DATA PROTECTION AND INFORMATION MANAGEMENT

Keeping Data Secure While Working Remotely

18 June 2020

In this briefing, we consider recent guidance on keeping data secure while working remotely.

With employees all around the globe being forced to work remotely in an effort to curb the spread of COVID-19, organisations are being forced to ensure that standards are maintained from a security perspective.

Insofar as home workers are handling personal data, the GDPR continues to apply, and organisations must demonstrate compliance with the principle of accountability in implementing technical and organisational measures to ensure a level of security appropriate to the various risks associated with remote working.

Policies and Procedures

Regardless of whether employers have long facilitated remote working or have just been required to "make it work" for the first time, all organisations need to ensure that their security policies are fit for long-term remote working arrangements.

In implementing these policies, staff should be regularly reminded of the security measures that they must adopt. In this regard, organisations should consider deploying online training to ensure staff know how to detect and report data breaches and how to keep their devices safe, etc.

Devices

Per the recent guidance of the Data Protection Commission ("**DPC**"), all work devices should have the necessary operating and software/antivirus updates.

Where it is not possible for employees to work on company-issued devices, the Irish National Cyber Security Centre ("**NCSC**") has advised creating a separate login for a worker's exclusive use of their personal device. Failing that, employee access to work systems and data should be facilitated only through "containerised" software applications, whereby user authentication (preferably multi-factor) is required to access the application instead of the device itself.

To safeguard against connectivity vulnerabilities, the NCSC has also advised that workers engage in "home router hardening" to protect their home WiFi from malicious cyber activity. In this regard, they have suggested changing the default wireless network SSID name, hiding the name from those in proximity to the home router so that it does not appear as an "available network," turning off any guest access feature, disabling WiFi protected set-up ('WPS'), and choosing a strong security protocol such as 'WPA2' or 'WPA3.'

Email

Where email has become the primary form of communication for businesses, there is a pressing need to be vigilant in respect of the threat of phishing, social engineering and Remote Access Trojans.

The NCSC has observed an increase in cyber scams, with criminals specifically

targeting staff who are working from home. In this regard, the NCSC has published a number of useful tips for identifying phishing emails, noting that it is important to be wary of poor grammar, spelling and punctuation, and to avoid clicking on web links or attachments which are unexpected or from an unrecognised source.

While it is important to adopt precautions to prevent malicious acts by external actors, the DPC has helpfully reminded the public that most personal data breaches are caused by human error. In this regard, it has recommended that individuals always check that they have selected the correct recipient and chosen the appropriate attachment(s) before sending any email in its recent guidance on data breaches and email correspondence. Further, employees should be asked to avoid taking shortcuts, such as using their personal accounts, to the greatest extent possible.

Video-conferencing

Organisations should conduct a thorough data security and privacy assessment in respect of any videoconferencing application before encouraging its use by staff. In its Data Protection Tips for Video-conferencing (available here), the DPC has advised that employees should be given clear guidance as to how to use these platforms securely and effectively. The NCSC has noted that appropriate controls may include requiring passwords, controlling access to meetings, restricting who may share their screen, utilising waiting room functions, and alerting participants when new participants join.

Working with Paper

Employees should be discouraged from printing sensitive information at home, as they are unlikely to have the means to securely dispose of printouts as they would at the office. However, where employees need to work with hard copies, organisations should provide practical guidance as to how these records should be managed, noting that they should not be disposed of with household waste.

Mitigating the Risks of Co-working

Where many people are working from home with family and housemates, employees must take additional precautions to maintain the confidentiality of their work, and where personal data is concerned, to avoid a data breach. In this regard, employees should hold conversations where they are less likely to be overheard and position their computer screen so that it is less visible to others. Devices should be fitted with a short inactivity timeout so that they will automatically lock after a short period of non-use. All work devices and documents should be locked away at the end of the working day to minimise the risk of loss or theft. The DPC's further practical tips for avoiding data breaches are available here.

Conclusion

Although many organisations may have been caught off-guard by the sudden need to enable large-scale remote working, it is probable that remote working will become part of the "new normal" for many organisations long after the COVID-19 crisis has passed. For this reason, it is important that organisations embed good working habits now to mitigate avoidable security risks long-term.

The authors would like to thank Lorraine Sheridan for her contribution to this article.

KEY CONTACTS

Colin Rooney
Partner
+353 1 920 1194
colin.rooney@arthurcox.com

Caoimhe Stafford
Associate
+353 1 920 1328
caoimhe.stafford@arthurcox.com