Cybersecurity & Data Risks Associated with Remote Working

Robust cybersecurity policies, defences and training are essential to viability of remote working, advises Claire Morrissey, Head of Data, Commercial and Technology at Maples Group.

Technology has been both the biggest enabler and risk for all businesses in the response to COVID-19 over the last 16-18 months. The increased reliance on remote working and technology has provided more opportunities for scams and cyber-attacks.

At the outset of the pandemic, the Data Protection Commission (DPC) published brief guidance on protecting personal data when working remotely. This guidance supplements existing DPC security guidance and focuses on keeping devices, emails, cloud and network access and paper records secure. The National Cyber Security Centre also provided guidance on securing home offices against cyber-related threats, including maximising home Wi-Fi security, good practice when using personal or work devices, and remote conferencing.

Year-on-year, data security breach notifications to the DPC are increasing. In 2020, there were close to 7,000 valid security breach notifications. When a breach occurs, the 72 hours mandatory reporting timeline ticks by very quickly. In fact, the DPC's first GDPR fine of a private organisation was a fine on Twitter for failing to report a breach within the requisite 72 hours of having become aware of it.

The recent ransom attack targeting the HSE brought home the real life impact of cyber-attacks. Cyber-attacks often start with phishing, smishing or vishing: employees are tricked by fraudulent emails, text messages or phone calls claiming to be from a reputable organisation, leading them to open a malicious attachment or link and disclose sensitive information, such as passwords or credit card details. This point of vulnerability reinforces the importance of staff awareness of IT security policies and cyber risks, staff training and phishing simulations.

Claire Morrissey, Partner and Head of Data, Commercial and Technology at Maples Group

TECH EXPECTATIONS

Cybersecurity risks are also a focus point for the Central Bank of Ireland (CBI). Its 2021 Consumer Protection Report outlines its technology expectations for the firms which it regulates. These include firms having: board-approved comprehensive, documented, IT and cybersecurity strategies, aligned with overall business strategies, and supported by sufficient resources; well-defined and comprehensive IT and cybersecurity risk management frameworks to identify and manage different threats, recognising that these IT risks are continuously increasing and that cybersecurity models are the subject of increasing maturity and continuous improvement; documented cybersecurity incident response and recovery plans outlining actions to be taken during and after a security incident, including communication with relevant external stakeholders.

Firms are also expected to prioritise the development of a strong organisational culture of cybersecurity at board and senior leadership level to support the effective identification, monitoring, reporting and mitigation of cyber risks. While these recommendations are specific to firms regulated by the CBI, they provide a useful roadmap for all businesses navigating technology challenges in a remote working environment.

Post-pandemic, remote, blended and flexible working arrangements will be the new norm for many businesses. Robust cybersecurity policies, defences and training will be essential to the mitigation of cyber risk and continued viability and success of remote working across all sectors.