SELF-ASSURANCE. HOME WORKING - INFORMATION SECURITY RISKS

Home routers

POTENTIAL RISK

Most employees working from home will make use of a home router in order to access data and if the home router becomes compromised, the home network may be compromised. Employees' routers may have inadequate Wi-Fi security making it possible for neighbours or other nearby individuals to connect and extract information without trace.

RELEVANT CONSIDERATIONS

- Have employees using home routers reviewed their router's security features and enabled the highest level of encryption?
- Have employees disabled remote access management from the internet, thereby potentially increasing the security of their router and their home working environment?
- Have employees configured and adequately secured their home router? (This might include for example the use of complex passwords, ensuring that the default password is modified and checking that any software patches are deployed).

Hardware, software and the use of personal devices

POTENTIAL RISK

Some employers will issue staff with hardware supplied by the firm, whilst in other cases staff may use their own devices. If staff use their own devices, then there may be additional security risks. Corporate hardware is likely to be configured to a higher security standard than personal devices.

Despite many firms using their own, or a provider's secure Virtual Private Network ("VPN"), if a personal device has been compromised with a virus or malware, a malicious actor could still access important and confidential data via the recording of keystrokes, or the viewing of an employee's computer screen.

RELEVANT CONSIDERATIONS

- Are staff aware, or have they been made aware through training or discussions, of the additional risks of using personal devices?
- Do all devices used by employees have adequate anti malware and antivirus protection and use the appropriate security settings?

POTENTIAL RISK

Home equipment may have unpatched vulnerabilities or lack crucial security updates or antivirus protections, which could represent increased risks if these devices are connected to the corporate network.

RELEVANT CONSIDERATIONS

- Have home working devices been patched and checked regularly to ensure that any software updates have been deployed?
- Do devices that employees use to access business systems or applications contain all updates installed to the latest versions of operating systems and software?

POTENTIAL RISK

With large volumes of internet users, connection speeds may deteriorate, which could result in users becoming frustrated and choosing to store business data locally on the hard drive of their device, which might mean that there would not be a backup. Additionally, such information may not follow a corporate data classification system and so may be at greater risk of theft, ransom or disruption.

RELEVANT CONSIDERATIONS

- Is downloading data to devices that are not under the firm's control discouraged, or even prohibited?
- Has web filtering been enabled, so that websites that are known to be compromised or linked to malware are not easily accessible to employees?

POTENTIAL RISK

The use of shadow IT (i.e. the use of systems, software or applications without explicit IT department approval - for example the ad hoc purchase of video conferencing facilities), may present a risk. When firms moved into lockdown there was an initial rush to ensure that employees were able to work from home. Some employees may have used or downloaded unauthorised software and systems to make their jobs easier.

RELEVANT CONSIDERATIONS

- Has the firm considered whether enterprise licences (which could provide more control and allow for the control of configurations), rather than personal licences or free licences, are most appropriate?
- Do employees use only authorised applications, software and services?
- Can employees install software on corporate device devices if such software is not approved?
- Have appropriate security provisions been enabled on any cloud service?

Staffing

POTENTIAL RISK

When employees are working outside of the office environment non-employees may also be in the vicinity of the work environment, for example employees may share a house with other occupants, and those occupants may also have visitors. Leaving papers on a desk at home, or leaving a computer unlocked may present additional security risks.

RELEVANT CONSIDERATIONS

- Are employees able to conduct telephone and video calls discreetly, and in a separate room, especially where confidential or sensitive data is being discussed?
- Have your employees been reminded about the importance of information data security?

POTENTIAL RISK

Whilst staff are working at home, employers may find it more difficult to identify employees that become disillusioned and this might heighten the risk of unauthorised transfer of key documents or data from the firm's systems.

Staff may move to a different department, or may leave employment, but retain system access.

RELEVANT CONSIDERATIONS

- Has the firm considered using e-mail scanning which identifies if an employee attempted to e-mail key documents outside of the firm?
- Are staff able to download information to personal devices from a remote desktop system?
- Are processes in place to track employee changes and is access to systems and data (including third party platforms) adequately controlled?

POTENTIAL RISK

Staff may be less security conscious whilst working from home, meaning that there is an increased risk that employees may be less vigilant with regard to suspicious emails and other security threats.

RELEVANT CONSIDERATIONS

- Are employees encouraged to keep their work environment separate from their personal social media accounts?
- Has additional phishing testing or training been considered?

Devices (Printers, scanners and USBs)

POTENTIAL RISK

Using scanners and printers in the home environment may also create additional risks. Allowing the use of USB sticks and other devices may result in the transfer of viruses and malware

RELEVANT CONSIDERATIONS

- Are security patches for printer and scanner software up to date?
- Can hard copy confidential information be disposed of securely?
- If use of USB sticks is permitted, are there controls in place?

Returning to work

POTENTIAL RISK

The return of hardware and materials at the point when employees return to the office, may also represent certain risks.

RELEVANT CONSIDERATIONS

- Has consideration been given to ensuring that returned hardware is appropriately inspected and patched?
- Has confidential information, whether it be notes or printed material, been disposed of securely?