

The evolving threat landscape

Dealing with intellectual property security

Clive Longbottom,
Service Director, Quocirca Ltd

- Early viruses were annoyances, generally from bored geeks
- “Back doors” were left in code by coders for support reasons
- The biggest threat to an organisation’s intellectual property was the leaver
- Commercial espionage only happened at the highest levels



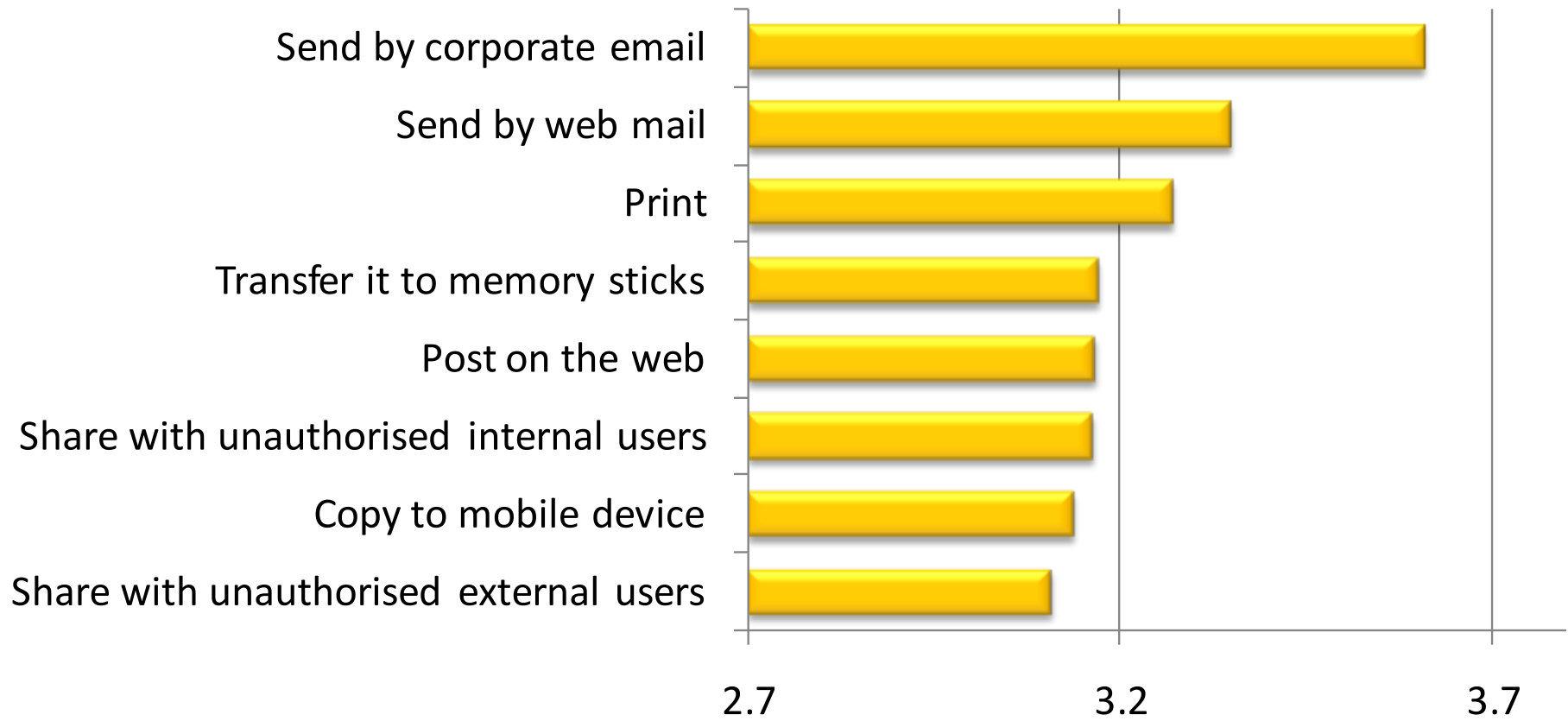
- Technology costs fell dramatically
 - Basic equipment costs no longer an issue
- IT users numbers increased exponentially
 - A much larger target audience of users and hardware
- The internet provided easy access to an organisation's periphery
 - With many more access types
- Value chains made information flows necessary
 - From supplier's supplier through to customer's customer
- Basic threat code became easily available
 - "Starter kits" are widely available



- Organised crime is big in threats
 - Commercial espionage
 - Blackmail
 - Financial theft
 - Financial details theft
 - Denial of business service
- The malicious insider
 - Sacking/unemployment
 - Disgruntled/overlooked
- Accidental information leakage is a threat
 - Phishing
 - Emails
 - Social networking
- Leading to far more advanced threats

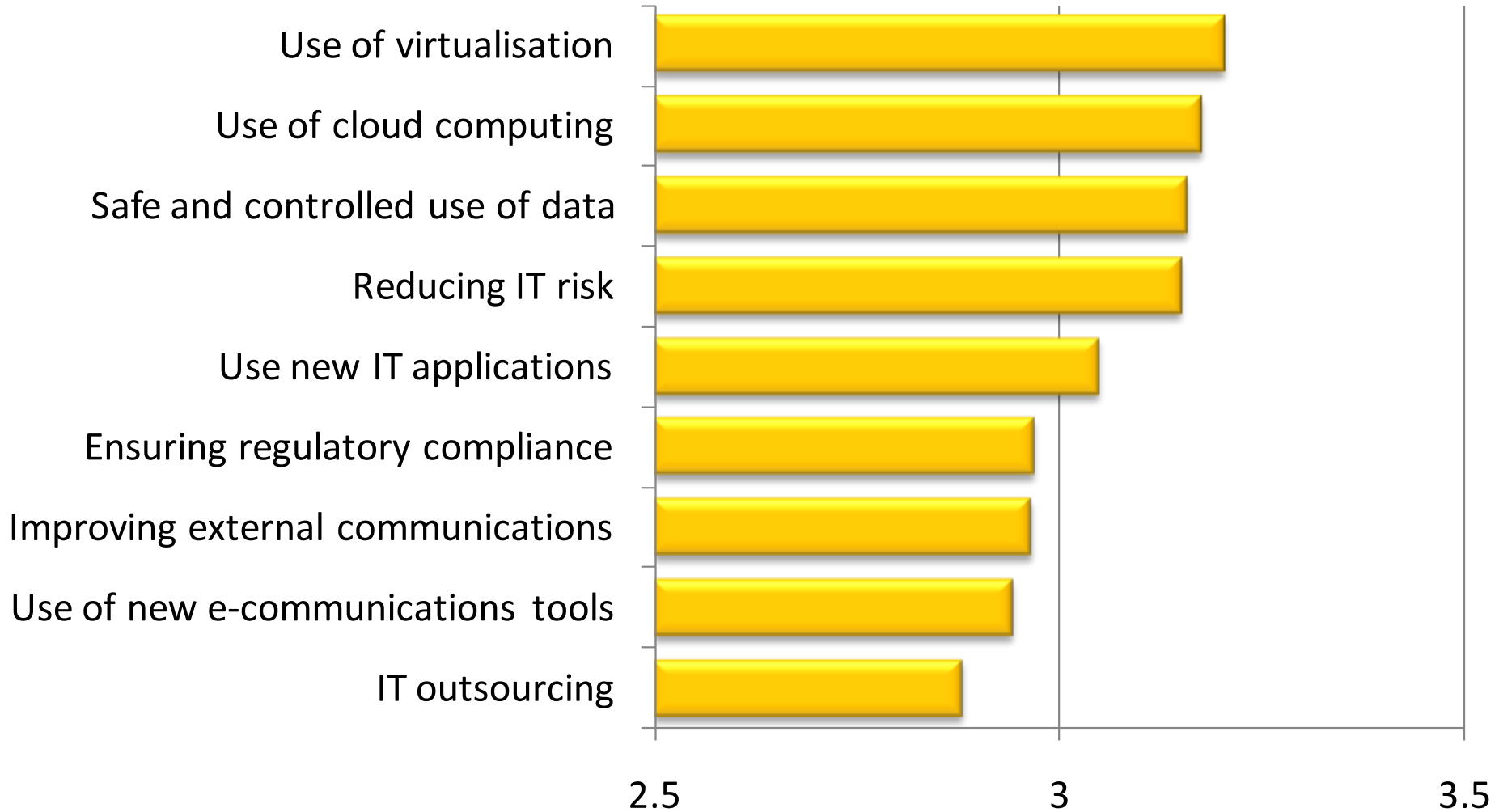


When users have legitimate access to data how confident are you that you can control their ability to do the following?

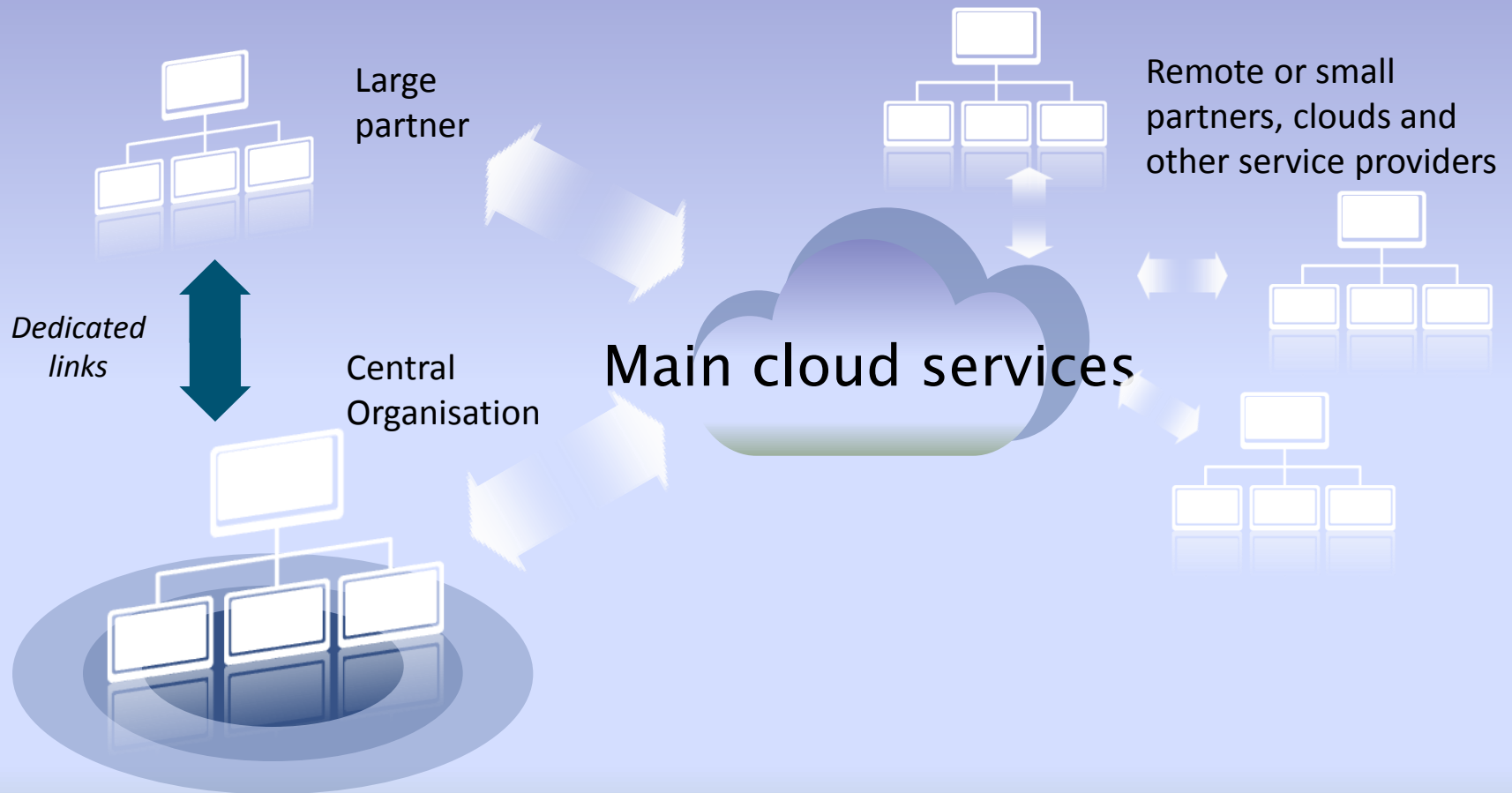


Scale from 1 = “not confident” to 5 = “very confident”

How important do you think IT security is in enabling the following?



Scale from 1 = “unimportant” to 5 = “very important”



- Targeted inbound threats
 - Hacking
 - Phishing
 - Keylogging
 - Trojans
 - Port scanning
 - Malicious sites
 - Download of payloads
 - Attacking wireless access points
- Business threats
 - Denial of service attacks
 - Botnets for DDOS
 - Information interception
 - Viruses, Worms

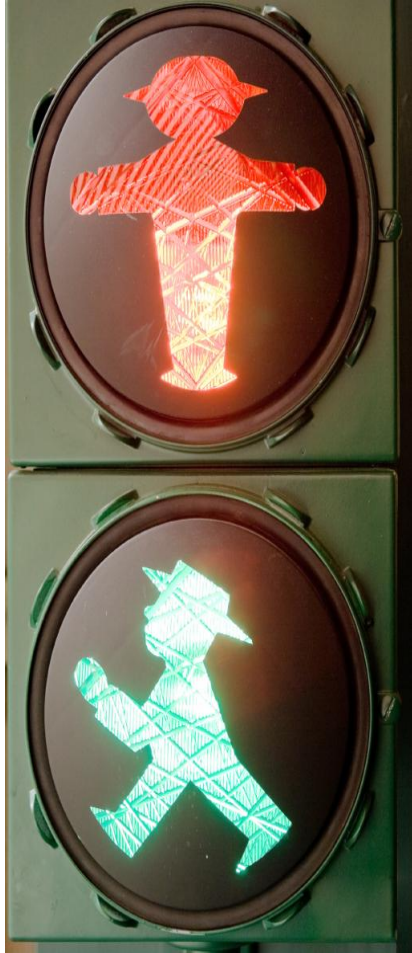




- Email
 - Hitting “send” to the wrong person
 - Attaching the wrong attachment
- Social networking
 - Discussions around Intellectual Property
 - Loss of patentability
 - Attacking the business
 - Brand impact
- Application errors
 - Wrong sharing of information across partners/customers

- Black hats are increasingly sophisticated
 - Full coding and development teams
 - Distributed platforms for attacks
 - Polymorphous threats become more advanced
- Point solutions leave gaps
 - Attempting to block each threat separately gives perception of security – not actual security
 - E.g. Port blocking via standard firewall allows unlimited Port 80 attacks
 - E.g. Anti-virus still allows Phishing attacks





- Anti-virus
 - Across all streams – not just SMTP
 - Fully maintained and monitored
 - Looking at all content – not just bodies, but compressed files, etc
 - Prevent payloads such as root kits, botnet code, etc
- Anti-Spam
 - Minimises volumes of incoming information
 - Increases attention span of user
- DLP
 - Aids stop accidental leakage
 - Helps prevent responding to Phishing attacks
- Full packet inspection
 - Identifies types and content of packets

- “Ultimate security” is a fast moving target
- The black hats are no longer doing this for fun – there is massive financial gain to go for
- A go-it-alone approach is not feasible to implement and manage IT security
- Point solutions will leave gaps that can be exploited
- Partnering with a supplier with deep domain expertise is becoming a necessity
 - They will be watching the “dark side” of bulletin boards and social networks
 - They will aim for zero day security
 - They will be faster in responding to new threats