EUROPE

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

Only **11%** 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.

**27%** say that their organisation currently has a BYOD policy.

## VALUABLE DATA IS LEFT AT RISK

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


Emails **67%**

Contact information **63%**

**47%** Customer data

**44%** Network login details

**47%** Corporate information in apps


## MOBILE SECURITY PLANS AND POLICIES

**40%** of surveyed IT decision makers think that their CEO has an in-depth understanding about the security risks posed by mobile devices. A quarter (25%) believe that the CEO takes the threat of mobile security very seriously.

**33%**

of devices still do not have password protection, and 55% of all respondents report that their organisations do not offer IT security training for all.

**38%** of respondents say that staff have an in-depth understanding of the security risks associated with mobile devices and less than 19% believe that staff take the threat of mobile security very seriously.

## MOBILE SECURITY BREACHES

**60%**

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