Irish businesses must monitor remote workers

Irish businesses are at risk due to workers not taking the correct security measures when using mobile devices remotely.

One-quarter of Irish office workers use unsecure devices for remote working when accessing and storing company data, according to Datapac, Ireland's leading technology solutions and services provider and Sophos, a global leader in network and endpoint security.

According to the survey 27pc of workers use an unencrypted mobile device when working remotely.

Unprotected data leaves sensitive company information vulnerable to hackers, potentially leading to identity theft, fraud, and theft of financial resources from employees and customers.

The survey also showed that 45pc of office-based employees in Ireland - amounting to more than 600,000 people - use mobile devices, including laptops, tablets and smartphones, to access or store company data, such as work emails or business documents.

The survey discovered that many employees fail to implement and maintain adequate security measures on both their work and personal devices. For instance, almost one-in-four office workers (24pc) have ignored a security update request on a work device. The vast majority (75pc) don't use two factor authentication - such as a code from a mobile phone - when accessing their company network for remote working on a personal device. Employees using public Wi-Fi pose another risk for businesses, with more 27pc admitting to connecting to unsecure public Wi-Fi networks without a password for remote work.

With regards to personal devices used for work purposes, 42pc of office workers who use their own devices don't use any anti-virus software. In fact, 11pc of Irish office workers who use their personal devices for work purposes don't take any measures to ensure their devices are adequately protected and secured.

Karen O'Connor, general manager at Datapac, said: "More flexible working options are increasingly in demand by today's workforce and employers are incorporating greater mobility in an effort to attract the best talent. However, employers must not lose sight of their obligations to protect sensitive data.

"Putting access rights management controls in place, implementing two-factor authentication processes, and restricting network access for unencrypted and unauthorised devices are all

essential elements in guarding against hackers and rising cybercrime. With these protective procedures in place, employees can securely enjoy a more flexible workstyle."

Ricky Knights, channel engagement manager for UK and Ireland at Sophos, added: "While employers are increasingly providing employees with corporate laptops and phones to enable remote working, basic security measures, such as encryption and anti-virus protection, are often lacking.

"Employers need to understand that this greatly increases the risk of suffering a data breach, which can expose sensitive customer and company information. Mobile device management solutions can help businesses to put security controls in place on these devices and ensure that only approved devices can gain access to the company network."

The survey of 500 Irish office workers who use a laptop, PC or smartphone for work was carried out by Censuswide on behalf of Datapac and Sophos.

Written by Stephen Larkin

Published on 8 August, 2019