

# Securing remote workers

## The right protection in the right place

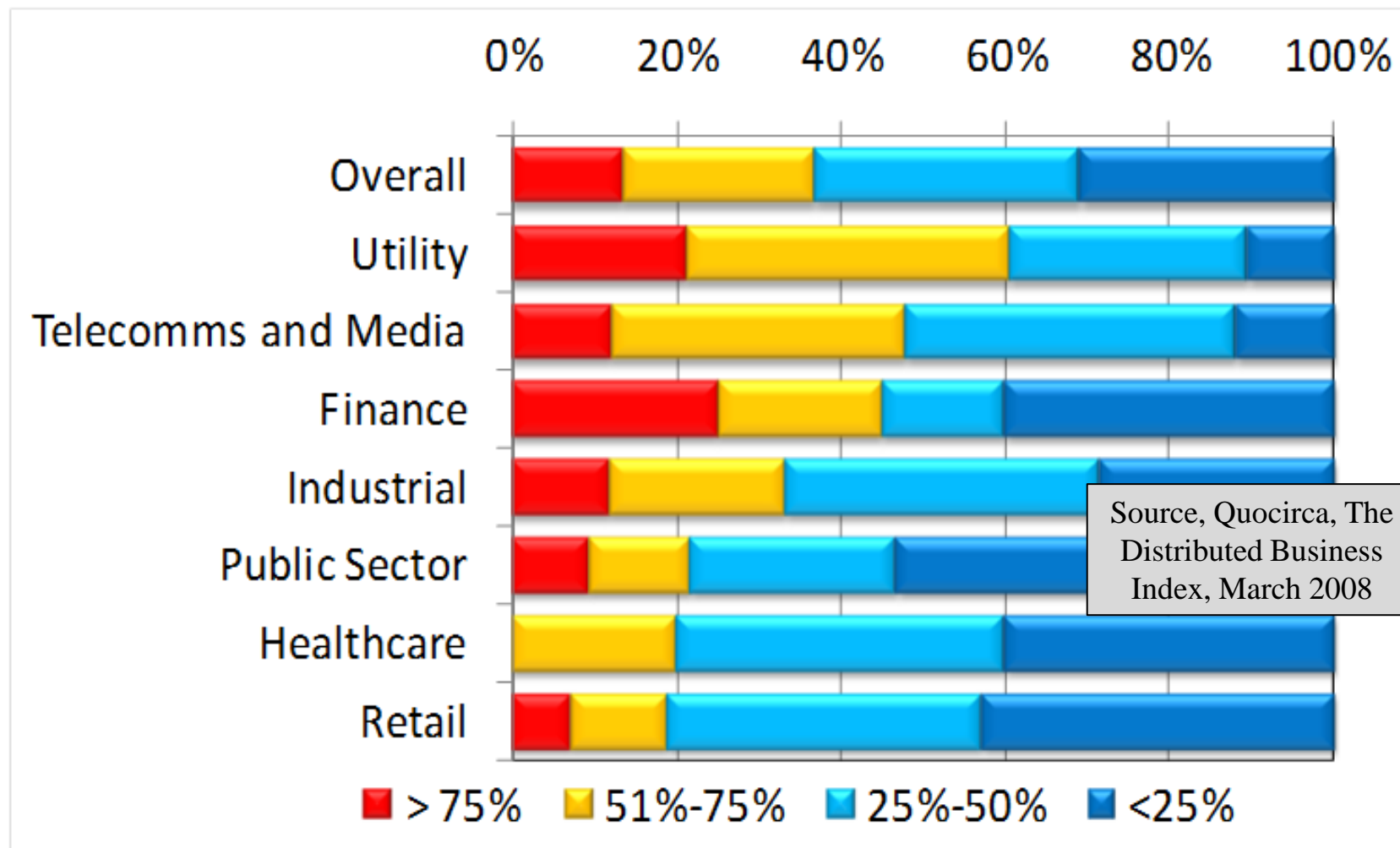


Bob Tarzey

Analyst and Director, Quocirca Ltd

Feb 17<sup>th</sup> 2011

# Percentage of employees working remotely at some point during a week



More and more employees are working remotely,  
for at least part of the time

# Three main challenges

**Malware**



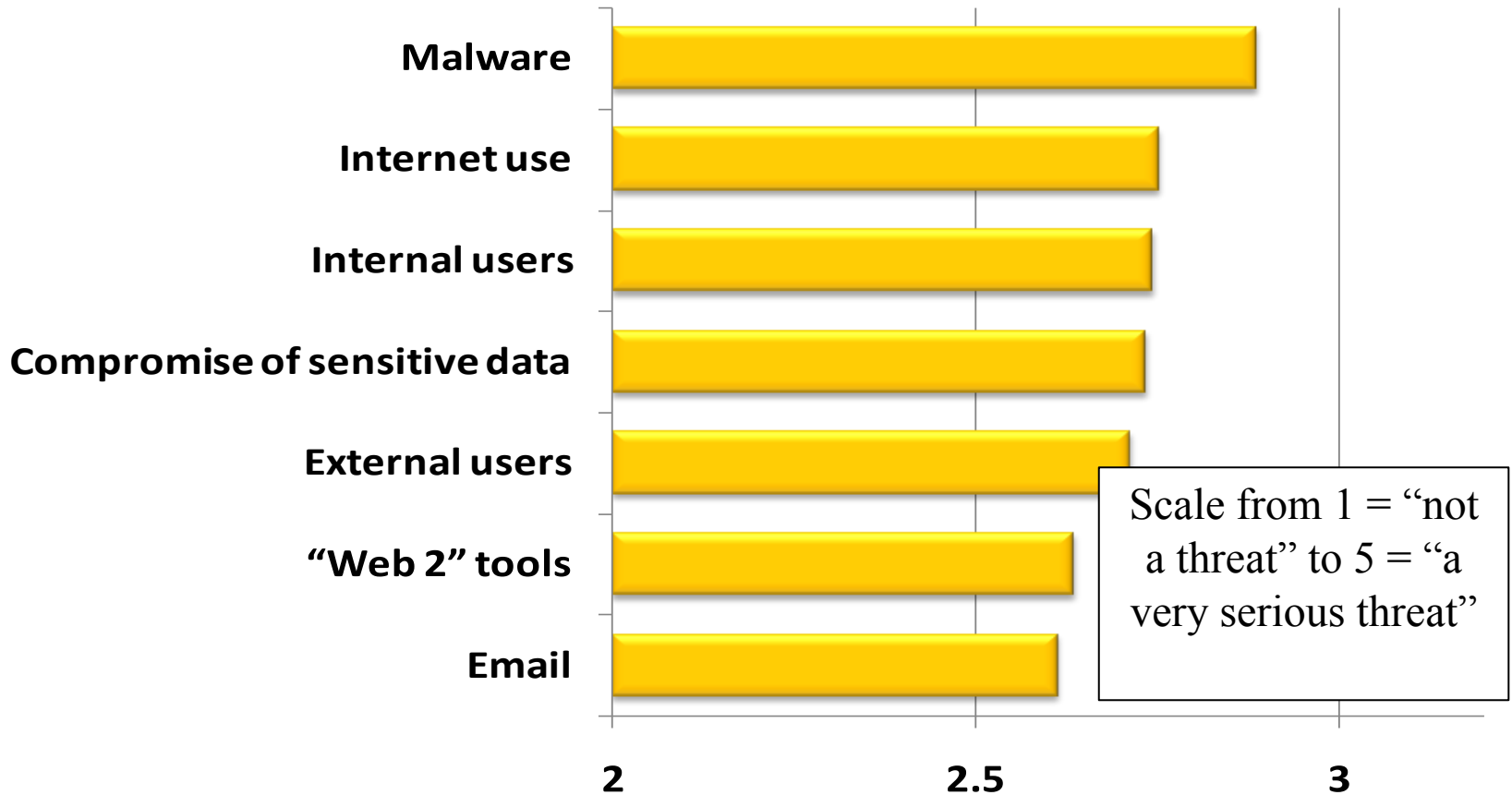
**Secure access**



**Data loss**

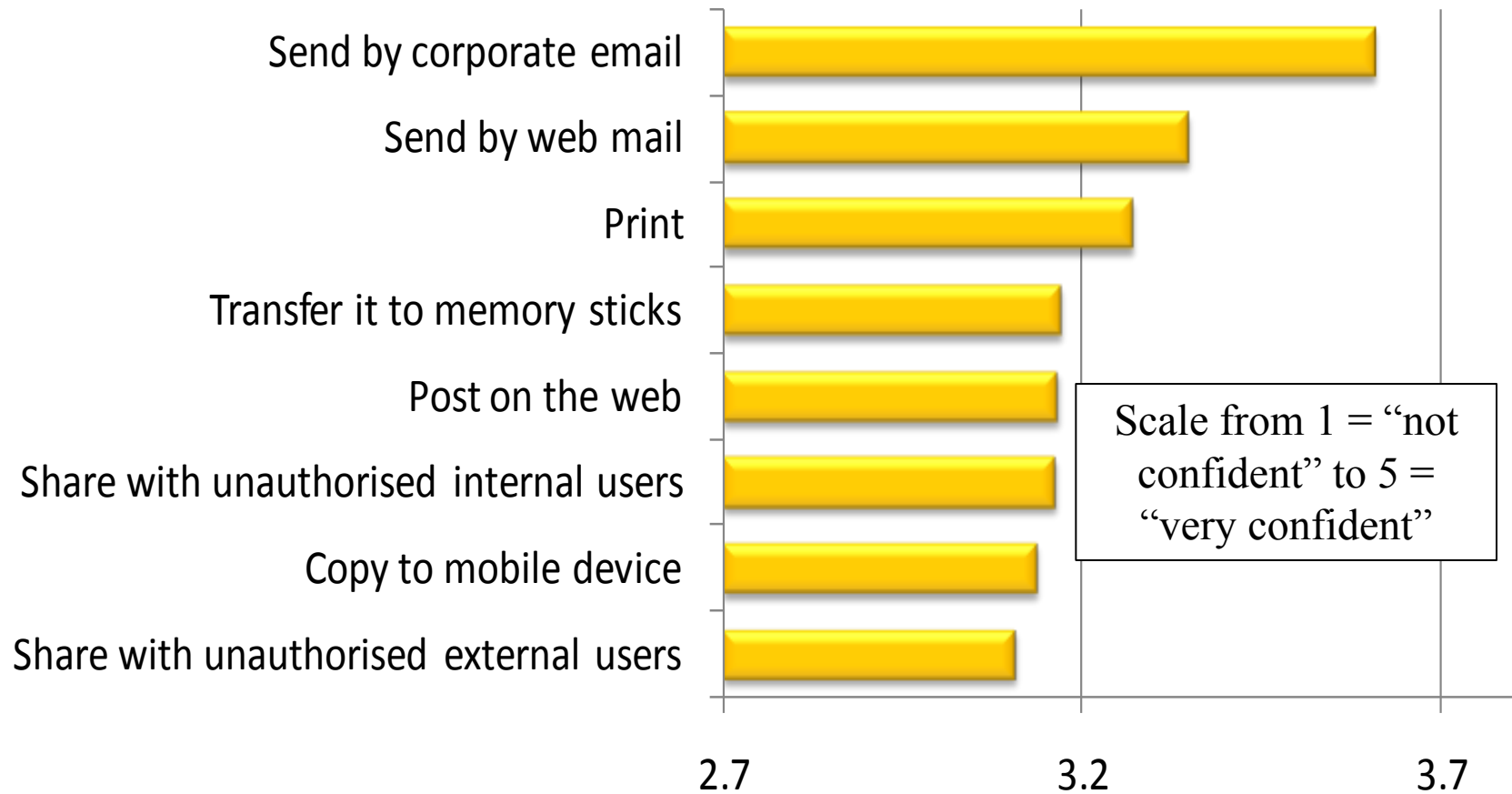


# Malware always the biggest concern



**To what extent are the following a threat to IT security in your organisation?** (source Quocirca "You sent what?")

# 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?”)

# Device diversity



**The range of devices and operating systems on end user access devices exacerbates the problem**



# Two extreme approaches



**Centralised  
control  
mechanisms**



**Host  
based  
security**

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

# 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
  - 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 most 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

**Consumerisation  
seems inevitable,  
it may be a secret  
weapon**



# 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](http://www.quocirca.com)

Thank you  
**bobtarzey@quocirca.com**