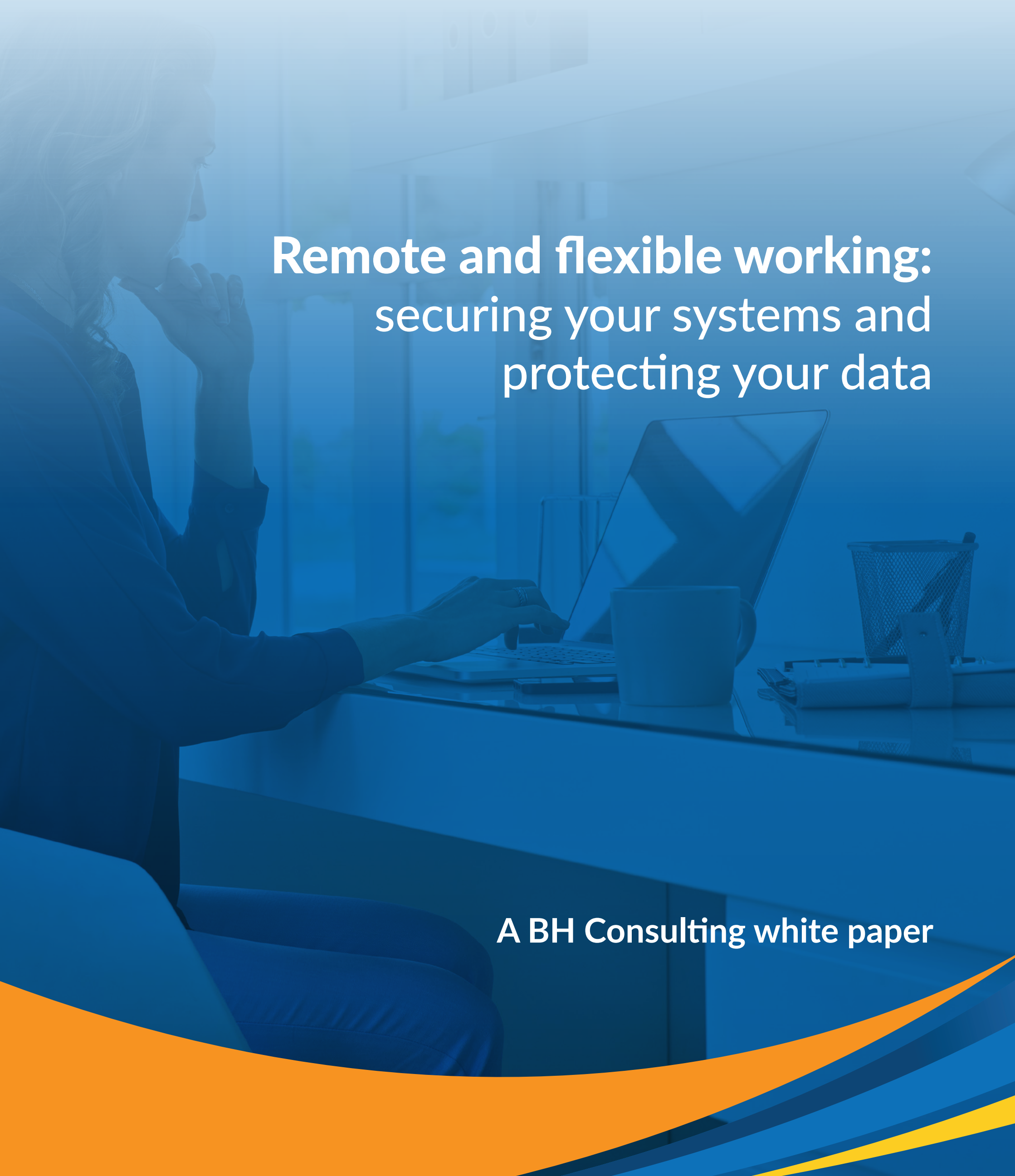
BHConsulting
Your Trusted Cybersecurity Partner



Remote and flexible working: securing your systems and protecting your data

A BH Consulting white paper

Remote and flexible working arrangements are likely to play a much bigger part of normal operations for many businesses as they start thinking about working life after Covid-19. This is both an opportunity but also a challenge – especially when it comes to security and data protection.

BH Consulting has prepared this white paper to help businesses and public organisations of all sizes to think about current gaps in their security when it comes to remote and flexible work. Using the advice in this guide, they can put in place a plan that enables efficient, productive work while minimising risks.

Risks and risk factors

Security researchers and law enforcement agencies have noticed a marked increase in cybercrime activity related to the Coronavirus pandemic, such as phishing scams and financial fraud, but remote working carries other risks that are present at all times. They include:

- Ransomware leading to business interruption
- Potential disclosure of sensitive information
- Corruption of sensitive information
- Loss or theft of assets containing company information
- Non-compliance with legal, industry and regulatory requirements
- Exposing users to risks such as disclosure of data, cyber-attack and system downtime.

These are some contributary factors to the risks of remote working:

- Unmanaged devices
- Unmanaged network/communications
- Unmanaged apps / cloud / services
- Loss or theft of device
- Printing, physical documents (shredders, etc)
- Data leakage – copying of corporate data to unmanaged device or system
- Corruption of company information
- Communications (to and from staff)
- Managing staff remotely (line managers)

Action to take

In the current climate of working from home, businesses have choices to make. They can either dictate what staff can and can't do, and rigidly police that. Or they can talk to their people, listen to what they have to say, get an understanding of the environments they are working in, and facilitate them as much as possible.

- Provide staff with clear rules around remote working: all parties should agree clear definitions of 'flexibility' to avoid any risk of misinterpretation.
- Understand the kind of working environment that employees have at home and facilitate secure working as much as possible. .
- Check if equipment that employees use, such as laptops, tablets or smartphones, are personal devices or company controlled.
- Check whether it is possible to ensure those devices are patched and up to date with the latest software versions, encryption and security tools.

It can help to have a member of staff with knowledge of technology and security on standby, to give advice and guidance on what to do in an open and non-judgemental way. Some workers may not know which anti-virus product is the best at any point in time, and for every type of device.

For businesses that do not have a fulltime security professional, or in-house IT manager, should continue to work with their usual IT support provider. Staff may need to have someone on standby to reach out to if they encounter a problem.

Culture and remote working

Working from home is a huge cultural challenge as much as a technical one. Managers of a business must set the right tone. When it comes to security, many incidents are due to human error rather than malicious action, and managers can encourage proper reporting by reminding their staff that it's acceptable to make a mistake.

It is more important for staff to know they can (and must) call it out if they think they made such a mistake, which might lead to a data breach or may have caused a malware or ransomware infection. The worst thing they can do is say nothing – which is why open, regular, open, and hopefully honest communication is essential.

Strengthening security: technical controls

Make sure your remote access solution is secure

There have been recent real-world examples of networking hardware being attacked by criminals through newly discovered vulnerabilities, so you need to check if the hardware and software your business has in place is up to date and secure. Ask your IT or network provider for advice if you're not sure.

Secure your email service

Email is a critical business tool at any time. Many companies, especially small businesses, use the Microsoft 365 suite, which comes with the Outlook email application. rather than assuming the default installation will be enough, run the cybersecurity self-assessment tools and apply the extra security features available. Take the extra steps to make it harder for attackers to breach, or else you could be exposing important financial or sensitive information. If you don't have the in-house skills to do it, ask your IT support provider to do this for you. (Here's a similar offering for Gmail)

Ensure laptops/devices have hardware encryption

This control is a must: encryption is fundamental. If the business doesn't already have this enforced on all laptops and mobile devices (including removable storage such as USBs), you might need to give the IT manager the ability to connect remotely to an employee's system to set up the encryption or facilitate it so the employee can do it themselves. This alone will significantly reduce your exposure if you do suffer a breach.

Make multi-factor authentication (MFA)/ two-factor authentication (2FA) mandatory for remote workers

This is another essential security control to put in place because it greatly reduces the chances of bad guys using compromised passwords to access your information. Apply this control for company email and for accessing any critical systems or applications, wherever you possibly can.

Refresh security awareness training

Test employees' knowledge of common security risks and check their reactions to incidents.

There are other steps you can take to promote good employee behaviour that help to protect important systems and data.

- Encourage staff to use a password manager
- Stress the importance of not sharing passwords (which often rises when remote working), including with your kids
- Where necessary, suggest that screen filters are used to make shoulder-surfing harder
- Remind staff not to open links or documents from suspicious sources or with unwarranted content, such as those with Coronavirus / COVID-19 information, as there are a large number of malware-infected scams out there
- Remind staff about the need to protect confidentiality
- Ask staff not to defer critical updates to software
- Remind staff that surfing illicit websites, amongst other things, can be dangerous to your device, and a breach of company rules from a company one
- Staff must not visit sites like illegal movie websites because they pose a risk of ransomware and malware infection
- Remind staff not to leave company devices in the care of children or other family members

Review the business continuity plan

Apply the experience gained during the restrictions to examine the business continuity plan (BCP) in detail and assess if it's fit for purpose. Was there an existing plan? When remote working became mandatory, did the plan work effectively as outlined? Did it include all of the options that were used to keep the business operating?

Reviewing, or creating, a BCP, is the responsibility of the senior management team or CEO: it's much more than just an issue for IT, security or risk departments.

BCP is often spoken of in hypothetical terms. It usually involves thinking about a range of potential scenarios and asking the question: "what would happen if...?"

Take a fresh look at where you might apply practical lessons based on experience. If it were possible to plan for a situation where remote working was mandatory for everyone, and the office was unavailable, what would you do differently?

Look at the BCP through the lens of people, process and technology. Why not start with an extreme example:

- Suppose for reasons of security, the company policy stated we didn't allow remote working at all? Clearly, in a situation like the one we're in now, that wouldn't work so we'd look to circumvent it. We need to write our policies and plans to be flexible enough to deal with extreme scenarios.

- Suppose the current plan calls for all employees to work from home using company laptops if a lockdown happens again. What if just a handful of people regularly bring their laptops home with them? What if the rest of the machines are still in the office that's locked up and no-one can access? Do you have the capability to pop down and order new laptops? Would the nearest store have enough stock? Do they have the apps and systems you need?

- In the past, some companies only granted permission to a privileged few to work from home out of hours. But if there's a situation where the office is physically 'out of bounds', does the business remote access solution have enough capacity for dozens, maybe hundreds of staff? Will all staff need tokens, fobs, or some other form of access control?

- What other equipment will people need to keep doing their jobs effectively and productively? Do they have proper chairs for their home office? (That is more important than you might think, since many people will probably be spending longer hours in them.) What about monitors? Will mobile phone contracts need to change during lockdown because employees will be consuming more data or making more calls?

Every business and workplace is different, so the BCP and the policies underpinning it need to take account of those specific situations. The plan might also need to be flexible enough to apply different sets of rules as circumstances dictate.

It's worth looking at the BCP through the lens of what happens when policy meets practice. Get different sections of the company involved in running desktop scenario exercises: ("Problem X, Y or Z has happened, what happens next and how would we cope?").

Now is the ideal time to see whether your BCP, as it's currently written, stands up to real-world experience. What gaps are there? Should there be multiple options: a plan A, B, C and very possibly D as well? And if you don't have one, what better time to write your first BCP?

Secure meetings

When working remotely, online meetings and conference calls become a feature of the working day. Here are some general tips to ensure privacy and security.

- Remind staff to MUTE the microphone when they are not speaking in a conference call
- Educate all staff to ensure webcams are blocked by default
- Remind staff NOT to leave their machines UNLOCKED, especially during a call or when visiting the bathroom
- Ask staff NOT to work from coffee shops or public places (if possible) – especially if they are on confidential calls or working on confidential documents.

Zoom became one of the de facto tools of choice in the early days of working from home during the Covid-19 restrictions. But closer scrutiny highlighted some security and privacy shortcomings, including meeting IDs that were easy to guess and brute forceable, allowing anyone to access and hijack them. If a meeting host failed to set screen-sharing to 'host only' or to disable 'file transfer' for the call, outsiders could share malicious software or other nefarious documents or images. While some of the guidance below is specific to Zoom, much of it applies to any conferencing or communications tools.

What to do (attendees)

- Each time you are invited to a Zoom meeting via a link in an email or document, check it before clicking to make sure it is a legitimate link
- Be cautious with all emails and files from unknown senders
- Keep your laptop or device camera blocked and only open it when you choose to permit the video to be used
- Do not take screenshots of the meeting unless you have made people aware that you are doing so
- Be aware that all chats, including private messaging, during a call are recorded and are available to the meeting host and the administrator.

What to do (hosts)

- Don't share the meeting ID publicly; restrict it only to those you wish to attend the call
- Avoid using your Personal Meeting ID (PMI) to host public events, as this may be hijacked by others
- Add a meeting password to your Zoom meeting and only share that password with those you wish to join the call
- Allow only signed-in users to join
- Add a lobby to your Zoom meeting and only admit those you wish to join your meeting from the lobby
- Put each participant on a temporary hold until you're ready to have them join. This allows the host to screen who's trying to enter the event and keep unwanted guests out
- Lock the meeting after it has started, so no new participants can join
- Don't give up control of your screen. Should you give control of your screen to another person, they can then manage the call.
- Where possible, do not discuss confidential or sensitive information on a Zoom conference call
- Where possible, do not record calls unless you absolutely must. If you wish to record a call, make sure all those attending the meeting are aware you are doing so
- Assume all chats may become public. You have little or no control over one of the participants taking screenshots or other types of recordings
- You may want to disable video to block unwanted, distracting, or inappropriate images on video
- You may want to turn off file transfer to prevent the chat from getting unwanted content
- You may want to turn off or control annotation during screen share
- You may want to disable private chat to stop participants from messaging each other privately and restrict participants' ability to chat with each another during your meeting
- Remove unwanted or disruptive participants. There is a function to allow removed participants to re-join in case you remove the wrong person.

What to do (administrator)

- Familiarise yourself with the security functions and additional options available; enable them if appropriate to do so.
- Enable Multi-Factor Authentication to add additional protection to your account
- Ensure the administrator account uses a strong password. Anyone with access to this account can download any recorded videos, add themselves to sessions and control the security of the entire system.

Copyright Notice

Disclaimer:

BH Consulting has made every reasonable effort to ensure that information contained within this document is accurate. However no representation or warranty, expressed or implied, is given by BH Consulting as to the accuracy or completeness of the contents of this document or any information supplied. Recommendations outlined in this document are based on accepted industry best practises.

The information contained in this document has been provided by BH Consulting for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate BH Consulting gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of BH Consulting will be corrected as soon as possible.

Any views, opinions and guidance set out in this document are provided for information purposes only, and do not purport to be legal and/or professional advice or a definitive interpretation of any law. Anyone contemplating action in respect of matters set out in this document should obtain advice from a suitably qualified professional adviser based on their unique requirements.

The information in this document may contain technical inaccuracies and typographical errors. The information in this document may be updated from time to time and may at times be out of date. BH Consulting accepts no responsibility for keeping the information in this document up to date or any liability whatsoever for any failure to do so.

BH Consulting are under no obligation to update this document or correct any inaccuracies or omissions in it which may exist or become apparent.

For more information please contact us:

+353 (0)1 440 4065

info@bhconsulting.ie

www.bhconsulting.ie