new normal” of remote working will continue for the foreseeable future. So, businesses must ensure high standards are maintained and prioritise data protection practices.

InfosecPartners
CYBERSECURITY

Understanding the risks

PHISHING

Phishing attacks are now being specifically tailored to target remote workers. Therefore it has become increasingly important that remote workers are made aware of how a phishing attack works, but also the possible impact that phishing can have to business reputation, its bottom line, and crucially, its business continuity.

BACKUPS

Ensuring access to up-to-date company data to remote workers is essential. With remote teams working from a variety of locations, and different conditions, regular backup plans may not be able to support the requirements of your team.

The cost of downtime can have enormous repercussions, and working remotely offers numerous challenges compared to the traditional office environment. In a remote environment, having an effective data backup plan is essential.

PREVENTING UNAUTHORISED ACCESS

Having a growing number of employees working remotely means that there will be increased access and processing of information from outside of the normal corporate security perimeter.
This access might also be through shared networks which in themselves can introduce security risks. Identity and access management helps tell who a user is and what they are allowed to do. The user's identity, not their device or location determines what data they can access.

SECURING REMOTE BROADBAND

With employees working from home you probably won't have any control of their networks.

Many home networks and wifi routers are not password protected, or use easily guessed, insecure or default passwords and may even be configured without any encryption. This new attack surface provides hackers with lots of weak points that can easily be exploited to gain access to sensitive company data through insecure home Wi-Fi networks.

Securing home networks is therefore essential when it comes to keeping out attackers and protecting company assets and data.

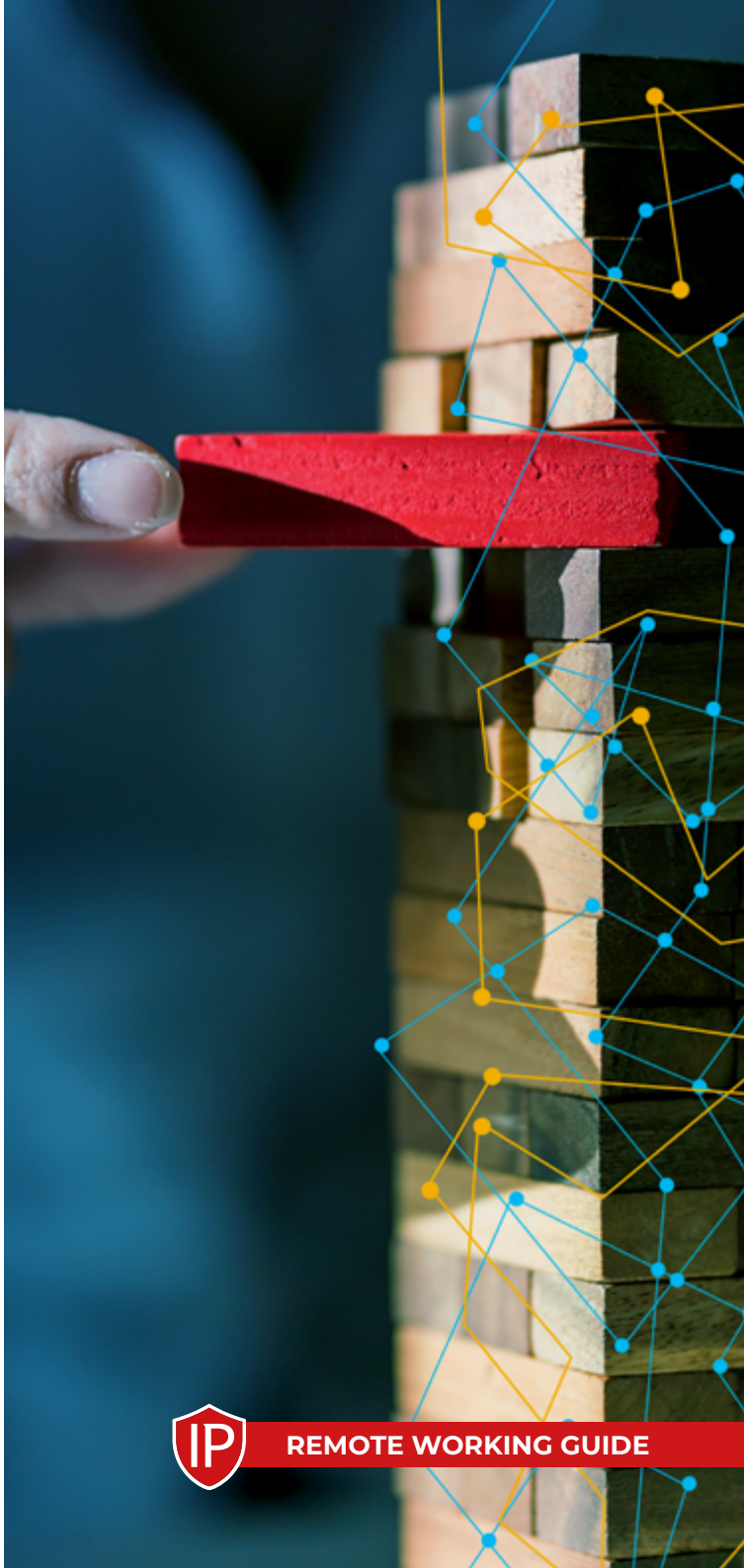
MAINTAINING VISIBILITY & CONTROL OVER CORPORATE ASSETS

You may have staff members using newly purchased IT devices, or in some cases, their own computer equipment in order to work remotely. If you can't see and control user activity across all endpoints used for work purposes, you most likely will face issues like unauthorised access, malicious external sharing and data protection.

ENSURING DATA PROTECTION

Within the traditional office and work environment you will have a number of security systems and measures in place to keep data secure, this is not the case for the home office environment. You need to understand where data resides when employees are working remotely and how it is accessed.

InfosecPartners
CYBERSECURITY



SECURING THE REMOTE WORKFORCE: CHECKLIST

If the following hasn't been implemented already the following steps shoud be implemented as soon as possible to help secure your remote team and get your organisation operating securely:

- [ ] Ensure all devices and computers are encrypted and require a secure password to open
- [ ] Ensure complex passwords or biometric authentication is enabled for all mobile devices
- [ ] Enforce a Bring Your Own Device (BYOD) security policy
- [ ] Use two-factor authentication to ensure you know exactly who is accessing your data
- [ ] Implement a device management framework to allow tracking, remote wipe or device lock in case of theft or loss
- [ ] Use encrypted connections to prevent data leakage over insecure networks
- [ ] Keep antivirus services and all software and firmware up-to-date
- [ ] Provide all staff with the cyber security education and awareness
- [ ] Implement solutions such as monitoring software for data leak prevention
- [ ] Control access to the corporate network
- [ ] Replace home routers low / end firewall or VPN solutions
- [ ] Implement virtual desktops to help maintain the common operating environment and organisational security policies

Call 0845 257 5903 or visit www.infosecpartners.com for more details on our bespoke remote working solutions

InfosecPartners
CYBERSECURITY