PROLIFERATION OF PERSONALLY-USED MOBILE DEVICES IN THE WORKPLACE IS NEARLY COMPLETE

Only 4% of organisations do not allow employees to use either their own personal mobile devices for work purposes (BYOD) or provide corporately owned personally-enabled devices (COPE) to employees.

48% say that their organisation currently has a BYOD policy.

MOBILE SECURITY PLANS AND POLICIES

42% of surveyed IT decision makers think that their CEO has an in-depth understanding about the security risks posed by mobile devices. 37% believe that the CEO takes the threat of mobile security very seriously.

MOBILE SECURITY BREACHES

32% of devices still do not have password protection, and only 46% of all respondents report that their organisations offer IT security training for all.

33% of respondents say that staff have an in-depth understanding of the security risks associated with mobile devices and 31% believe that staff take the threat of mobile security very seriously.

69% of respondents admit that their organisation has suffered a mobile security breach in the last 12 months.

FINANCIAL SERVICES

VALUABLE DATA IS LEFT AT RISK

97% say that corporate data is held on personal or personally enabled devices

- Emails 64%
- Contact information 60%
- Network login details 45%
- Corporate information in apps 45%
- Customer data 54%