October 2014

Art of Connecting:

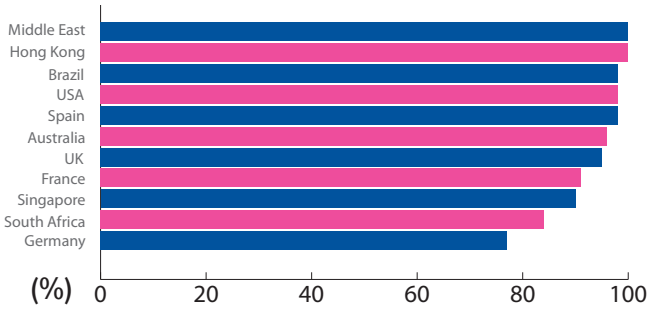
BT Security research on mobile security threats

This global research provides an insight into business practices around managing mobile devices and explores IT decision makers' attitudes towards mobile security within their organisations. It reveals that the use of personal mobile devices at work is very high, even though these devices represent a significant security risk to organisations. Despite the very real threat of a mobile security breach, many businesses are failing to make adequate provisions to protect their valuable data, which is costing them greatly.

This report is based on 640 interviews with IT decision makers in large organisations (1,000 plus employees) across 11 countries including: Australia, Brazil, France, Germany, Hong Kong, Middle East, Singapore, South Africa, Spain, UK and USA. Respondents were drawn from the finance, retail and the public sector.

The proliferation of personally used mobile devices

- Only seven per cent 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. In Hong Kong and the Middle East, proliferation is complete, as 100 per cent of organisations allow their staff to use BYOD or COPE devices.

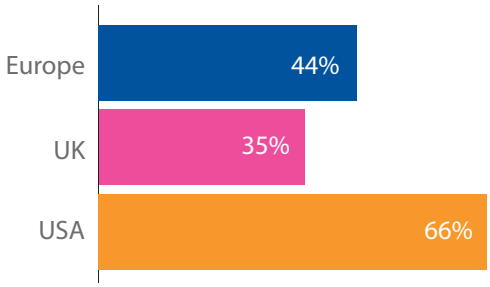


Accessing the corporate network and data

- Ninety-seven per cent of respondents with BYOD or COPE devices say that corporate data is held on these devices. Emails (70 per cent) and contact information (64 per cent) are most likely to be stored on these devices, but over four in ten also report that customer data (49 per cent), network login details (46 per cent) and corporate information in apps (41 per cent) are held on employees' personal devices.
- One third of employees are enabled with full remote access to an organisation's network, and 87 per cent have remote access of some kind.
- In Germany, 75 per cent of employees have some kind of remote access to the corporate network, whereas in the Middle East, up to 100 per cent of employees can remotely access the organisation's networks.

Mobile device management policies

- Despite this, only around four in ten (44 per cent) say that their organisation currently has a BYOD policy. In the UK, this figure is even lower, at 35 per cent compared to 66 per cent in the USA.
- Thirty per cent of organisations have neither a BYOD or COPE security plan in place.
- Three in ten devices do not have password protection, and less than half (45%) report that their organisation has IT security training for all.



Mobile security breaches

- Unsurprisingly, sixty-eight per cent of respondents admit that their organisation has suffered a mobile security breach in the last 12 months.
- And around half of all respondents' organisations who have experienced a mobile security breach have suffered more than four in the last year.
- Only around one quarter (26 per cent) of those in organisations which allow BYOD or provide COPE devices strongly agree that their organisation has sufficient resources in place to prevent mobile security breaches.

Types of incidents

- Forty-four per cent have experienced malware infections and 23 per cent admit that customer or their organisation's data has been compromised or stolen.
- Eighty-two per cent of those that have experienced lost or stolen devices, report that they have suffered this multiple

Art of Connecting:

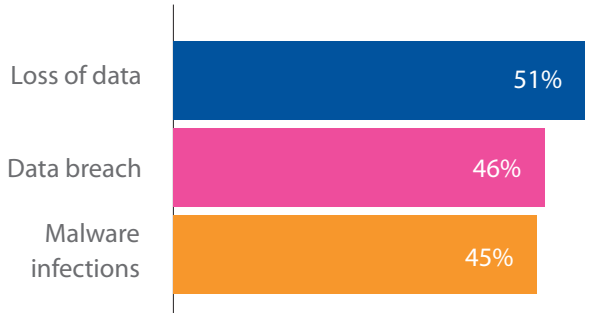
BT Security research on mobile security threats

times in the last 12 months.

- Eighty-four per cent of those that have experienced malware infections, report that they have suffered numerous infections and 72 per cent that have had company or customer data compromised confess that their organisation's company or customer data has been lost multiple times within the same period.
- Ninety-five per cent expect security threats to increase over the next three to five years, with malware infections and malicious apps downloaded onto mobile devices seen as most likely to increase.
- Currently, losing customer or the organisation's data (51 per cent), data breach attacks/errors from the introduction of mobile (46 per cent), and malware infections (45 per cent) are seen as big or major concerns affecting their organisation's mobile security.

Cost of mobile security breaches

- On average, the most significant mobile security breach cost organisations £28,000 and around one quarter (27 per cent) say that their most significant mobile security breach cost them over £30,000.
- Four in ten respondents whose organisation has suffered

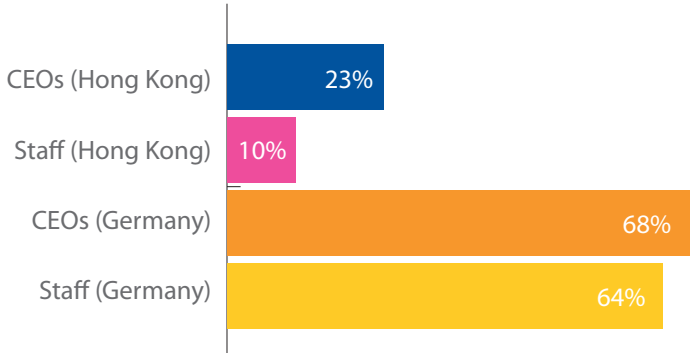


a mobile security breach in the last 12 months report that IT resources (45 per cent) and help desk time (39 per cent) were either majorly or severely impacted by this breach.

- Two thirds (66 per cent) cite reputational damage as being moderately to severely impacted, and 61 per cent say that customer experience was negatively impacted at least to a moderate extent as a result of the breach.

Understanding the threat

- Only around two fifths (42 per cent) of surveyed IT decision makers think that their CEO has an in-depth understanding of the security risks posed by mobile devices. Even fewer (31 per cent) believe that the CEO takes the threat of mobile security very seriously.
- Just over one third (36 per cent) of respondents say that staff have an in-depth understanding of the security risks associated with mobile devices and only 26 per cent believe staff take the threat of mobile security very seriously.
- There are, however, discrepancies between countries: in Hong Kong, only 23 per cent of CEOs and 10 per cent of staff have an in-depth understanding of the risks posed by security devices, whereas in Germany, 68 per cent of CEOs and 64 per cent of staff are found to have an in-depth understanding of mobile security risks.



Percentage of CEOs and staff who have an in-depth understanding of security risks

Other security threats

- Fifty-four per cent of surveyed IT decision makers believe that the 'Internet of Things' poses a threat to network security.
- Nine in ten (90 per cent) of all surveyed IT decision makers have major concerns about Bring Your Own Cloud (BYOC), yet 45 per cent of respondents say that there is evidence of employees adopting BYOC.
- The most common concerns associated with BYOC are loss of management control (53 per cent), loss of overall data access control (53 per cent) and increased risk of data loss (45 per cent).

Our mobile security solutions have been developed to help our customers secure their network, devices, applications and data; all supported by our BT Advise consultants who develop and implement mobile security strategies.

To learn more about this research and find out how BT is working with customers to ensure they are fully protected against mobile security threats, please visit www.bt.com/security.