Remote working - Ensuring the risk remains remote.

March 2020

Made possible

QBE

The Covid-19 pandemic and recent Government directives are forcing us to work remotely, more extensively and more rapidly than perhaps planned. For some businesses, remote working already forms part of their day-to-day operations, albeit perhaps to a lesser extent than we are likely to see. For others, it will be a completely new way of working. It has great value in the current situation and as an aid to business flexibility generally, but this can be offset by increased risks. This guide aims to highlight areas of concern so that remote working practices can be developed to mitigate those risks.

System access and resilience

How well do your remote access systems work if a significant percentage of your workforce (potentially all of them) are logging-in remotely?

If you do not know the answer to this, it is important to find out quickly. Arrange a test whereby you ask everyone to log in to the work network at a certain time, *at least 50% from home* (asking them to do so from the office environment is likely to give a false positive), but ideally (if not done already), have a full test day where all, or nearly all staff attempt to work from home. Collate feedback on the results and the problems. Remind everyone about the IT help channels available but be prepared for this function to become a bottleneck and require extra resources.

How many people would be able to access all their work-critical systems from home, if, without warning they discovered that they were unable to access the office?

People will likely need reminding to take laptops home but if left in the office, will they be able to access relevant systems from their own device if necessary? Does that option provide them with access to all necessary systems for their role? Certain functions, such as HR and Accounts, and some limited licenses software may require specialist access rights. Identify these requirements early and consider workarounds to ensure service continuity.

Secure access and work practices

Do you have a policy on secure remote working, which addresses use of public WiFi, working in public places, and security controls if using employees' own IT equipment?

Working outside of the office environment means fewer controls on how and where people work. It is critical that you have a comprehensive and clear policy on remote working. Staff should be issued with summary guidelines highlighting the key messages and requirements, as this is much easier to reference than a full policy and so more likely to be followed. This should extend to wider issues about ways of working; rules for taking hard copy files and documents out of the office, and for protocols for telephone/other conversations in public, as well as security precautions to be taken to reduce the risk of lost devices (memory sticks, smart-phones, tablets and laptops) are equally important. Links to QBE template checklists are provided at the end of this guidance note.

Even with encrypted connection to the work network, once logged in the risks are significant. If your staff must access WiFi on the move, provide them with a smart-phone and an unlimited data-plan SIM to provide a 'WiFi hotspot'. This has the added benefit of providing a secondary internet connection on occasions when a broadband service has an outage for any sustained period. If there is absolutely no alternative to using a public WiFi, (including those that require log in or a password - which are no guarantee of additional security), ensure that connections are made:

- through a VPN; and
- with 'File Sharing' turned off (in Windows 10: Settings/Network & Internet/Status/Sharing Options)

Wired / ethernet connections For more information, view the National Cyber Security Centre resources on Home & Mobile Working.

Your usual penetration tests could be redirected to focus on aspects of remote working to identify areas of vulnerability.

Are all your employees working on Windows10 (or up-to-date Apple OS) computers, with current anti-virus software, and all latest patches installed?

Windows7 is no longer supported, and is therefore insecure, regardless of what antivirus technology is installed. If staff are using their own devices, any security update should be circulated (and acknowledged) requiring work systems to be accessed from Windows10 devices (or equivalent up to date Apple computer). It is also worth enforcing the message, at intervals, that security patches must be installed promptly, or auto-updating employed.

Are staff familiar with relevant policies and procedures, and are they easy to find and follow?

It is essential to keep staff regularly updated on the organisation's policies and procedures for protecting them and the business - particularly when working remotely as there is a greater risk of people's behaviour altering and exposing the business to cybercrime, fraud or data breaches. Issuing a policy is not enough. Other forms of education and awareness should be employed to ensure the policy requirements are clear to all staff that may undertake flexible working even on the odd occasion. Everyone should be expected to follow policy - from Board Executives to front-line staff.

Awareness training should include the following (and any other key requirements relevant to your organisation):

- Best practice security guidelines for remote working (including the consequences of poor practices)
- Social engineering including Phishing/Vishing/Smishing risks – attacks are already on the increase as criminals exploit the remote working push necessitated by the pandemic. Awareness should be raised that using mobiles and smaller screens generally, makes it difficult to spot a phishing email so extra vigilance is needed
- Secure storage and handling guidelines (information in transit, and in situ) including controls for removal of files and documents - and retrieval from home locations should people become unwell
- Incident reporting and next steps/damage limitation
- Bring Your Own Device (BYOD) policies
- Social media guidelines
- Personal security (e.g. social media, email account, internet banking and shopping, password management).

Are there other information security controls that you should be implementing?

There are many technology-based tools and controls that can assist make remote working as safe as possible. Speak to your IT manager or consultant. You can also refer to our technical security tips, appended to this guidance.

Supervision

Have arrangements been put in place to ensure that there are regular update/review meetings between team leaders and their staff, whether or not those staff are physically present in the office?

In an open plan office, supervision can be continuous to an extent but that is clearly limited in remote working conditions. Frequent, regular and structured catch-ups will need to be agreed for each homeworking individual, based on the type of work, level of experience, remote monitoring capability etc. There is no 'one size fits all' and arrangements should always be risk-based. Where homeworking is limited to, say, a day a week, it may not impact on the existing supervision arrangements, however day-to-day authority levels, sign offs and reviews needed should be made very clear. If you operate a central document/file management system, and it is well used and effectively monitored, this also provides a valuable form of ongoing review, and aids service continuity, should a staff member become suddenly indisposed.

Some processes including approvals and escalation of concerns may be reliant on a limited number of individuals so build capacity and flexibility of cover for key functions that may be more susceptible to illness.

What central management reports can you run, and how valuable an insight do they provide into key operational metrics for supervision?

Management reports should enable risk behaviours and factors to be identified remotely, for example:

> work / file inactivity

> high work-in-progress levels and those nearing or exceeding fee estimates

> out of scope workload and/or variety

> imminent deadlines / key dates

> high-risk triggers

> unusual patterns of file downloads

> unusual patterns of payments.

What system-based risk controls do you have in place?

As the above suggests, well designed systems allow detailed reporting metrics. They also can provide another line of defence, particularly useful when staff are remote working, by building in alerts and supervisor sign off requirements at key stages or when certain high-risk flags are triggered. In the absence of systematised controls, it may be worth putting in place reporting templates which form the basis of regular review meetings between remote teams and their managers.

We see many claims even during normal working times where distractions are a contributory factor - working at home during holidays or whilst travelling. The level of distraction looks set to increase considerably, with children and/or sick relatives at home for extended periods and the challenges that could bring to what might normally be a quiet place to focus. Be aware of this heightened risk - double check and check work again, or better still, operate a tighter review protocol for work considered to be at higher risk.

Even basic service continuity arrangements will be important for preventing claims so client communications management will be vital. Ensure that:

> forwarding of office landline calls is working fully

> physical post is scanned/copied and accessible in the usual way (although email may be further encouraged)

> Clients are reminded about the importance of checking that instructions and documents have been received, especially when deadlines are tight.

Work risk assessments

Can any pre-emptive strikes be made to spread workloads and advance manage potential issues?

Work that is in-progress or due to start, will be impacted by remote working, where resources become stretched, and when the surrounding infrastructure and economic conditions change with likely impacts on project planning, key dates and deadlines, contractual conditions, and client relations. Reviews should be conducted for each team to ensure all work matters are risk-assessed as to likely impact and where possible, pre-emptive action agreed with clients.

The importance of keeping records up to date should be strongly emphasised, given that more frequent handover of work may be needed due to illness.

For lawyers, some excellent technical considerations are recommended by QBE panel lawyers Beale & Co in their article on Limiting the Risk of PI Claims during the Coronavirus Pandemic and the Law Society has looked at potential factors in Residential Conveyancing transactions specific to a pandemic situation.

Prevention of financial crime

Will your controls withstand extended remote working whilst being targeted by fraudsters determined to exploit the situation?

It is essential that the robust controls put in place to prevent financial crime are not undermined by remote working and/or resource shortages. Fraudsters will always use the uncertainties and vulnerabilities of the time to apply social engineering techniques to exploit those weaknesses - especially when individuals are isolated from the pack. Email traffic is likely to increase in extended remote working circumstances and this could be used to mask spoof emails such as fake ‘updated’ payment details for salary or purchase payments. Levels of awareness around social engineering always need to be maintained and refresher training sessions held at appropriate times.

Made possible

QBE

In relation to payment fraud on client accounts, our standard advice to have a three-tier verification process (two-tier in micro-businesses) involving requester, approver, and releaser all independently checking payment instructions against evidence of authentic bank details should be maintained regardless of the location of the parties involved. Ideally, a core checking team will continue to operate centrally, but if that is not practical, a process for remote checking or collaborative checks using screen sharing should be available so that risk management controls are never dependent on a single person verifying payment details, particularly if there is email correspondence providing different details to the original ones provided.

How will your usual visual checks for Client Due Diligence be conducted if clients cannot attend? Simple videocalls may be a solution for some. Greater use of local agents and electronic searches may be needed but if the latter has limited licenses or other restrictions, flexibility may need to be negotiated with your service provider. Think also both about accessibility to the CDD function from home, and how your escalation process will work should concerns arise in the search results.

Knowledge sharing/ communications

Are periodic team meetings and cross-team meetings arranged, in person where feasible, to counter siloed working?

Regular face-to-face contact helps foster a co-operative, shared organisational culture, and enables the most effective exchange of ideas and information. Home workers can be liable to miss out on the social interaction and learning infrastructure which the office environment provides. This includes day-to-day discussion, regular team meetings, training sessions, access to reference documents etc.

Use telephone and video conference tools (such as Skype and Microsoft Teams) to better enable both formal and informal one-to-one meetings and group settings, particularly for intermediate periods when in-person meetings are not possible. Functionality should be tested for both internal and external meetings involving clients and other stakeholders. A start-of-week short update call for departments/teams is recommended.

Health & safety and mental health

Have you made adequate provision to address health & safety, including mental health, requirements of remote-workers?

Anyone who works at home for any period, whether ad-hoc or for extended periods, will need to undertake a workstation and display screen assessment to ensure everything is set up to prevent strains and injury. Other checks should include fire hazards, ventilation, heat and light, lifting & carrying etc. to ensure a comfortable work environment. Training and assessments can be combined and should be refreshed periodically. Ensure you have relevant policies in place to support this. The Information Guide on Managing Remote Working by IOSH includes three ready to use checklists for assessment, feedback, and audit of remote working.

Time and money will likely need investing to ensure all home working set-ups are of the desired standard so the time and amount needed for this should not be underestimated as assessments and outlay will likely be needed for each individual. For longer-term home workers, provision will need to be made for items such as:

- ergonomic office chair and possibly a desk if adequate working space is not available
- docking station set-up including keyboard, mouse and monitor/s as working on laptops and/or iPads for extended periods is not recommended
- possibly a printer, depending on how central support will function, and if so, consider the need for shredders
- telephone line/broadband (or you may opt for the employee to bill you for a proportion of the cost of their existing telephone/broadband line rental)
- miscellaneous items including stationery, foot/head/wrist rests, etc.

Isolated working, working under non-routine and sub-optimal arrangements, and covering for others' absence can lead to anxiety and stress for some people but will be linked to the amount of time they are spending under those circumstances. A buddy arrangement and a regular check-in regime, both for one-to-one or using a team-talk facility like Skype or MS Teams can help people feel more in touch. More guidance on caring for your mental health while working from home can be found here.

Insurance

Are relevant insurances in place to address home working risks?

As an employer, you should tell your Employer's Liability insurer that you are arranging remote working for your staff. It's also a good idea to recommend that your employees discuss working from home with their home insurance provider.

Closing Thoughts

Whilst it's difficult to think about future contingency events in the present uncertainty, capturing feedback on how well continuity measures are working, and keeping records of discussions, decisions and actions taken in response to the myriad of guidance, will ensure that come the debrief, the right improvements lead to even better levels of resilience.

Resources

QBE Template - Technical Security Considerations for Businesses

A template that businesses can adapt and use to review the level of security controls in place for mitigating against remote working risks. The guidance provided can help businesses to consider and identify what the most effective security controls might be for their business needs.

qbeeurope.com/documents/index/23371

QBE Template - Remote Working Security Checklist for Staff

A template checklist of security requirements that businesses can adapt to reflect their own, and provide to their staff, enabling them to understand and become familiar with the security requirements they must follow when working remotely.

qbeeurope.com/documents/index/23374

QBE Template - Remote Working Reminders Handouts

A template hand-out available for businesses to update with their own remote working priorities, before providing them to staff, to serve as a continuous reminder when out of the office. Printed on A4 paper or card, this produces 2 A5 hand-outs.

qbeeurope.com/documents/index/23376

Contacts

Deborah O'Riordan
Practice Leader
+44 (0)7786 734542
deborah.o'riordan@uk.qbe.com

Jaini Gudhka
Senior Risk Manager
+44 (0)7900 088 321
jaini.gudhka@uk.qbe.com

Calum MacLean
Senior Risk Manager
+44 020 7105 5723
calum.maclean@uk.qbe.com

QBE European Operations

Plantation Place 30 Fenchurch Street
London EC3M 3BD
tel +44 (0)20 7105 4000
QBEeurope.com

Made possible