ramsac
at the heart of IT

The Digital Commute:

Adaptable Working After the Global Pandemic

The Digital Commute:

Adaptable Working After the Global Pandemic

Contents:

Social Distancing in offices – IT considerations for a safer reopening

Despite changing restrictions in the UK, which ease and tighten according to the global pandemic, the eventuality is a return to some kind of a 'new normal'. During this journey, UK businesses will need to decide on the fate and ultimately, the future of remote working.

There are many organisations now considering their options for how to safely integrate staff back to their work environment. One thing that seems clear is that few organisations will return to the way things once were. Working from home, or remotely, will be here to stay for a while. Staff that are shielding or caring for children, and with the health and safety risks taken from a global pandemic, businesses need to think about their long-term ability and viability to work in different, possibly hybrid, ways.

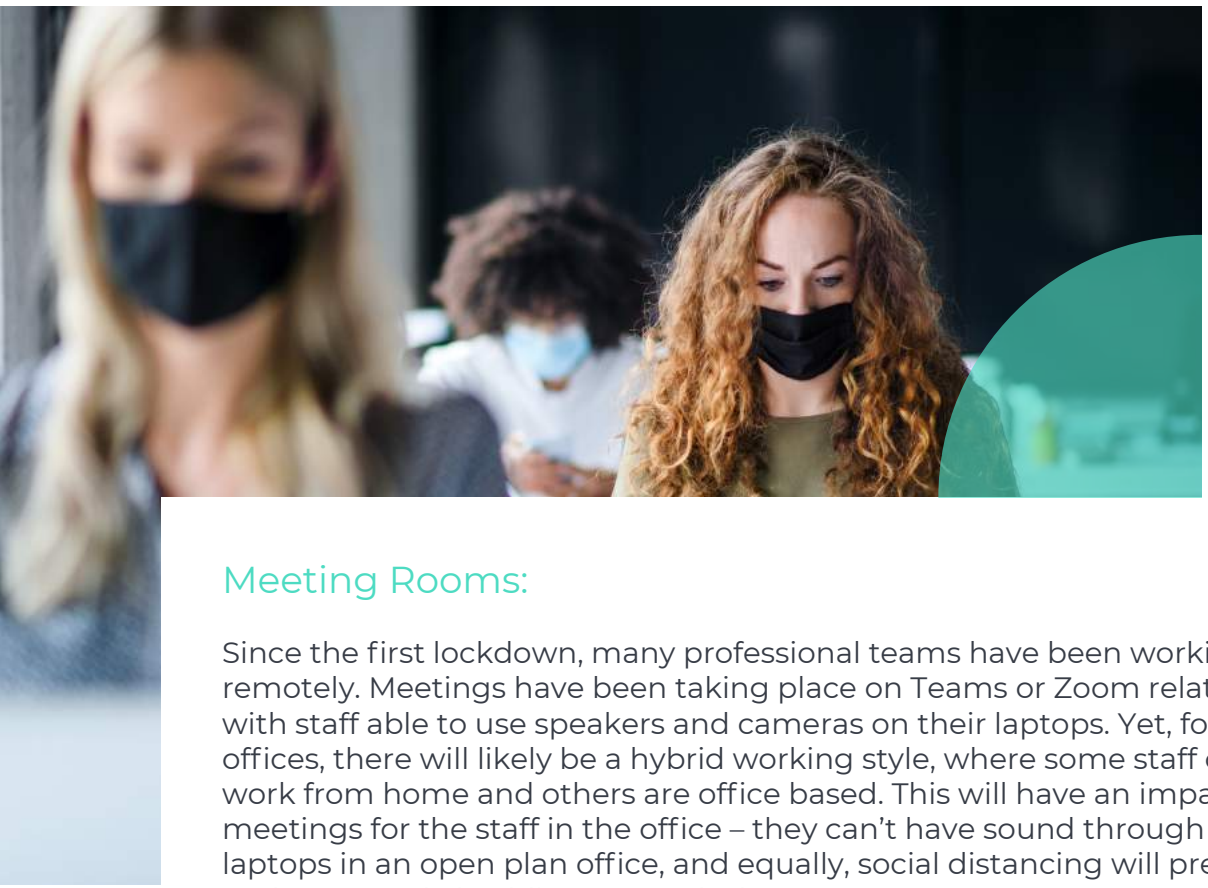
Reopening the office:

If you are bringing staff back from furlough, it's likely that passwords will need to be reset and machines tha t have been switched off for weeks will need to run updates, catch up on Antivirus versions, etc. There is a chance that machines could take a while to be fully work-ready and you may need to have some IT staff available to help on the first few days of reopening, to ensure people are back up and running as quickly as possible.

Staff that have been working from home for the duration of UK-wide restrictions will, potentially, be bringing kit back to the office and this may need resetting, especially to connect to the network. If users took PCs home, these may need re-cabling. Again, think about your IT staffing requirements in advance, or consider staging the return to work to ensure that your IT team or outsourced partner aren't inundated.

Social Distancing:

- Hot desking set-ups, where users share hardware (such as phones, keyboards, mice etc) may not be advisable under safety guidance. So, think now about additional hardware that might be needed.
- Consider removing hardware that is traditionally shared, such as reception desk kit, meeting and staff room PCs, etc.
- You may need to consider moving desks around or creating blank desks on bench style desking in order to ensure that staff can continue to be socially distanced.
- Consider closing off/restricting huddle spaces and removing seats from meeting rooms to reduce capacity.



Meeting Rooms:

Since the first lockdown, many professional teams have been working remotely. Meetings have been taking place on Teams or Zoom relatively easily with staff able to use speakers and cameras on their laptops. Yet, for reopened offices, there will likely be a hybrid working style, where some staff continue to work from home and others are office based. This will have an impact on meetings for the staff in the office – they can't have sound through their laptops in an open plan office, and equally, social distancing will prevent two or three people huddling around a laptop in a meeting room.

It's time to think about the tech in your meeting rooms. You'll need a decent camera, sound output, and easy ways for people to connect to meeting tools, so that your office teams can safely connect with those working remotely. There are a host of ideas for how to do this, ranging from £20 headsets to £5000 whole room systems! Talk to your IT team about this in advance of your main reopening to ensure things are ready from day one.

Laptops:

- If your staff took work PCs home during any of the national lockdowns, returning to work will be a challenge, as they can't realistically carry a PC between home and work each day, if they chose flexible working. Consider whether some of those people now need company laptops to be issued.

- Hot desk users previously using shared devices may now also need personal issue laptops.

- Staff that were sent home hurriedly at the start of the pandemic may be using personal machines. This is a security risk and does not pass the Cyber Essentials framework for several reasons:

    - You have no control over personal devices
    - data is being stored on hard-drives you have access and can manage
    - you're not monitoring or securing them from external threats
    - you're opening up access that you may struggle to manage
    - you've lost control over antivirus protection

It's time to go back and address the personal use device issue and make a longer-term fix.

For those that continue to work from home, check that they have got what they need to work effectively. A staff survey asking questions about their home set-up, such as anything needing to be more efficient or comfortable, is a good idea. You might, for example, focus on posture requirements and ensure health and safety is continued when working remotely. This survey may highlight the need for additional monitors and external keyboards, or other devices, or even show the need for extra support regarding posture or communication.

Data Access:

Under GDPR, you're obliged to have a data asset register – in other words, a list of all the places you are storing data. If the quick response to lockdown has changed some of this information, it's time to revisit. Have people now got data stored on local drives, USB devices etc, just to get them up and running? With more home working for many, you need to address these potential breaches.

Many businesses were looking at moving to a true cloud platform such as Office 365 prior to Coronavirus. So, if you have been struggling with access to on premise or hosted servers perhaps it's time to think about a true cloud alternative? The versatility of having email, folders and Active Directory completely cloud based means all you need is a good internet connection on the user side, making working from home a lot easier.

Future planning:

It makes sense to revisit your business continuity plan and see if you are prepared for another wave of infection. Also take into account changes in staff roles going forward that may affect your process.

There are a lot of people that have really enjoyed the experience of working from home and having proven that they can be effective away from the office.

This unique period in our history will change the shape of working culture forever and IT has an important role to play in this.

Your IT security considerations will have been impacted by changes in working practices. It's time to re-visit your risk assessment and your Data Impact Assessment and ensure that they are both now fit for purpose.

Is Hot Desking Safe?

With most organisations now planning their return, or having already returned to the office, many need to reduce the capacity of previously full workspaces in order to maintain a comfortable social distance. Many businesses are considering 'closing' alternate desks, and others are wanting to capitalise on the benefits that remote working has helped us all to discover during lockdown.

Through it all, one thing has become clear: the days of each employee being allocated their own desk is becoming a thing of the past. If staff are going to carry on working from home two or three days a week, it makes no sense to invest in real estate that will remain at 60% capacity. Hot desking seems like a valuable solution.

But, with hygiene being of primary concern right now, business owners need to consider: is hot desking safe?

Hot Desking: COVID-19 Rules

On Government guidance

It's worth noting that, during government guidelines addressing the procedures that offices should follow to create a safe working environment, hot desking was mentioned.

How to make hot desking safe in the future

IT equipment must be a *personal* issue.

The first obvious adjustment has to be that IT equipment becomes a personal issue. For hot desking to be safe, staff will need their own laptop. If users prefer to use an external keyboard and mouse, these too need to be issued one per person, either being stored in a locker, or carried between home and the office in an appropriate bag or case.

Phones should ideally be removed from hot desks, and employees should be making use of mobile devices or softphones wherever possible. If your phone system demands a handset on the desk, consider a supply of antibacterial wipes and, ideally, a personal issue phone headset to help make hot desking safer for the future.

Clean and clear desk policy

A clean, prioritised environment is often associated with productivity. For hot desking to work properly, desks need to be 'reset' each night with personal belongings being taken home or stored in a locker. Clear desk policy also is part of good cybersecurity, as removing potentially sensitive documents at the end of every day stops unauthorised persons accessing them.

Social distancing

It's clear that social distancing is here to stay for some time to come, especially for offices. To make hot desking safe then, you need to sit down at an employees current desk with a tape measure and work out the best order to have people seated, in order to maintain recommended distances. Consider a system of 'red' and 'green' desks and how these can be clearly labelled.

Building a rota system

Hot desking may be possible but hopping from desk-to-desk in one day will definitely be a thing of the past. The capacity of the office will not be the same as it was before the government advised everyone to work from home. When you've worked out how many 'green desks' you have, consider making a booking system so that people reserve their desk before heading into the office.

Unless you can fully clean a desk in-between user, consider a system of marking a desk that was used in the morning, as 'dirty' until the cleaners arrive and reset it for the following day.

Extra hygiene measures

To reduce the spread of the virus when moving back into the office, it's important that extra hygiene measures are taken in all areas. Cleaning should be maintained every day, especially when hot desking. Chairs, desks, and any other equipment left on the desk (e.g., monitors and keyboards) need to be wiped down before and after use.

Ask staff to do this on arrival and departure and provide appropriate products to do this. You should also put in place regular additional cleaning to the normal office cleaners. Some organisations are looking at introducing disposable desk pads, whereby any personal items are placed on these during the working day. To make hot desking safe, the pad is disposed of when work is finished.

Meeting Rooms

Whilst not strictly hot desking, meeting room capacity also needs to be looked at, and huddle spaces should probably become single-user desks for the time being. With reduced meeting room capacity and an increase in the hybrid work environment (where some employees are at home and others in the building), consider what you need to make conference rooms work effectively. This could be large display screens, wide-angled webcams, and software that allows users to quickly set up room-based video calls. An efficient, working meeting room will become an increasingly important feature of the post COVID-19 office.

The pandemic has brought a new way of thinking on how office landscapes will change and be maintained.

Employee concerns should be at the forefront, and the returning of hot desking in the office should be taken with caution and sensitivity.

Workplace culture in general should prompt the idea of positivity and safety at this time, as staff re-enter the office landscape. It's important for your organisation to consider the various ways that office working can be reintroduced safely, and to make hot desking safe if that's one of the route's you'll adopt.

Making a home office a productive, healthy place to work

During the global pandemic, record numbers of people were working from home, many of whom were not used to working in this way. For people unfamiliar with homeworking, or being away from the office, making sure your employees are comfortable in your working environment is key to enable them to work to the best of their ability. It is possible to be very productive from the comfort of an employee's own home. Whether working from home due to isolation from coronavirus or just working from home, here are some tips that we think will help create a routine and a suitable space to work.

When speaking to employees about the transition to working from home, especially in short term cases such as the two-week COVID isolation, it is important to encourage good habits to allow them to separate work and home life.

We have compiled a series of tips to ensure this can happen.

1) Try to maintain a regular morning routine for getting ready for work.

When working in a home office, even living room or bedroom, it is important to make sure that you are motivated to start your day. It is a great way of motivating yourself and tricking your mind to maintain that working balance. Make this the first thing that you do each day (depending on your work schedule) as this helps to reduce the amount of procrastination that may occur throughout the day. Have breakfast, do some exercise, get de-stressed, follow your usual patterns. By keeping the mental association that you have between work and an office, you'll be able to get work done in the same way at home.

2) Make a plan for the day.

Plan your meals and your day-to-day activities as much as possible. This helps your mind to formulate a structure. Try and make this as specific as you can. This will be good to help you manage your workload and to stay on top of things.

3) Missing the usual hustle and bustle of a busy office?

Being at home can sometimes be very quiet, especially if you are alone, some people miss the sounds of a busy office. You may find it useful to have some background noise while you work, but music and podcasts can quickly become distracting.

4) Make sure you get some fresh air

Especially during this pandemic, ensuring you get outside and get some fresh air is vital to a successful and productive day. It is found that 53% of workers in the UK are likely to regularly suffer from cabin fever-like feelings about their office environment, so it is only natural that you may feel this way when you are working in a home environment. Getting outside once a day will boost your mood and is of course good for your physical and mental health.

5) Limit the distraction of social media.

Social media can be a distraction while working from home and it is easy to get sucked into random posts on Facebook, Twitter, Instagram and LinkedIn. Set yourself a limit, for example 15 mins after mealtimes, for when you can access social media, you will then be ready to focus back on your work with minimal distractions. You may find it beneficial to turn off your social media notifications during work hours. This can be done via your device settings.

6) Try to have a designated space for work

A change of scenery can make you more productive. But it is important to remember if you change where you work within your home, that you are able to be comfortable and set up ready to get on with your tasks in the best way possible. Having a good ergonomic set up is very important. Having a good chair and desk space to ensure you are not crouched over your laptop, will help reduce the risk of long-term injury at your desk.

Here are some useful tips to reduce the risks of long-term injury and maintaining good posture while working from home.

- Balance your head – make sure to not lean your head too forward.
- Arms relaxed by your side – make sure that your forearms are parallel
- Sit back in your chair with good posture
- The top of your screen should be at eye level and your feet flat on the floor.

7) Use technology to stay connected

During your time working from home, you may feel cut off from the rest of the organisation and the social element of the office. Staying connected with your colleagues via instant messaging and video conference calls will help maintain relations and prevent a feeling of isolation.

There are plenty of applications and your organisation is probably already using them, finding the right tools to remain connected and productive is essential to making working from home that little bit easier.

How to Improve your Home Internet Speeds

With most of the nation working from home and competing for bandwidth with their partners, who are also working from the same kitchen table, now more than ever, the need for good broadband connection seems to be a bone of contention in houses throughout the country.

So how can you improve your home internet speed?

1) Make sure strangers aren't taking up your bandwidth:

If your home router is not secure, it allows others to freely connect to your broadband. As well as a host of associated security concerns, this will impact on your internet speeds. To make your connection secure – add a strong password to your router.

2) Mind the Gap

Try to position your wireless router close to where you are working from, ensuring that your wireless router has good air circulation and isn't tucked away in a cupboard. Ensure you move it away from devices that may interfere with your signal, such as microwaves, cordless phones and baby listening monitors. If this doesn't work, try to connect the ethernet cable from your router directly to your device.
Placing the router higher up in the house is what internet providers commonly suggest. Positioning it centrally and high up ensures even reach. In offices, routers are often secured to ceilings, so liken this to home working.

3) Reduce connected devices:

Look around your home and count the number of devices connected to your network.

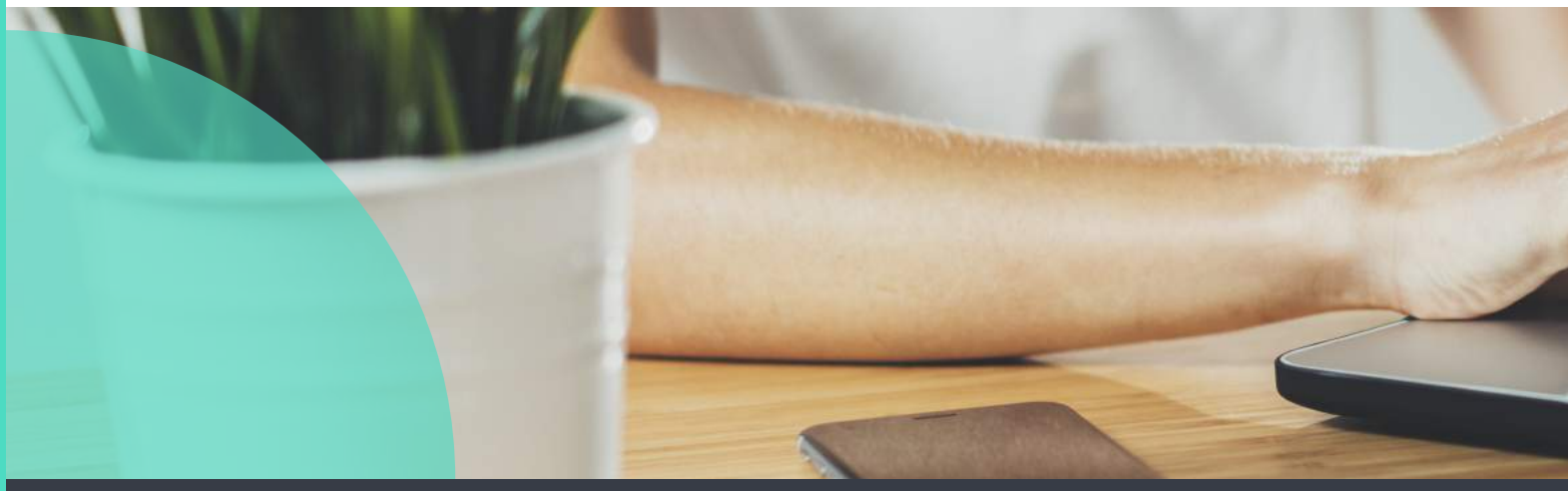
You'll be surprised how quickly they add up – smart doorbells, televisions, mobile phones, telephones, smart heating controllers, wireless lighting systems, Sonos players and Internet connected kitchen appliances.

Most home routers are only designed for a dozen connections and we are overloading them with devices all taking up your bandwidth. Disconnect devices that are not being used during your working from home time. This tip maybe a little bit harder when kids are at home, but during essential times when you need to have a fast connection, for example, during video calls, try and get a non-technology filled activity ready for the kids.

4) Give it a boost

Home routers are often simply not designed for the workload we now place on them. There are some relatively inexpensive, and some fairly pricey options for increasing home Wi-Fi coverage. The more sophisticated solutions create a 'mesh' of Wi-Fi signal and work by having several connected devices that you can place strategically throughout the house which work together to provide a seamless Wi-Fi connection throughout your home. Solutions such as Google Wi-Fi and TP-Link Deco system are great examples to explore.

You can even use their respective apps to give different devices a higher priority – meaning your Microsoft Teams conference call should get priority for internet connectivity. These are simple to set up and install but can have a huge impact on the strength of the signal and are normally designed to support more like 100 devices, rather than the dozen or so devices most ISPs say their home routers are designed for.



Mesh Wi-Fi systems add a layer of connectivity over the top of your existing network connection, which allows for better speeds. There are other options of ways to boost your system, including plug-in booster that can extend the reach of your broadband, perhaps in a room far away from where the router is.

Remember, this isn't just about improving connectivity whilst working remotely. There isn't going to be a sudden decrease in the number of internet-connected devices we install in our homes over the coming years. Therefore, extenders, mesh systems or other Wi-Fi devices are a great investment for the future too.

5) Speak to your provider

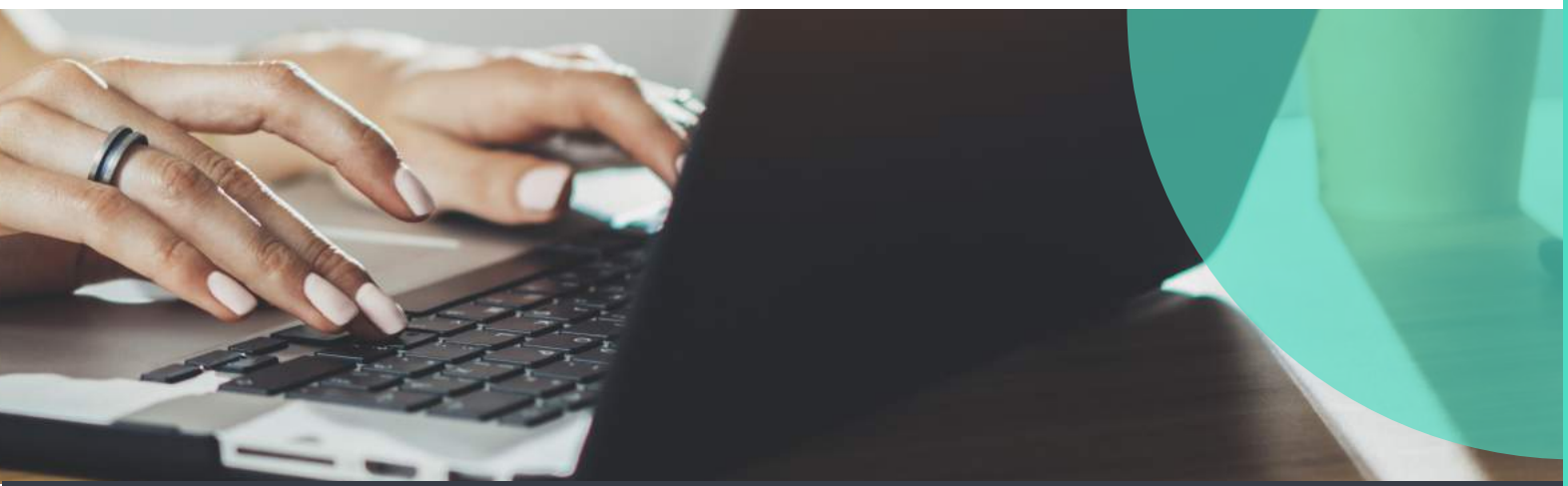
It's an obvious one but, check with your home internet service provider to see if you're able to upgrade your service. It's often possible to subscribe to a faster service without changing provider and possibly even keeping the same hardware at home. Upgrades can sometimes happen within a few hours, so it's a good time to check what service packages are available to you.

6) Check your hardware

Just like a computer, older routers will perform worse than more modern devices. If you have a router at home that's more than four years old, it may well be time for an upgrade, but before you do so, check to see if there's a firmware update or patch that can be applied. In our offices, we are accustomed to keeping networking devices updated but we don't often take the time to do so at home. If you're not sure how to do this, speak to your ISP or search of the instructions for your particular device.

It's also worth 'power cycling' your router – sounds confusing right? You'll be pleased to know that the way to do this is just to turn it off, leave it off for 5 minutes, and turn it back on again! This can often clear faults and the router will often then choose the least busy Wi-Fi channel.

Ofcom has also provided some useful information to help public users to improve their internet connection. The broadband universal service obligation (USO) has said that they will be giving people in the UK the right to request a decent and affordable broadband connection.



Microsoft Teams VS Zoom: video conferencing comparison

Video conferencing applications have become organisations' lifeline during the Coronavirus pandemic and will remain to long after. More people are working remotely than ever before, and applications such as Microsoft Teams and Zoom have had a dramatic increase in popularity as organisations look to continue group collaboration across multiple locations. Both Teams and Zoom are designed to improve communication and can be used for quality video and audio conferencing, both internally and with people beyond your business.

Many professionals are already familiar with Microsoft Teams, which has been integrated with Office 365 for five years now. Yet, there has been a rapid rise in the popularity of Zoom as people search for new or clever ways to connect both for work and with family and friends. Some organisations have been using both applications to meet different needs, so how do you know which tool is the best fit for you?

What is Zoom?

Zoom is a cloud platform for video and audio conferencing that allows you to collaborate, chat and hold webinars. You can join Zoom meetings on any device and bring HD video and audio to up to 1,000 video participants. The application also allows you view multiple camera feeds all at the same time, which has made it a popular choice for large team meetings; it offers 'waiting room' functionality, telephone dial-in and it's easy to control things like muting participants and sharing cameras. Zoom has meeting analytics, such as top users by meeting minutes, and you can save, record and document sessions.

What is Microsoft Teams?

Microsoft Teams helps organisations to communicate more effectively through group chat, online meetings, calling, and web conferencing. Like Zoom, it has extensive video capabilities, but it also enables users to collaborate on files with built-in Office 365 apps, such as Word, Excel, PowerPoint, and SharePoint. It also has the functionality to add in your favourite Microsoft apps and third-party services to keep your business moving forward.

Microsoft Teams has seen over 900 million meeting and calling minutes generated by 44 million daily users over the space of a single week during this pandemic. Teams is a very different product – conference and video calls are one feature, but its core purpose is to bring groups of individuals together into workgroups, giving them ongoing chat windows (think of WhatsApp groups for business) as well shared document libraries and embedded applications and features useful to a specific group.

Security: Teams Vs Zoom

Millions of users have turned to Zoom for their video conferencing needs during the Coronavirus pandemic, and this has led to questions and concerns over Zoom's security. Many have wondered, because of these privacy concerns, how secure Zoom video conferencing is. As a comparison of these video conferencing platforms, users want more reassurances beyond Zoom's video and audio quality.

The application has been criticised for a range of privacy issues, including sending user data to Facebook, wrongly claiming the app had end-to-end encryption and allowing meeting hosts to track attendees. Ex–National Security Agency hacker Patrick Wardle has discovered a range of problems with Zoom's security, including an issue which left Mac users vulnerable to having webcams and microphones hijacked. Zoom has had an unprecedented rise in users from 10 million daily meetings in December 2019 to 200 million daily meetings in March 2020. Zoom's Chief Executive Eric Yuan has said that Zoom are working hard to address these security issues.

Microsoft, however, has stringent security measures in place to ensure personal information is only used to enable user access to subscribed services. Teams enforces team-wide and organisation-wide two-factor authentication to prevent hackers from getting access to people's accounts. Data is encrypted end-to-end, both while in transit and at rest. Files are stored in SharePoint and are backed by SharePoint encryption.

Pricing:
Teams Vs Zoom

There is currently a free version of Zoom, which gives 40-minute-long video calls for up to 100 people. In testing, we have found the Zoom video quality is not as good on the free version of the app and the call quality, overall, is slightly compromised. The 40-minute limit for meetings is quite restrictive for work meetings. The pro-version is reasonably priced, but when you start to look at any additional functionality such as running webinars, for example, the price per month starts to become prohibitive.

Microsoft Teams gives the most value per user per month. As the pricing for Teams includes access to Office 365, which means not only can users access audio and video calling but also the other Office 365 applications, Word, Excel, Outlook, PowerPoint, SharePoint, OneNote, OneDrive, and the list goes on. As Teams comes as part of Office 365, this is a full business solution rather than just a video calling application.

Video Quality Comparison: Teams Vs Zoom

Both Zoom and Teams give organisations video conferencing functionality, or the ability to connect through video and audio. Yet, both apps have beneficial features.

Zoom and Teams have gallery views, giving users the ability to see everyone on a video. Zoom also provides features such as multiple screen sharing to support web-based presentations. Teams includes a robust chat service that allows users to communicate quickly without setting up a conference. Setting up a meeting in Zoom is a little more intuitive than in Teams, but once a user is familiar with Office 365, Teams is very easy to use too. Teams benefits from the full Office 365 integration and functionality, whereas Zoom is focused on just video conferencing.

Which Video Conferencing App is Right for My Organisation?

During this pandemic, we have been using both tools. Office 365 is key to our business and we use it across all areas of the organisation. For instant messaging, file sharing and collaboration, video meetings with select participants and for our online events, we are using Teams all throughout the day. We are using Zoom, however, for occasional team meetings where there are large numbers on the call so that everyone can be seen and heard.

The functionality of Office 365 means Teams would be our first choice as a secure end-to-end solution that includes video conferencing, and of course, because we are already using Office 365, we have an extensive selection of tools unlocked form our subscription.

Part four: Internet Security Whilst Working Remotely

Cybersecurity considerations for remote working

Understanding cybersecurity in COVID times and immediately thereafter is vital to keep your business well protected and guarded against risk. One question that comes up regularly is: “What things (both from a cybersecurity and a technology perspective) should we consider with staff working from home due to the Coronavirus outbreak?”

To answer this, you need to explore the details more closely.

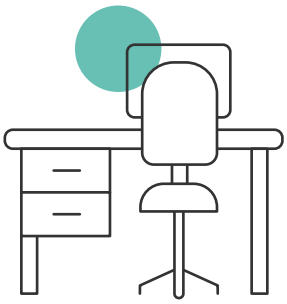
The basic building blocks that you need to be thinking about are:

- **What to and how are you connecting?**
- **When do they need to connect?**
- **Is the connection safe and secure?**

If you allow remote users to connect to your systems, there is always a risk. If their machines are not secure then, by default, neither are yours. Whatever access you’re giving and however you’re going to facilitate it, you need to be thinking about security and your human firewall. Your human firewall is both your best line of defence and your biggest risk.

Cybersecurity in COVID Times (and immediately thereafter)

Cybercriminals are opportunists, and like any other event that can cause vulnerability, they are making the most of the effects of coronavirus in society. Cybersecurity is a buzzword and may seem more relevant now since criminal activity online has increased. What can organisations do to keep cyber safe when employees are working remotely?



Access to machines

A common issue is that in the past, employers have simply asked staff whether they are able to work from home, and have access to a computer, and have been told yes. The nuance with the current scenario, however, is that we need to consider what happens when an entire family is working from home. You need to know if all your staff have sole access to a machine.

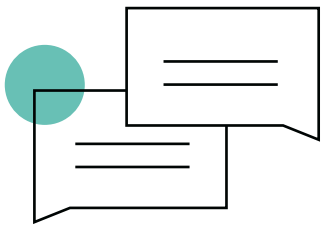
If not, for some the solution is to allow staff to take their work machines home with them (laptop users probably do this anyway). If you're doing this with a desktop you need to think about connectivity. Most home networking is Wi-Fi based, so you'll either need a Wi-Fi dongle or consider long ethernet cable to run from the machine to the home router.

Remote access tools

An increasing number of digital applications are now cloud-based. This makes remote working a lot easier, but for any on-premises applications you are going to need to a remote access tool. Which tool you use will probably be decided on based on what your IT team/provider are most proficient at using, and your appetite for ease versus cost.

Connectivity considerations

With increased remote users accessing an on-premises solution, you may face speed issues due to the size of your connectivity pipe. Many people have a larger bearer (the pipe that carries the service) than the service they are paying for. This is an ideal scenario as it is quick and easy to increase the speed of connectivity for your office.



Anti-virus for all users

One of the most important considerations regarding cybersecurity in COVID times is that a good anti-virus product needs to be used by everyone. For many businesses there is a quality anti-virus policy in the office, but no control over what people use at home. Consider a licensing agreement whereby home users are provided for under the office license agreement. This will allow you to ensure that everyone has good protection. Don't allow users to use a free anti-virus software.

Cybersecurity concerns

Now more than ever you need to put in place a good **password policy** and, wherever available, use **multi-factor authentication** (2FA/MFA).

Don't be fooled into thinking that having a VPN provides you with all the security you need. Alone, that is not what a VPN does. A VPN is about providing privacy and a private connection, rather than a **secure** connection. A VPN is a private tunnel from a user to the main system, and it's imperative that we take the security steps to ensure that the tunnel is secure at both ends. If not, cybercriminals can simply come through the tunnel and attack your systems.

Cybercriminals are making the most of the current environment of heightened fear. They're using Coronavirus-related opportunities to attack users and their machines.

There are a lot of cyberattacks and malware problems being delivered under the guise of either Covid-19 advice or as an interactive Covid-19 Virus Outbreak Map. Please advise your users to be aware of this and not be tempted to click on social media clickbait.

Coronavirus spam

Coronavirus-related spam is also booming now. In addition to the usual filtering platforms, you can reduce the problem by getting your mail domain and system administrator to lock down your generic email accounts.

Account settings

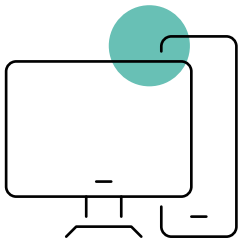
Help safeguard a machine by paying attention to the local-admin account setting. The user account that someone uses on their machine should always be set to 'standard' and not to 'local administrator'.

In the office, your IT team should have this in hand but, at home, many users have a default local administrator account. What this means is that if the machine is compromised, a cybercriminal has full access to make changes and cause maximum harm.

To fix this problem at home, follow these steps:

- first create a new user as a local account (you do this under control panel and users),
- name the account admin,
- change that user's account type to be a local administrator,
- select and change the normal user account type to be standard.

Users should now use their standard account on an ongoing basis, only switching to the admin account when they want to make changes to their machine configuration.



Data protection

You must give thought to what data remote users are generating and where it's stored. This has an implication on your GDPR responsibilities as well as prompting thought about backup needs and requirements. Where possible, save to your corporate system/cloud solution and if not, you may need to consider a local backup solution such as rotating external hard drives.

Webcams and video calling

As more people work from home, we've seen more webcams being deployed. It is worth opting for a camera with a lens cover, or if a camera is not supplied with one add it retrospectively (they can be obtained easily and cheaply online). Most webcams have an activity light but it's possible for malware to disable that. The internet will show you thousands of live feeds from hacked security cameras and you don't want any voyeuristic crime in a home office.

Insurance implications

One last thought, if you are asking staff to work from home who don't normally do so, you might not have thought about insurance implications. It's also important that you ensure that staff still comply with health and safety regulations.

Home working environment

Good advice to staff working from home is to make sure you create a suitable environment that protects you from postural risks, in the same way as you would at work. Make sure you sit at table of a suitable height, using a chair that enables you to comfortably use your keyboard and mouse, and allows you to rest your feet on the floor.

If staff need to take a monitor/keyboard home to work for long periods, employers should facilitate this. Business owners should ensure that managers are talking to their direct reports to ensure that they can work safely and securely.

At a time when business leaders are forced to contend with all sorts of unforeseen complications, because of coronavirus, cybersecurity concerns might not be at the forefront. The truth is, cybersecurity in COVID times is a whole new ball game, and we all need to learn as time goes on.

How to stay protected against COVID-19 scams

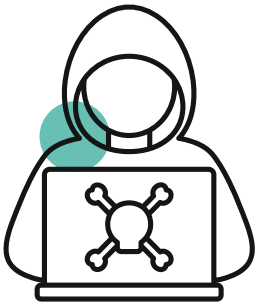
Cybercriminals are unscrupulous people who will capitalise on anything to extort money from individuals and organisations. The current Covid-19 (coronavirus) pandemic is no exception. Since the early days of the virus, we've seen hackers exploiting people's fears by sending phishing emails and messages related to the Coronavirus. At a time when many organisations have taken their eye off the importance of IT security to focus on their immediate response to the UK lockdowns, the impact of these attacks has been greater than ever. Here, explore some of the latest coronavirus cybersecurity scams have been circulating.

Cybercriminals posed as the World Health Organisation (WHO) to steal money and information from the public. The attacks range from fake landing pages, downloads and malicious email attachments all relating to the coronavirus outbreak.

In a press release the WHO said: “If you are contacted by a person or an organisation that appears to be from WHO, verify their authenticity before responding”.

Almost as soon as the Government had announced greater support from HMRC, we started to see text messages supposedly from HMRC, promising a goodwill tax refund if recipients just follow the link.

On closer inspection, there are grammar mistakes in the text, and HMRC has confirmed that they would never text you a link for claiming a tax refund. If you look closely, you’ll see that the link does not look like a legitimate link to HMRC or gov.uk which is a classic sign that an offer is too good to be true. If you are unsure about any text messages, you receive you should always call the company to verify the legitimacy of the message.



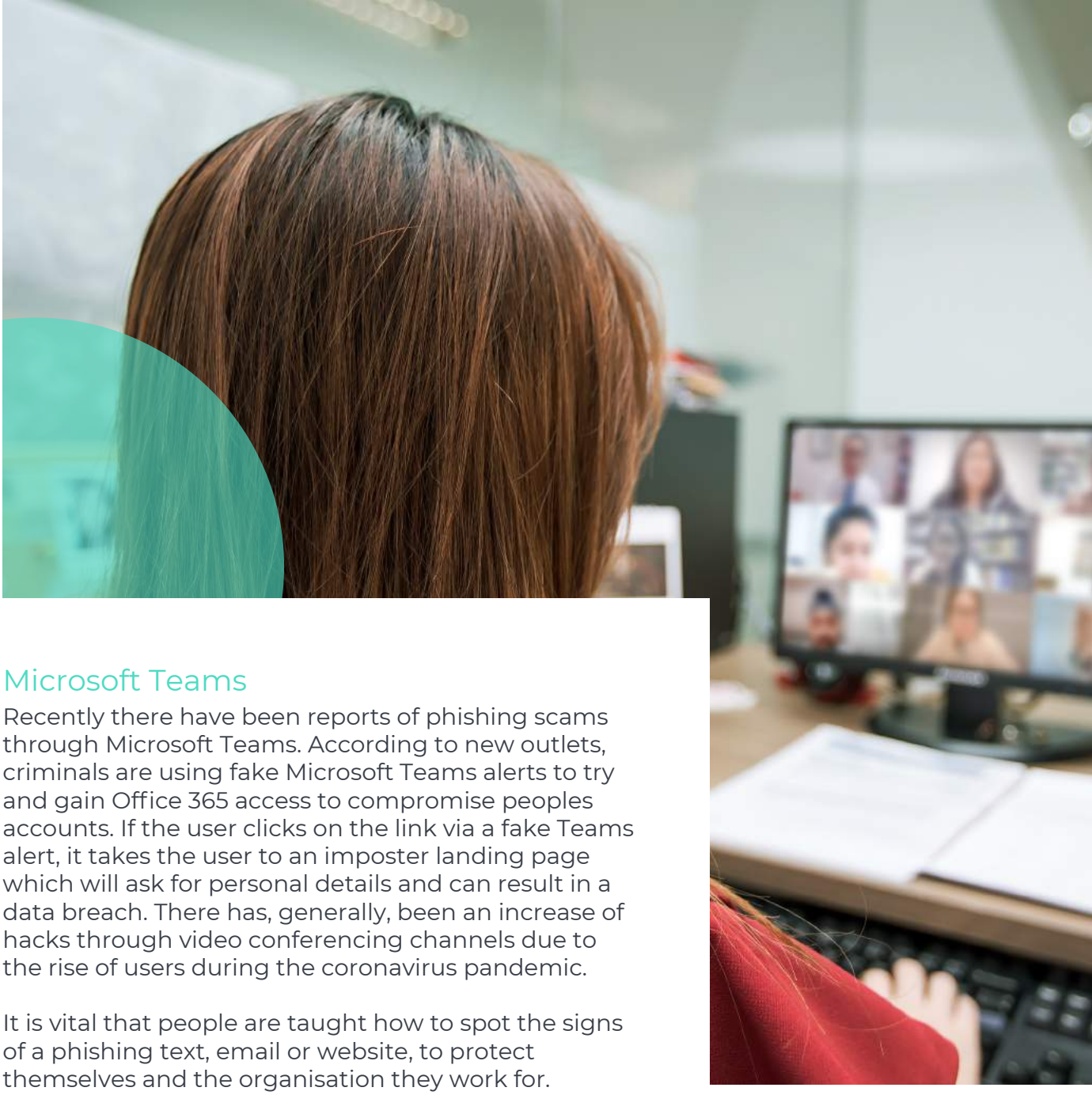
This example of smishing is just one of the most common attacks (a form of phishing where someone tries to trick you into giving them your private information via a text or SMS message). A text supposedly from the ‘City Council’ circulated, for example, stating that you could receive a tax refund. This was proven counterfeit, too. Often poor grammar in the message is a clue – but these are desperate times and people have been falling for this message.

The Gov.uk website has been realistically copied in order to lure people into sharing personal information and, in this example, the website looks similar to the gov.uk site. However, the URL does not look legitimate. The poor spelling also points to the fact that this is a fraudulent website, such as the typo COVID-19 “Relieve” scheme, rather than a relief aid.

And on a similar theme, we’ve also seen emails claiming that the Government has taken action to provide people with a tax refund. This imitated GOV UK with the email design and also had links for the recipients to click on to “Access their funds”.

We’ve said it before – but this just isn’t how the Government would proceed – they wouldn’t ever make it that simple. Remember, if it looks too good to be true – it probably is.

In the example above, the email was directly impacting people’s fears by giving false information on the current pandemic and virus transmission. This email has been created by using the legitimate Centres of Disease Control (CDC) emails, but it has been sent using a spoofing tool. By sending an email of this kind during a period of such high stress and uncertainty, cybercriminals are capitalising on people’s fears to trick them into giving out their details.



Microsoft Teams

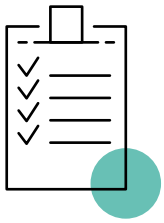
Recently there have been reports of phishing scams through Microsoft Teams. According to new outlets, criminals are using fake Microsoft Teams alerts to try and gain Office 365 access to compromise peoples accounts. If the user clicks on the link via a fake Teams alert, it takes the user to an imposter landing page which will ask for personal details and can result in a data breach. There has, generally, been an increase of hacks through video conferencing channels due to the rise of users during the coronavirus pandemic.

It is vital that people are taught how to spot the signs of a phishing text, email or website, to protect themselves and the organisation they work for.

During the lockdowns, the UK government worked with various social media firms to help to stop the spread of fake news and dangerous content – launched under the banner of their 'Don't feed the beast' campaign - to help the public think about the content that they are sharing on the internet.

The key message here is to be extra vigilant when reading emails and text messages related to the Coronavirus. Many hackers are currently exploiting people's nervousness through phishing attacks. Many employers have taken their eye off the ball when it comes to cybersecurity as they have taken a 'do whatever it takes' approach to getting their people set up to work from home. This is not the time to cut back on your security services, and indeed, perhaps this is the perfect time to get your staff to spend some extra time on cyber awareness training.

Are you planning for coronavirus in your business?



Your planning

We can learn from other pandemic outbreaks in recent years and can sensibly predict that more remote working is likely to be needed over the coming months. We've already seen examples of organisations employing remote working habits for the longer term.

It is, therefore, essential that you consider your ability to facilitate staff working remotely. It is therefore essential that your remote working policy is fully tested as a matter of urgency. In the past, we have seen many organisations leave it until their office has been cut off (by snow, for example) before they have issued instructions to normally office-based colleagues, on how they can access systems remotely.

Whilst some clients are fully cloud based, others depend on VPN connections to work remotely. You need to consider whether you have enough licenses and bandwidth if suddenly, your entire team will be working from home, rather than perhaps a handful that do so routinely.

You also need to consider what services will work remotely, thinking about phone systems, email, access to files, CRM systems, finance systems etc. If any of your core platforms are not routinely worked on remotely, now is the time to test and plan.

Questions to ask of your organisation:

1) If you start to see unusually high absenteeism and several of the team are coughing and feeling unwell, what are the implications? Who can work remotely? Do you need to make further allowance for this?

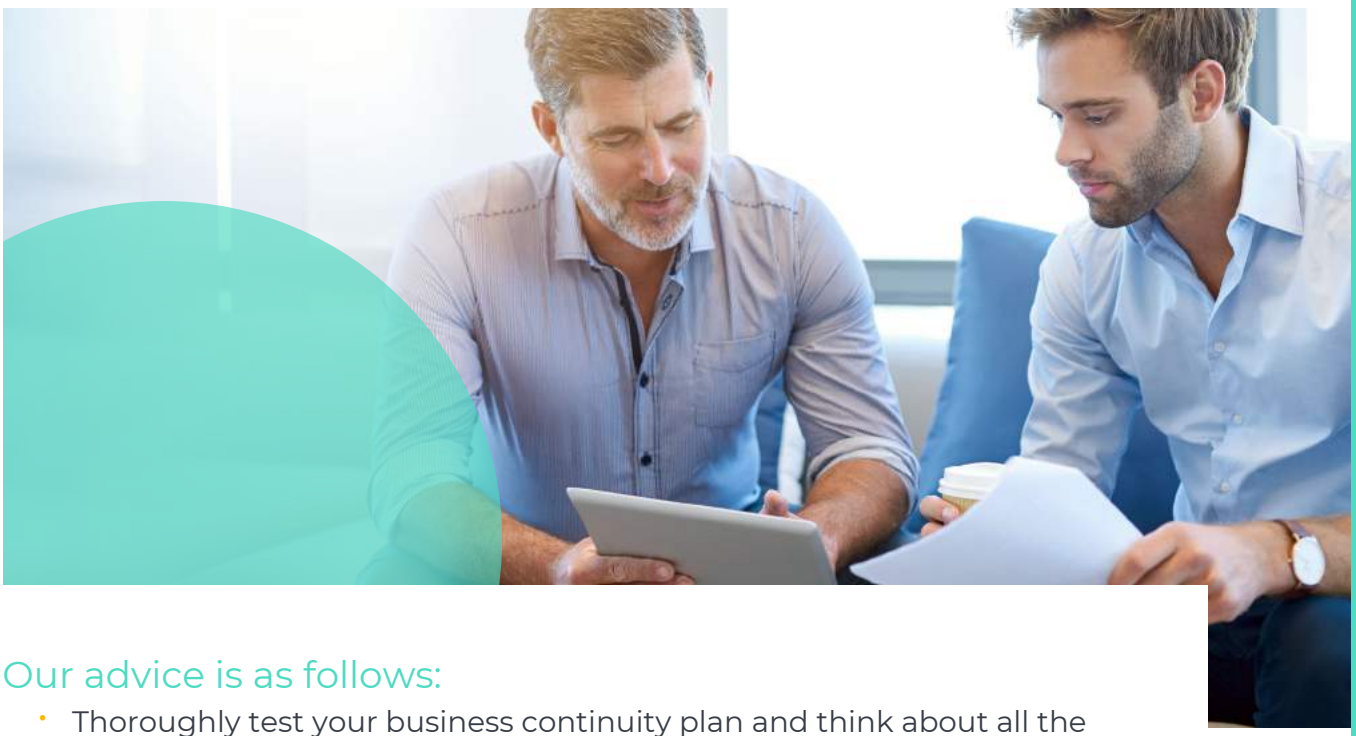
2) What happens if a key supplier must close again? Or are there any members of your team that have unique skills or knowledge? What are the implications of this and how can you reduce the risk?

3) How will you deal with staff who don't attend work? What do your policies say? How will you deal with the workload? Think about how many people are needed to provide your service too, if your staff numbers were to drop to just 20% what does that mean to you?

4) Another gloomier consideration is what happens if a member of your team were to die? How do you communicate this? How do you support your team and their natural grief? What happens to that person's desk or email auto-response? It seems callous to be thinking of this but unfortunately, we've witnessed this in other businesses (for other tragic reasons), and we've seen how hard it is to think about these things in the middle of the crisis.

5) Then there are press considerations, if news of your colleague's infections is picked up on social media how do you deal with the inevitable interest from the media? Who deals with them?

6) You might also consider a scenario where you need to boost your numbers using temporary staff -what could they usefully and successfully do? Can you do anything now to help plan and prepare for that situation?



Our advice is as follows:

- Thoroughly test your business continuity plan and think about all the questions raised in this blog
- Test your remote working plans to ensure that they work as you expect them to. Test remote access to applications used by staff that don't typically work remotely, and test what happens if a larger group of employees than usual, need to work remotely
- Communicate your plan for a post-pandemic recovery to your employees to reassure them there is a plan in place
- If appropriate, communicate with customers, partners, suppliers and other stakeholders of the organisation to check their plans for a further Covid-19 outbreaks
- Encourage any unwell employees to stay home. You may need to adapt sick leave policies to support this
- Identify your employees or departments with critical skills to ensure a backup plan is in place if any of these are affected
- Cancel non-essential travel and all travel to the most affected areas
- Provide tissues, alcohol-based hand sanitiser (antibacterial hand gels) and encourage good hand hygiene
- As the adage says, if you fail to plan in business, then you plan to fail. The best time to consider disaster is when you're not in the middle of one.

ramsac Limited
Godalming Business Centre, Woolsack Way
Godalming, Surrey
GU7 1XW

www.ramsac.com
01483 412 040

ramsac
at the heart of IT