Homeworking

Homeworking – The Risks

Homeworking without supervision

There will always be greater risks for lone workers such as a lack of motivation, lack of understanding with no direct supervision or anyone to assist if things go wrong. It is important for organisations to keep in touch with lone workers, including those working remotely, whether that is at home or a different external environment such as working on a client's site.

Organisations should ensure regular contact to make sure they are healthy and safe. If regular contact is not maintained, workers may feel disconnected, isolated or abandoned. This can have an impact on the stress levels and mental health of workers.

The home working environment does not have the same level of physical security that would be present in most offices. If home workers are likely to be working on sensitive material then consideration needs to be given on how they can prevent people in their household from accessing the information, and the measures that the home worker need to take to protect against the threats of theft of equipment or documents.

Screen and Mental Fatigue

Computer work comes with a number of health-related issues, although steps can be taken to reduce the risks:

- Breaking up long spells of computer work with rest breaks (at least 5 minutes every hour) or changes in activity,
- Avoiding awkward, static postures by regularly changing position,
- Getting up and moving or doing stretching exercises,
- Avoiding eye fatigue by changing focus or blinking from time to time.

Working from home makes these precautions more important because of tendency for some home workers to take less breaks.

Lack of Productivity and Stress Related Issues

Working from home can result in a fall in productivity if workers become complacent and do not continue to push through without the office effect and social pressure from colleagues. To mitigate this risk and ensure that homeworking meets the organisation's requirements, workers should stay in touch with their colleagues whether via remote meetings or on-line collaboration applications.

Homeworking can cause work-related stress and affect people's mental health. Being away from managers and colleagues may make it difficult to get proper support. It is important to put procedures in place so managers can keep in direct contact with homeworkers and can

recognise signs of stress as early as possible. It is also important to have an emergency point of contact and to share this so people know how to get help if they need it.

How to setup a secure homeworking environment

Virtual Private Network (VPN)

Many people are familiar with using a VPN to encrypt our internet traffic, so that it is unreadable to anyone who intercepts it. This theoretically makes it unreadable by third parties including your Internet Service Provider (ISP), government agencies, or hackers. It is however worth noting that using a VPN can slow down internet speeds. If you need to perform high-bandwidth tasks such as holding video conference calls, you need a VPN known for its speed and reliability.

Regularly Patching of Software

Updates to device software and other applications can be a source of annoyance, but they really are important. Updates often include patches for security vulnerabilities that have been uncovered since the last iteration of software release. In many cases, you can set updates to run automatically, often while you are sleeping, so you do not have to worry about downtime.

Backing up data

While hardware backups are still an option, one of the most convenient and cost-effective ways to store your data is in the cloud. Cloud backup services come with a wealth of options enabling you to customize your backup schedule and storage options, but they also raise several security and data protection issues.

Cloud backups will automatically save and sync the files on the computer to the cloud as opposed to cloud storage where it is done manually through selection and storing the documents on drives in the 'cloud' to free up space on hard drives.

One technique that some providers offer is that data can be encrypted so making it impossible to access without the appropriate decryption key. This means that even if the data is copied or accessed without authorisation then the data is not readable. The security of such a service depends on the strength of the encryption mechanism used and the protection given to the encryption keys used to lock and unlock access to the data.

Backing up personal data in the cloud can be problematic if data ends up in countries that do not have laws in place to protect data privacy.

When using cloud backups for your data you should ensure you have checked any offshore policies that your organisation has for storing sensitive data. For example, many countries enforced new regulations where customer data needs to be stored in the user's country of residence. Data protection laws differ greatly between countries. This applies to both data and the parties who can access it. In addition, some countries or jurisdictions may be lacking the same level of IT or data security that your own country or organisation has. This can result in overvalued security expectations and assurances across jurisdictions.

Data storage in the cloud is 'multi-tenancy', meaning all data from many clients is stored together. This type of architecture can mean that someone else might gain access to your

data if there is an error or corruption in the database and secondly, the cloud provider employees could potentially gain access to your data. Even if sensitive data is encrypted the employees or provider can still view your data if they also have access to the decryption key.

The service provider may want to retain a decryption key because if you lose your key then they could restore your data access. However, if the data is particularly sensitive, then the provider may offer to encrypt the data with a key which the user manages. However, this approach may be unacceptable with loss of the key resulting in permanent loss of access because there are no other key holders.

It is worth noting that all of the major cloud providers spend a huge amount of time and resources ensuring that client data is kept secure in terms of confidentiality, integrity and availability. There are a range of schemes for validating the security of these providers including:

- Cloud Security Alliance's STAR scheme,
- The European Security Certification Framework (EU-SEC),
- ISO 27001 / ISO 27017,
- NIST Cloud Computing Standards Roadmap (Special Publication 500-291)

Firewalls

Firewalls act as a line of defence to prevent threats entering your system. They create a barrier between your device and the Internet by closing ports to communication. This can help prevent malicious programs or people gaining access and can stop data leaking from your device. Your device's operating system and home router will typically have a built-in software-based firewall. Just make sure that yours are enabled.

Use antivirus software

Although a firewall can help, it is inevitable that some threats can get through. A good antivirus software suite can act as the next line of defence by detecting and blocking known malware.

Even if malware does manage to find its way onto your device, an antivirus product may be able to detect and, in some cases, remove malware.

Intrusion Detection Software (IDS)

An IDS will monitor the network traffic and any malicious activity going on. While some IDS will only detect and alert, more advanced systems are capable of taking action on the malicious activity. This includes blocking the network traffic from any suspicious Internet Protocol (IP) addresses. Although systems capable of preventing malicious activity as opposed to detecting it are called 'Intrusion Prevention Systems (IPS)'. These systems primary focus is preventing the threats having an impact. The detection systems will hopefully detect any suspicious activity prior to hackers doing any serious damage.

An IDS can also be implemented on cloud-based storage and can protect data and systems stored there.

Managing staff working from home and their productivity

Expectations and Accountability

Provide clear instructions to each team member letting them know what needs to be done. This might mean assigning specific tasks through a workflow management tool or setting up one-on-one calls before a project. In addition, conduct team meetings where goals for each project are laid out in advance. The more information you can provide, the easier it will be to keep groups aligned – even when they are remote.

Ensuring staff aren't disillusioned or isolated

Setting up calendar schedules for video conferences is a great way to manage team collaboration. Ideally, try and stick to the same meeting time each week. This way, your employees will know how to build the rest of their schedule around the conference. Regular meetings are also great for creating relationships between dispersed team members. It's also worth asking people to regularly report in on the progress they are making. Visual project management help with this. In these tools, team members can drag tasks from "*to do*," to "*in progress*" lists. Visual project management is a concept that integrates data visualisation and thinking tools with traditional project communication.

Integrating collaboration tools with analytics and workforce optimisation systems helps to see what is working. For instance, the visual projects allow for staff work to be tracked, if the work is complete within the scheduled time then it is evident that the remote work is effective. The assignments can also be tracked via activity tracking or basic time tracking for example, how long it would take to complete the assignment and how long the member took to complete it to decide on the effectiveness.

Working/Office Life Balance

While remote working has a lot of benefits, it has its negatives too. For instance, a study by the Chartered Institute of Personnel and Development (CIPD) in 2017 found that 32% of staff couldn't switch off in their personal time when working remotely. Remote working may be more productive, but that extra productivity may lead to a burnout so creating the correct work/life balance is essential.

Creating a clear divide between work and life when working remotely can be achieved initially by creating a schedule and routine. For instance, if a line manager or senior staff member sets a task then they should be aware of how long the task/assignment should take to complete. In doing so, they could set an appropriate deadline which ensures the worker is only working on the assignment during this time frame. The time frame could be the weekdays only which gives the worker time to rest on the weekend. This approach would take 'productive burn outs' into account and assist the balance of work/office and life for the worker. Furthermore, let your teams know that just because they are online does not mean they have to be "available." Many collaboration and communication tools have presence tools that staff can use to show their status. Teaching everyone how to use presence features correctly can help to eliminate confusion in the workforce. This means that the worker is not always in 'work mode' and does not feel obligated to work constantly.

Differences in productivity - On Site versus Remote

The common worry is that remote employees are easily distracted by other work or non-work-related tasks when they are not present on site. Employers worry that "work" days at home will consist of starting late and stopping early with extended lunch and coffee breaks.

Employers also worry that remote workforces do not engender a productive work culture as there is a lack of idea sharing, human interaction and collaboration.

On the other hand, office work can also have its distractions and a significant amount of day can be spent by staff getting to and from the workplace. A working paper from the National Bureau of Economic Research published in 2013[1] identified that, homeworkers work a true full-shift (or more) and found it less distracting and easier to concentrate at home. In addition, employee attrition decreased by 50 percent among the telecommuters, they took shorter breaks, had fewer sick days, and took less time off.

In reality, home working may be just as productive as office-based staff, but home workers tend to work more flexible hours. This can lead to benefits for both the company and individual if companies address the risks that it can introduce it creates successfully.

Conclusion

Before you begin your homeworking, you should ensure that you comply with your employer's information security requirements for remote access and use of personal devices and have a secure workstation. This can be done by following the previous steps and information:

- Have a working area within the home working environment, such as study, which is not overlooked by others in the household or by neighbours
- Consider whether the home worker is going to need to print documents or store sensitive printed material whilst at home. If this is likely then consider whether to equip the home worker with lockable cabinets, shredders, etc
- Make sure that the data is securely backed up, for example using cloud backups.
- Ensure that operating systems and applications have the latest security updates applied.
- Have a secure means of connecting to the office (e.g. using VPN, 2 Factor Authentication, Endpoint Protection software)
- Install Intrusion Detection Software (IDS) both on the central systems and remote workstations
- Install antivirus software
- Configure firewall services to prevent any unauthorised access both on the central systems and the remote workstations.

Furthermore, when working from home you should also focus on the mental and physical effects, take regular breaks and continue social interactions whether that is with family or

[1] https://www.nber.org/papers/w18871.pdf

colleagues online to ensure you are not getting burnt out. If all these steps are followed, then home working can be effective as a secure alternative to office work.