Data protection considerations for the hybrid environment

Companies' obligations under the General Data Protection Regulation do not change just because staff are working away from the office. Choy Lau and Alex Dittel outline how risk assessment changes for hybrid working

Changes in working practices will have an effect on the employer's information security obligations under data protection laws. Every data controller must implement "appropriate technical and organisational measures" to safeguard personal data. But how will the risk assessment change for hybrid working? The GDPR security obligations do not fall away just because staff are not at the office.

Access to company systems

While business systems used to be exclusively accessed from the well-guarded office network, hybrid working means that remote access is granted to a large number of external users. This increases the risk of infiltration by malicious third parties.

However, instead of hacking the system, many attackers focus on hacking the person. The convenience of home working comes at the cost of workers being more isolated and therefore more susceptible to phishing attacks such as emails disguised as genuine VC invites or emails from HR, designed to extract the worker's login credentials. The convenience of simply asking the person sitting next to you if they also received that weird email is gone and with it the natural safety net that colleagues create in an office environment.

"Firewalls, network monitoring and other measures are much needed but the business must strike a balance between safety and inconvenience"

A secure VPN, strong passwords and two-factor authentication are the bare minimum for remote access. Firewalls, network monitoring and other measures are much needed but the business must strike a balance between safety and inconvenience.

All staff should use the same systems and apps, as too many systems could multiply the security exposure.

Remote but where?
Will the employee be allowed to work from anywhere when not in the office? Working in public spaces exposes the company to higher risks; confidential conversations may be overheard and laptop screens may be visible to unauthorised persons. If staff do not have appropriate Internet connection, the employer should offer a secure solution to mitigate these risks.

"Any excessive requirements may defeat information security efforts. Instead of isolated training, companies must focus on establishing a security culture"

Allowing staff to work from abroad will have information security as well as tax and employment law implications. In addition, the act of accessing company systems from abroad could in some cases constitute an international data transfer which is subject to additional rules under data protection laws.

Paper files
Notwithstanding the environmental arguments, some staff simply work better with printed documents. Instead of restricting printing which could affect productivity, employers could explore safe ways to manage documents.

Staff must have secure storage at home and shredding facilities to dispose of documents. Bringing documents back to the office for disposal will probably increase the risk of data loss in transit.

Staff must understand the importance of keeping documents safe and the risks of a data breach, breach of confidentiality and the resulting liability. The company's home working policy must explain that any breach will result in disciplinary action and could, in serious cases, lead to dismissal.

Equipment
Equipment must be properly secured. Encryption, hardware locks, firewalls, antivirus, monitoring and remote wiping software will help reduce the risk.

However, if security software slows down every task, it becomes a hindrance and staff will soon find ways to make their lives easier. Controlling the employee's ability to travel with the company laptop could also backfire if staff decide to use their personal equipment for business data storage in breach of policy.

Documentation
Written policies and procedures will be essential but any chunky documents may be ignored by staff. Clear easy-to-follow policies must be implemented and accompanied by regular training.

Training
We have seen IT departments stepping up and creating a security culture at work. Training videos and quizzes alone will no longer suffice. Instead, best practices and incident awareness are fostered by firmwide security campaigns by email, notice boards, screensavers, incident debriefs and reliable IT support on-site.

Moving forward
Appropriate security comes in different shapes and forms and there is no one size fits all. The risk assessment must be a fluid exercise that anticipates and counters new risks as they arise. Any changes in work practices will likely give rise to new risks or increase existing risks.

A home working policy should set critical rules which must be appropriate as well as reasonable. Any excessive requirements may defeat information security efforts. Instead of isolated training, companies must focus on establishing a security culture.

"In some cases, convenience over security may be appropriate if supported by a risk assessment and justified in a data privacy impact assessment"

Hybrid working adds complexity to the risk assessment. Nevertheless, highest security may not always be the most appropriate and proportionate solution. In some cases, convenience over security may be appropriate if supported by a risk assessment and justified in a data privacy impact assessment.

Businesses should also be reminded to check their insurance policies to ensure that they cover staff working from home.

Choy Lau is employment lawyer and Alex Dittel is data protection lawyer at Wedlake Bell LLP