

End-point security

The right protection in the right place



Bob Tarzey

Analyst and Director, Quocirca Ltd

June 15th 2011

What is an end point and who owns it?

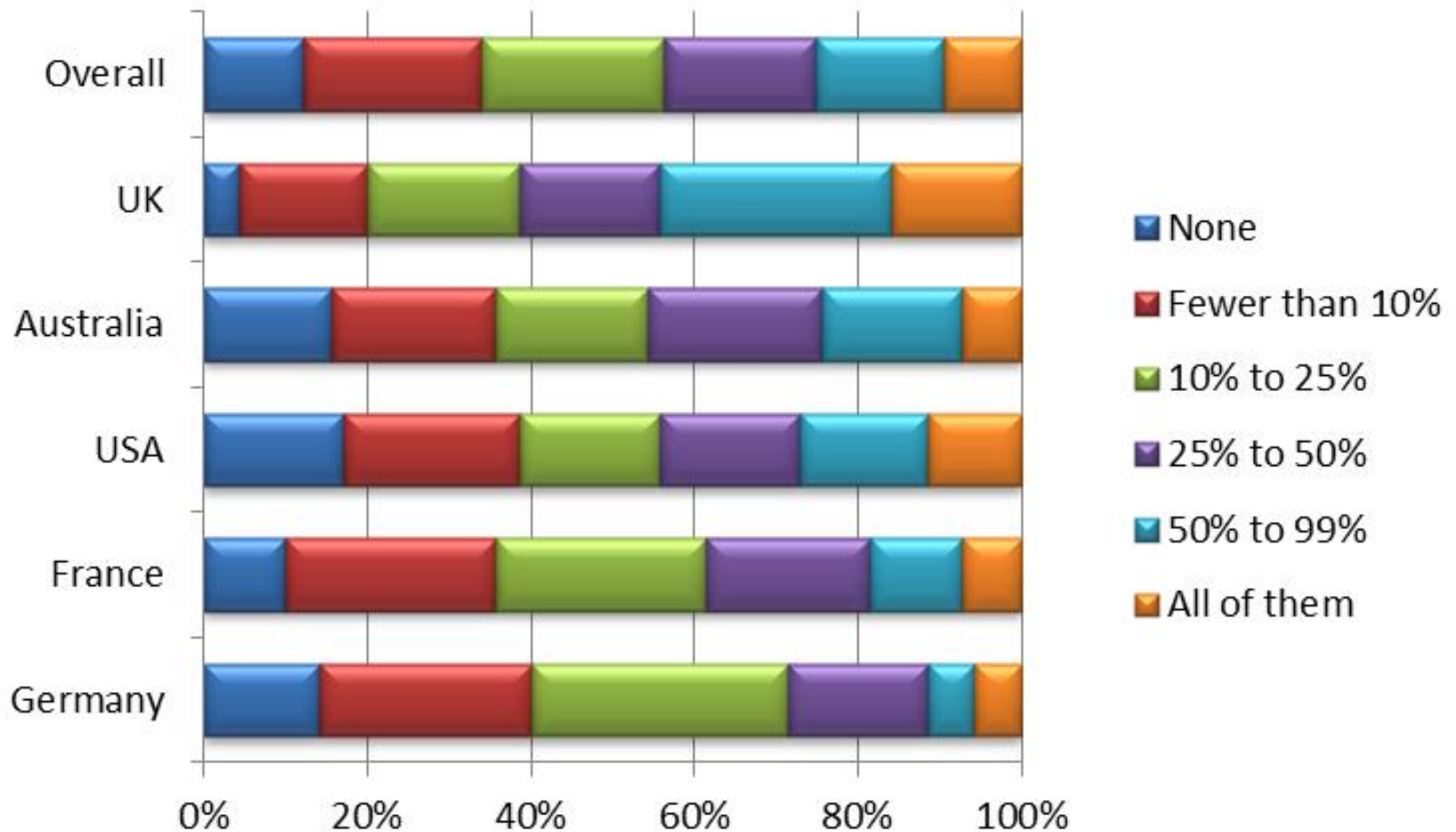


FIREWALL



Employee access devices	Customer access devices	Other devices
<ul style="list-style-type: none">• Desktop PCs• Mobile PCs• Thin client devices• Smartphones• POS devices• Public devices such as PCs in airport lounges and internet cafes• Shop floor devices; hardened PDAs, controller screens etc.	<ul style="list-style-type: none">• Video displays• Ticket machines• ATMs• RFID readers• PCs• Smartphones	<ul style="list-style-type: none">• Printers and copiers• Network routers• Branch office servers• Appliances; e.g. network security devices

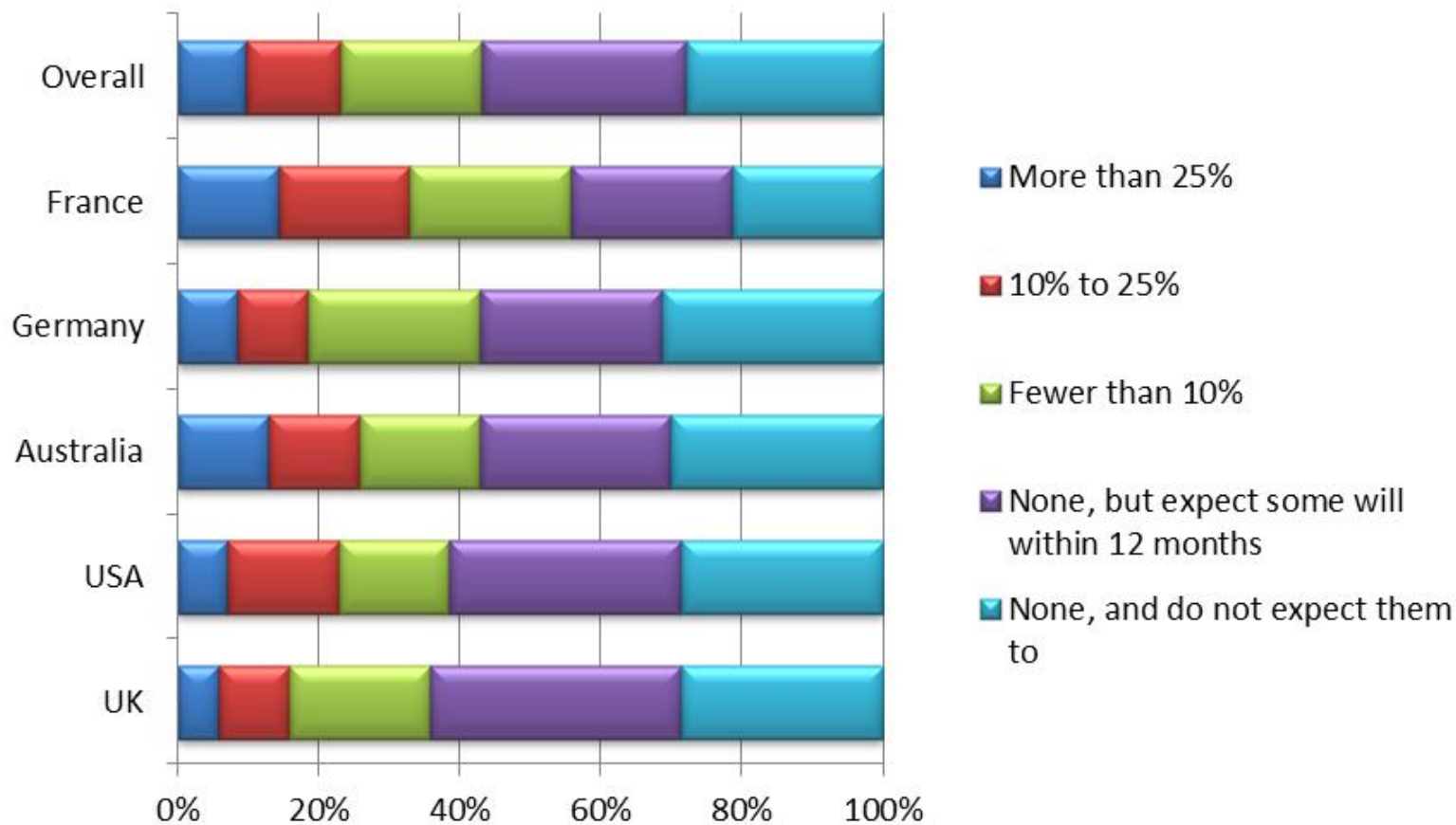
What percentage of your users is using smartphones for business purposes?



Sponsored
by



How many of your employees are now using tablet computers to access your IT systems?

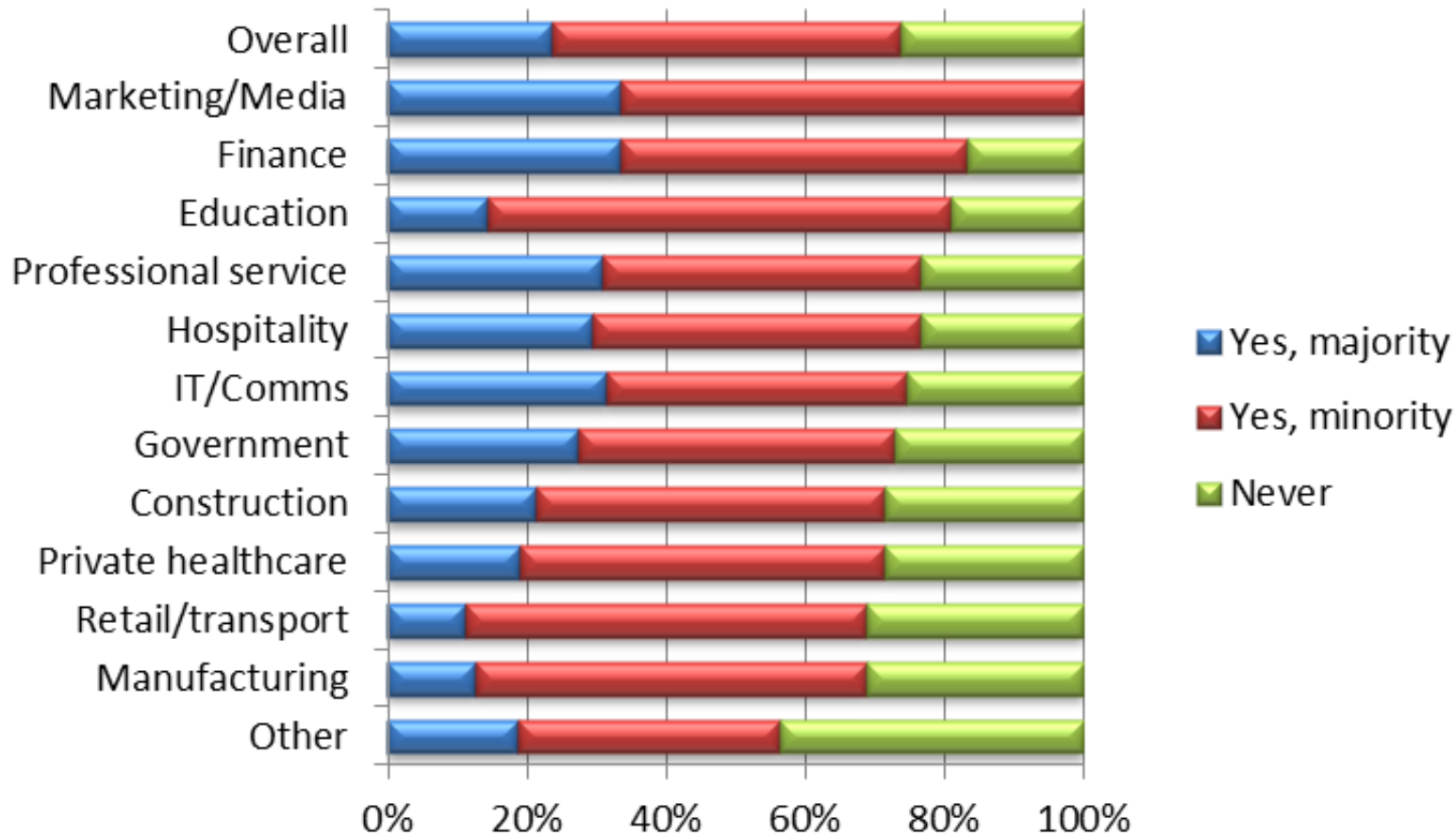


Sponsored
by



TREND
MICRO™

Do you allow employees to use their own devices to access data and certain applications?

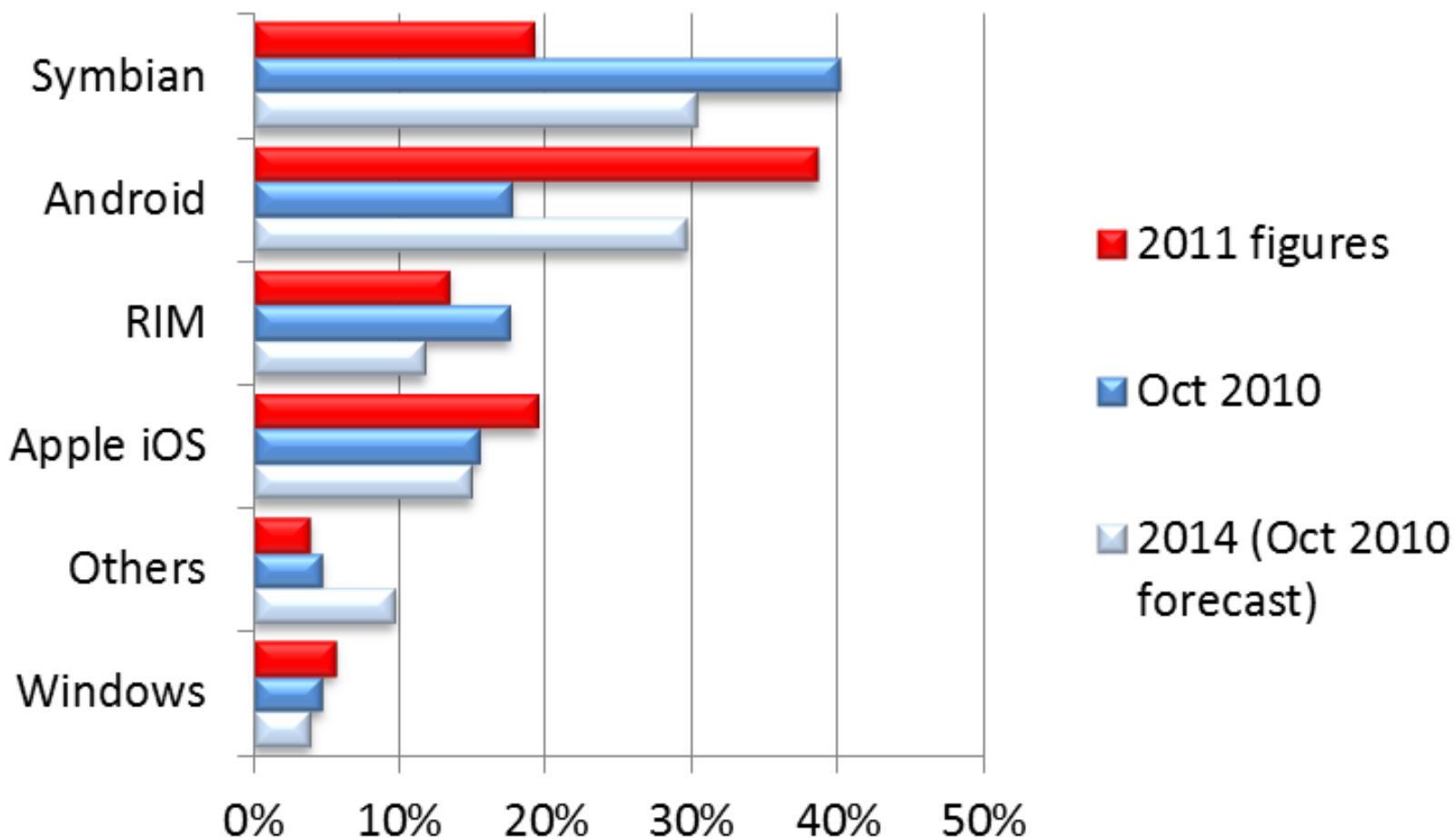


Consumerisation

**Consumerisation
is a reality, it
may also be a
secret weapon**



Diversity of mobile devices (% market share)



Source: Gartner

Published in Information Age (Oct 2010)

Three main challenges

Malware



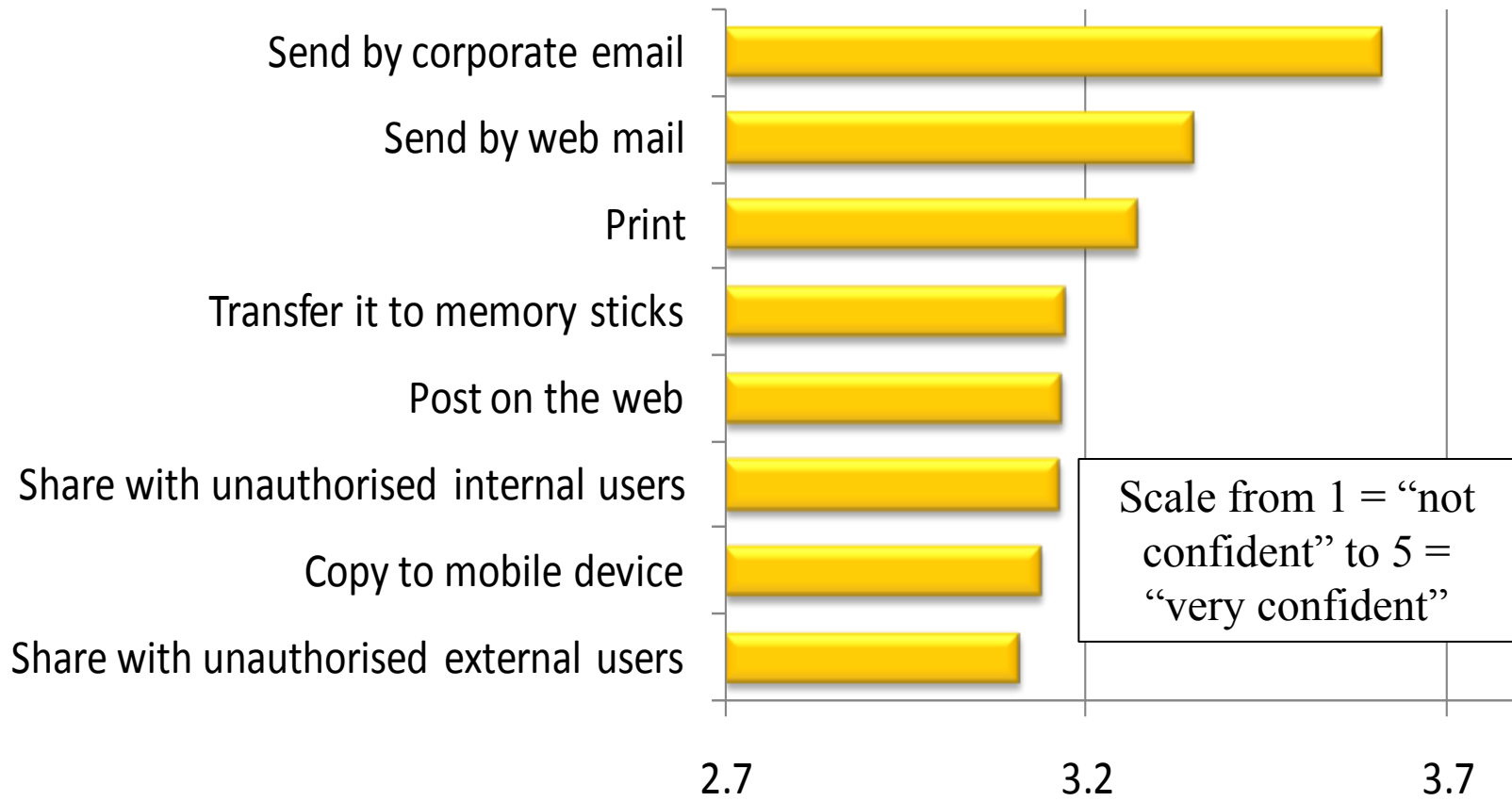
Secure access



Data loss



A threat to data



When users have legitimate access to data how confident are you that you can control their ability to do the following? (source Quocirca "You sent what?")



Three main factors to consider

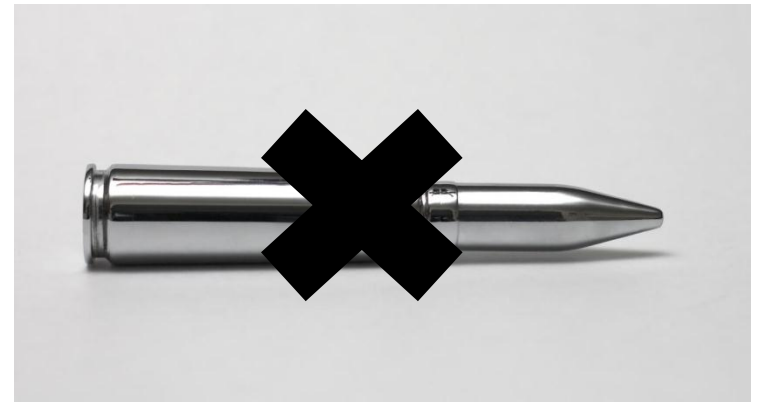
The type of device



The user

- Employee
 - Information worker
 - Transactional worker
- External

The transactions/data involved



Two extreme approaches



**Centralised
control
mechanisms**

**The
approach
taken
should be
somewhere
between the
two**



**Host
based
security**

Centralised control

- **Force all application and/or internet access via central control points**
- **Suits**
 - Some mobile PC use
 - Remote/home workers
 - Limited use for smartphones
- **Tools**
 - VPN
 - VDI
 - Restricted data stores
 - Locked down apps
 - Next generation firewalls
 - Web proxies
 - Email filtering
- **Problems – creates choke points**

Host based security

- All devices are security in the own right (aka Jericho Forum)
- The only practical way to protect some smartphone use
 - Password protection
 - Malware protection
 - Device firewall (on-device filtering)
 - Encryption
 - Remote disablement and wipe
 - SIM recognition
 - Geolocation using GPS
- Problems
 - Hard to manage
 - Consumes resources
 - Consumerisation

Management tools

- Ensuring protection is in place and remains so
 - keeping device software and security up to date
 - Taking action can be taken when a problem arises
 - Auditing of device ownership and use (e.g. logging phone calls made, SMS content and photos)
 - Asset and licence management
 - Taking remote action
-
- End point management tool
 - End point security tools
 - Mobile device management



A final thought - end of life



This presentation will be available on
www.quocirca.com

Thank you
bobtarzey@quocirca.com