BT Assure: *'Rethink the Risk'* Research Summary

Jeff Schmidt, Head of Security
BT Global Services

24th April 2012

BT Assure. Security that matters

Research methodology

- Commissioned by BT to examine current priorities in corporate IT security:
  - Explore key themes of ‘bring-your-own-device’, cyber-security and on-demand services delivered through cloud computing.
  - Contrast views and expectations of employees with plans and priorities of IT decision-makers in enterprises across public and key private sectors.
- More than 2,000 online questionnaires carried out by Vanson Bourne in March / April 2012
- Enterprise size organisations (>1,000 employees) across five sectors:
  - FMCG
  - Finance
  - Logistics
  - Pharmaceuticals
  - Government
- Four audience types: Office workers (1,000), IT decision makers (860), Finance decision makers (150) and HR decision makers (150).
- Eleven countries: UK, France, Germany, Spain, Italy, Benelux, USA, Brazil, China, India and Singapore.

Key themes:

a) Pressure to take advantage of new technologies to enhance productivity and competitive advantage

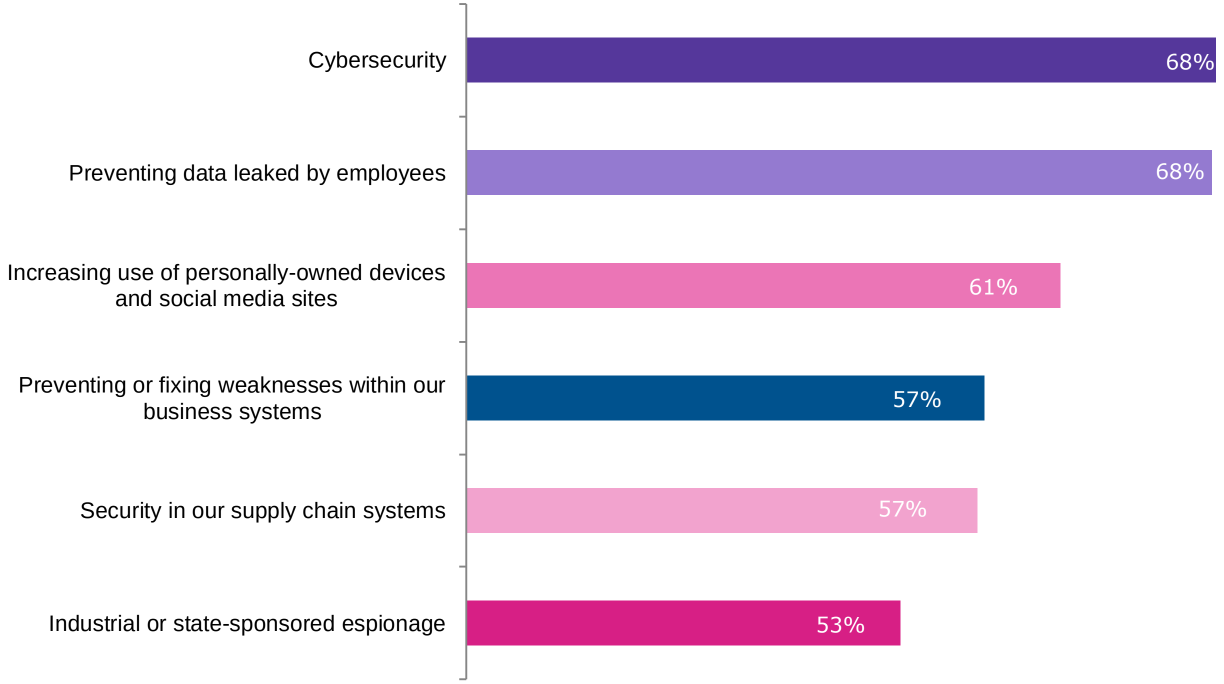
b) Excitement over the possibilities and benefits, but limited awareness of concerns over security implications

c) IT departments see the risks, but are struggling to manage them within their established corporate security framework

The risk landscape is changing, fast...

Emerging threats already rank alongside established cyber-security challenge

- Employees leaking data, BYOD and a mobile workforce are in the same threat league as cyber-security

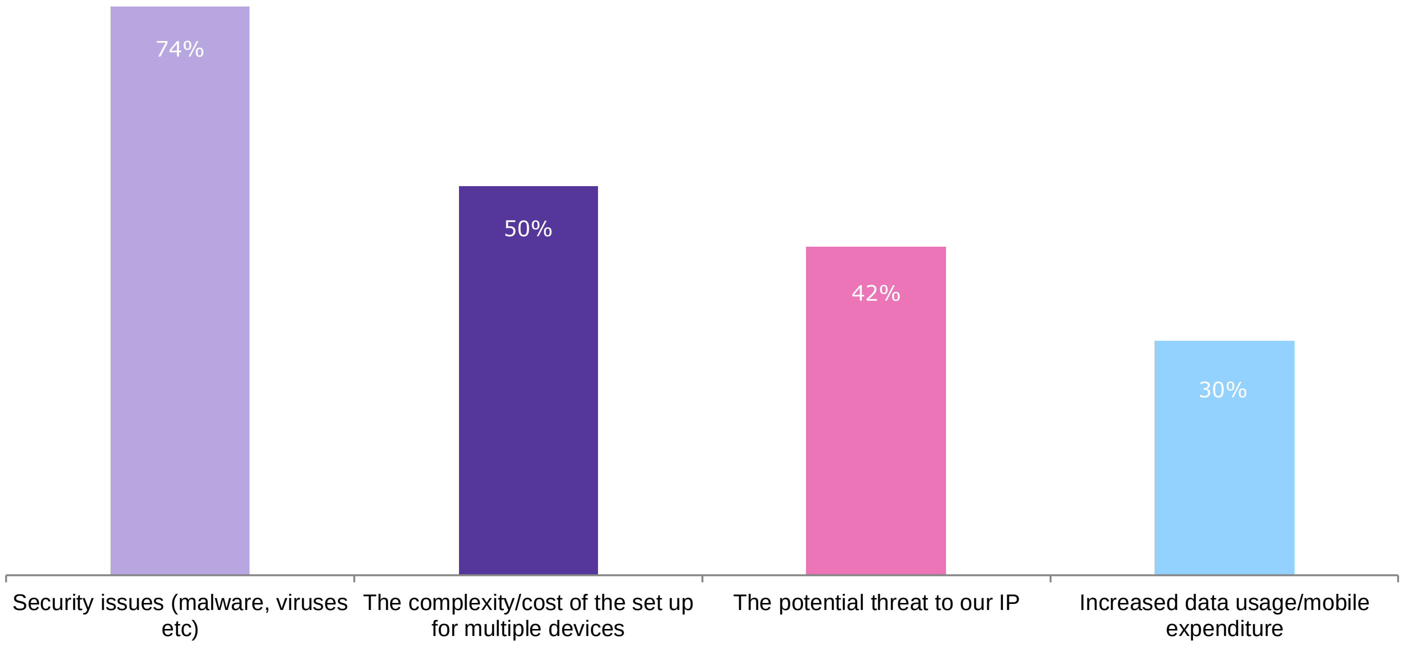


Number of respondents rating each of these threat areas as "'challenging" or "very challenging' (BASE: IT respondents)

BYOD presents unprecedented challenges

Priority concerns before introducing BYOD

- IT decision-makers need to tackle a range of issues before they feel able to introduce a BYOD policy.

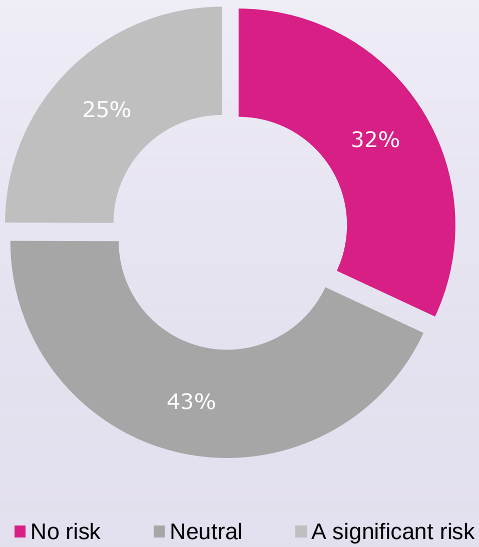


Which of these factors/concerns did you have to deal with before being able to allow employees to use their personally-owned devices for work purposes? (BASE: IT respondents)

Employees recognise the rewards but not the risks

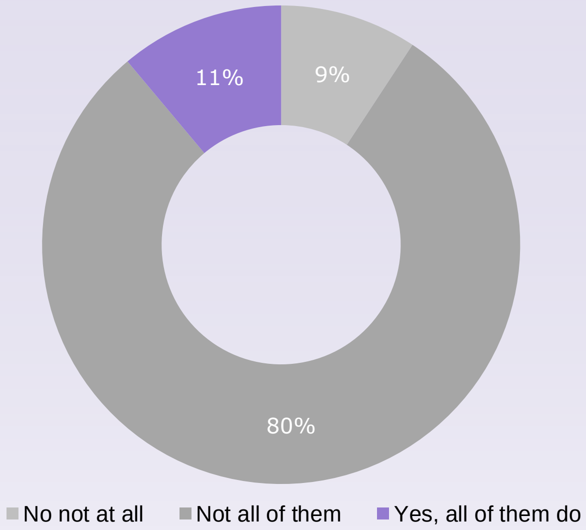
- 42% of employees using their own device for work believe they are more efficient and productive, but…

- 1 in 3 employees see “no risk” in using their own device in a work context



How big a risk to company security do you perceive using your personal device in a work context to be? (BASE: Employees)

- Only 1 in 10 IT decision-makers think all BYOD users recognise the risks



Do employees generally recognise the risk to company security that using a personal device in a work context could represent? (BASE: IT respondents)

Global perspectives on BYOD

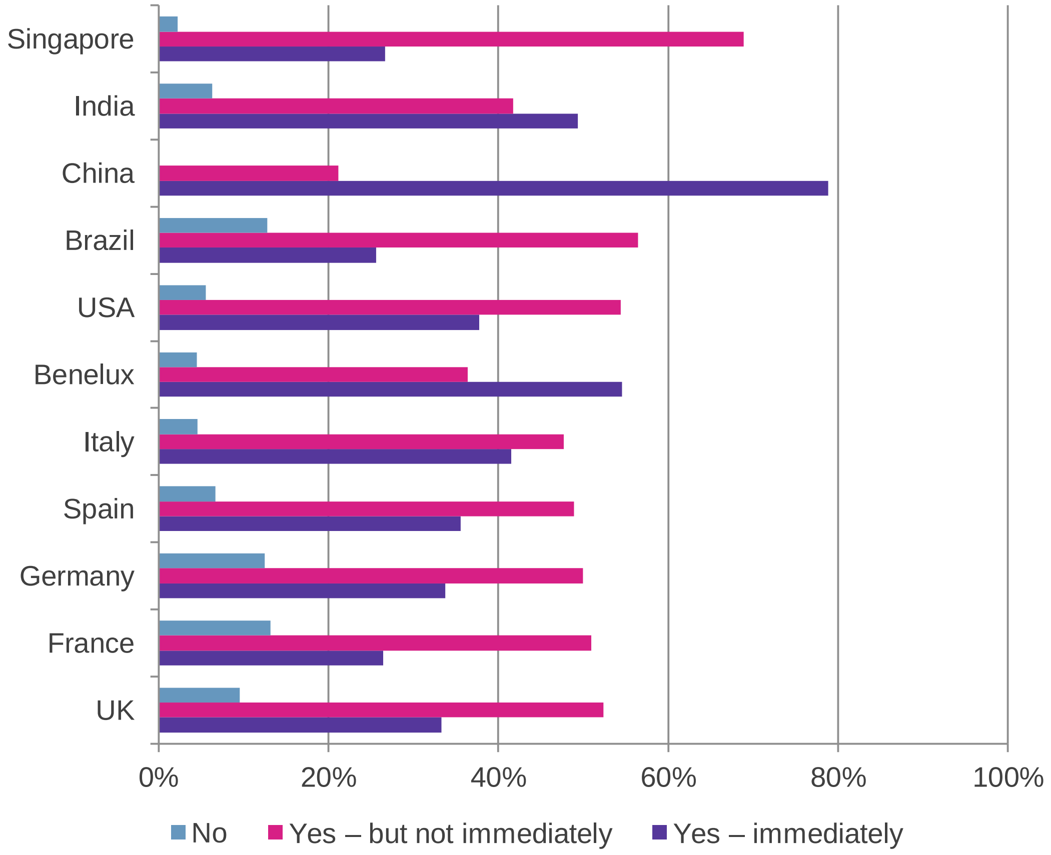
The BYOD ‘genie’ is out of the bottle

- 60% of employees say their companies permit them to connect personally-owned devices to the corporate network and use them for work – this drops to 37% in the UK, but increases to 80% in India and 92% in China.
- 46% of employees who currently can’t, would like to be able to use their personal devices for work.
- While company sanctioned BYOD adoption is generally high, the level of use stated by employees is higher than IT decision-makers acknowledge.
- Organisations in China (53%), Brazil (51%) and the USA (50%) are most likely to have formal BYOD policies in place, but there is still significant acknowledged penetration in countries least likely to already have a policy - Italy (25%), UK (31%) and Germany (34%).

Tackling the BYOD security challenge

- Of IT decision-makers within organisations with BYOD policies, providing the security infrastructure has had the greatest impact in the USA (with every aspect scoring between 62% and 89%).
- 15% say the cost of BYOD is unclear – this more than doubles in the UK and Benelux to 38%. In Spain and Brazil, more than half report a net saving (52% and 53% respectively), compared to an average of 36%
- Whilst 31% of the total number surveyed report a net cost, in China and India this reaches 53% and 50% respectively - so while they may appear to be top of the game, it is costing them.
- On average 47% think BYOD may threaten auditing and compliance obligations – this reaches 60% in the UK and 65% in India.
- 73% (almost double the average of 39%) of IT decision-makers in India admit they have had a security breach due to an unauthorised device. This is also high in Singapore (58%) and Brazil (49%).

Varying levels of oversight

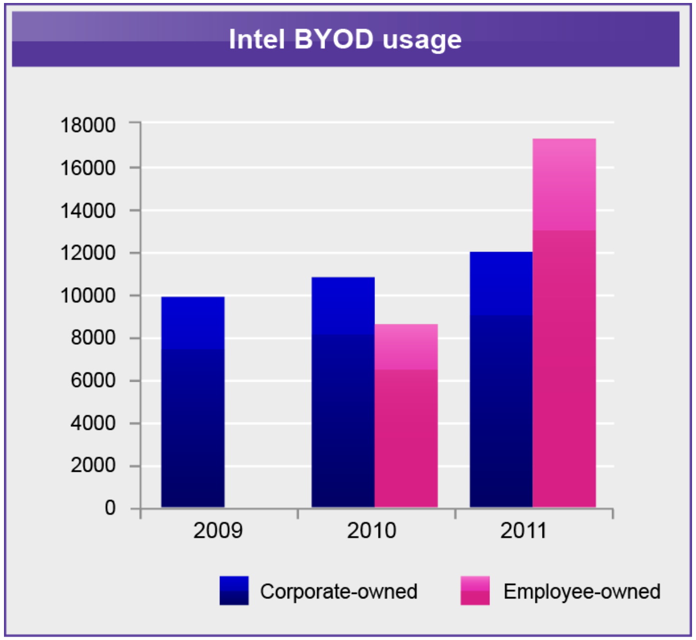


Can you tell if someone is using an unauthorised device on the system? (BASE: IT respondents with a BYO policy)

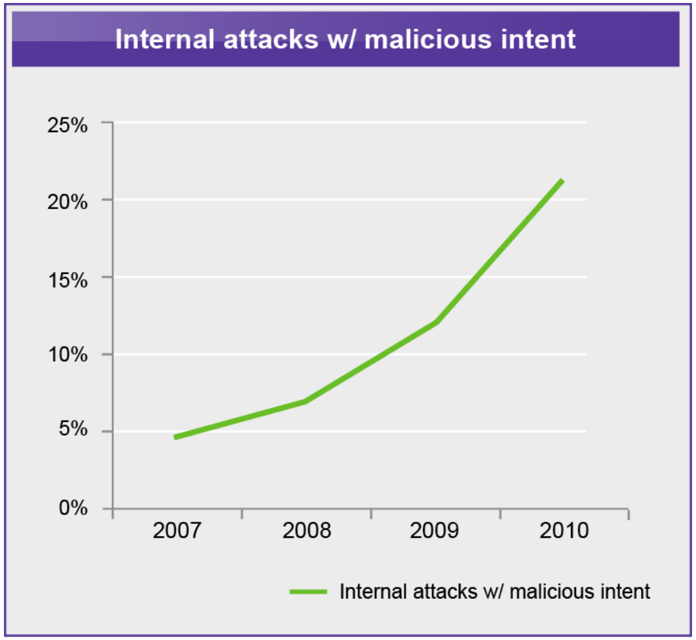
- Only 43% are actively monitoring for people using their own device on the network.
- A third (33%) can tell immediately if an authorised user misuses their device
- IT decision-makers in China have the greatest vigilance on their corporate network. 79% say they can tell immediately if an unauthorised device is connected to their network and 71% can tell if an authorised user misuses their device.

It’s not just our own network anymore…

- Connectivity and ubiquitous access have changed the landscape of security perimeters dramatically. What was once restricted must now be permitted; what was previously unthinkable is now routine; and the adoption of innovative new tools is being pulled through from the most senior executives, rather than pushed from below by IT
- The new perimeter is everywhere, defined by employee-owned devices, clouds, and extranets. The risk of abuse and attack has multiplied along with this massive expansion
- Our response has to make the leap from new ideas to happy customers. And we have to protect millions of new portable devices, each of which contain huge amounts of data
- We must **Rethink the risk**



Source:http://www.intel.com/content/dam/www/public/us/en/documents/ best-practices/intel-it-annualperformance-report-2011-12.pdf



Source: KPMG Data Loss Barometer

BT Assure

Security that matters

www.bt.com/btassure/securitythatmatters