CPA
Practice Advisor

bring you own device (BYOD) policy, especially with nearly 50 per cent of companies having reported lost mobile handsets in the last year. According to IT services specialist ITC Infotech, lack of a stringent BYOD policy can lead to the risk of a major security breach.

Isaac M. O'Bannon • Sep. 03, 2014

Device and data security will assume critical significance for companies adopting a bring you own device (BYOD) policy, especially with nearly 50 per cent of companies having reported lost mobile handsets in the last year. According to IT services

specialist ITC Infotech, lack of a stringent BYOD policy can lead to the risk of a major

employee, so BYOD has become very attractive. However, far from enjoying flexibility and lower costs, companies that rush into BYOD without a strong policy face considerable risks," comments Hardeep Singh Garewal, President – European Operations, ITC Infotech.

A Freedom of Information Act request from security software vendor McAfee discovered that 15,000 mobile phones were reported lost on the London Underground in 2013 alone. Only around 2,000 of these were eventually returned. Larger devices also proved to be at risk, with 506 tablets and a further 528 laptops also reported lost.
"For unprepared companies, a lost or stolen device represents a catastrophic security risk, with the potential cost to their business far outweighing the savings. There are many solutions available, but we see many companies failing to implement a clear policy on keeping track of work devices. This hinders them from acting quickly to prevent breaches," adds Garewal.

Apart from security, companies also face risk of a different kind if they fail to set a clear boundary between the personal and business functions on a BYOD device. Many businesses erase personal information along with work data when wiping or locking a device for security. This is almost an open invitation to potential legal action. ITC Infotech has also found that businesses often fail to track 'unofficial' BYOD devices that have remote access, creating further complications for lost devices or when employees leave the company.

Choose Your Own Device (CYOD) on the other hand, offers an increasingly popular solution to both security and personal data concerns. This ensures that full ownership of the device is retained by the company. This eliminates any uncertainty in safeguarding information on the device, whilst still allowing for user freedom in choice and application.

Garewal adds: “While CYOD means the company must ultimately foot the bill for the

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.