

The security of IT users and managers

Protecting organisations from their employees

Protecting employees from themselves

9th Sept 2009

Bob Tarzey,
Service Director
Quocirca Ltd



- Are your users taking the security of your organisation seriously enough?
- Can you be sure that information is not being compromised through either malicious or accidental acts within the organisation
- Are the controls you currently have in place adequate enough to protect information from user behaviour, malicious or otherwise?
- Are you confident that for those users in which you place the most trust, the trust is well placed?

- **Are your users taking the security of your organisation seriously enough?**
- **Can you be sure that information is not being compromised through either malicious or accidental acts within the organisation**
- **Are the controls you currently have in place adequate enough to protect information from user behaviour, malicious or otherwise?**
- **Are you confident that for those users in which you place the most trust, the trust is well placed?**

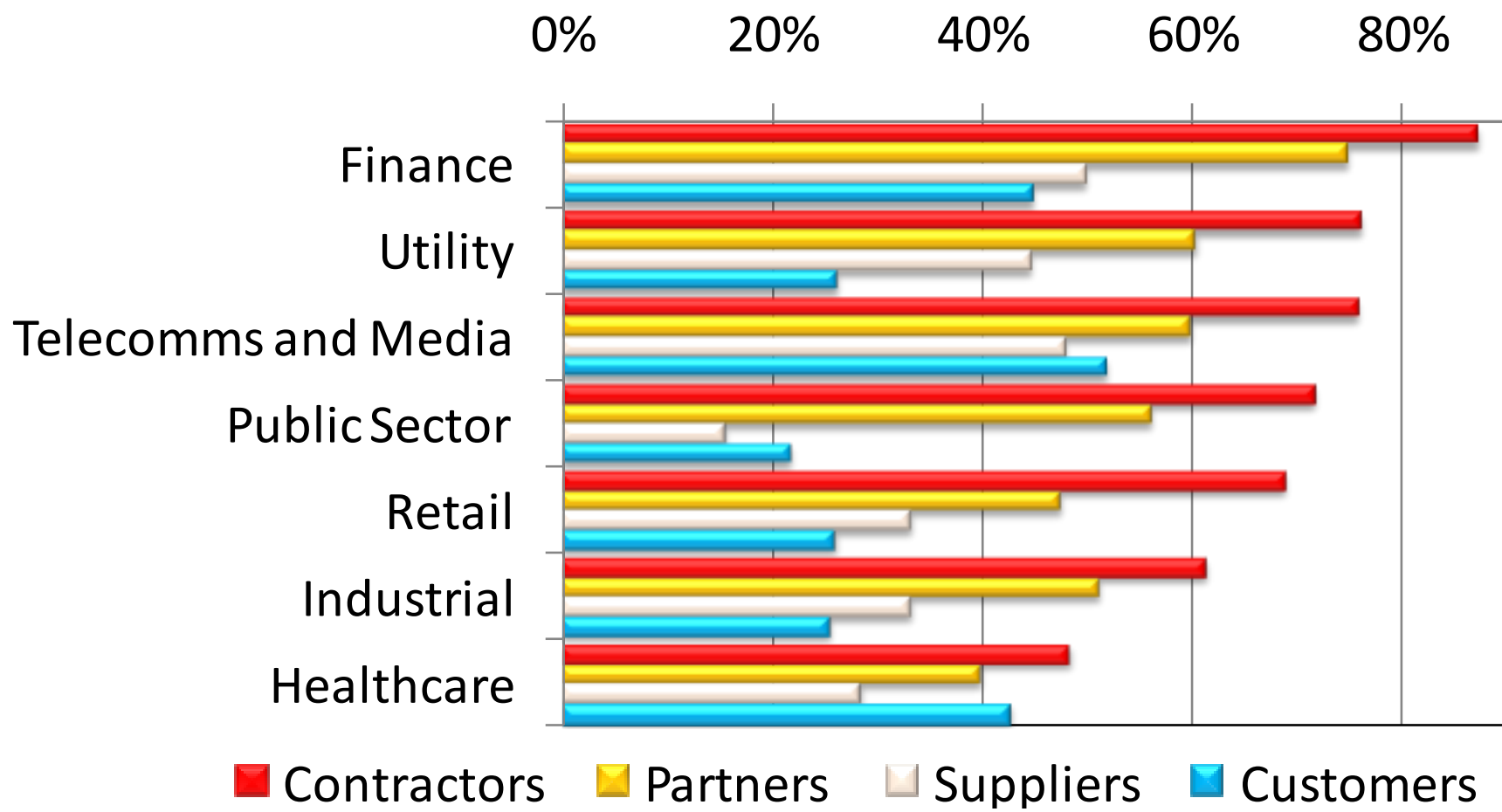


Internal

Privileged

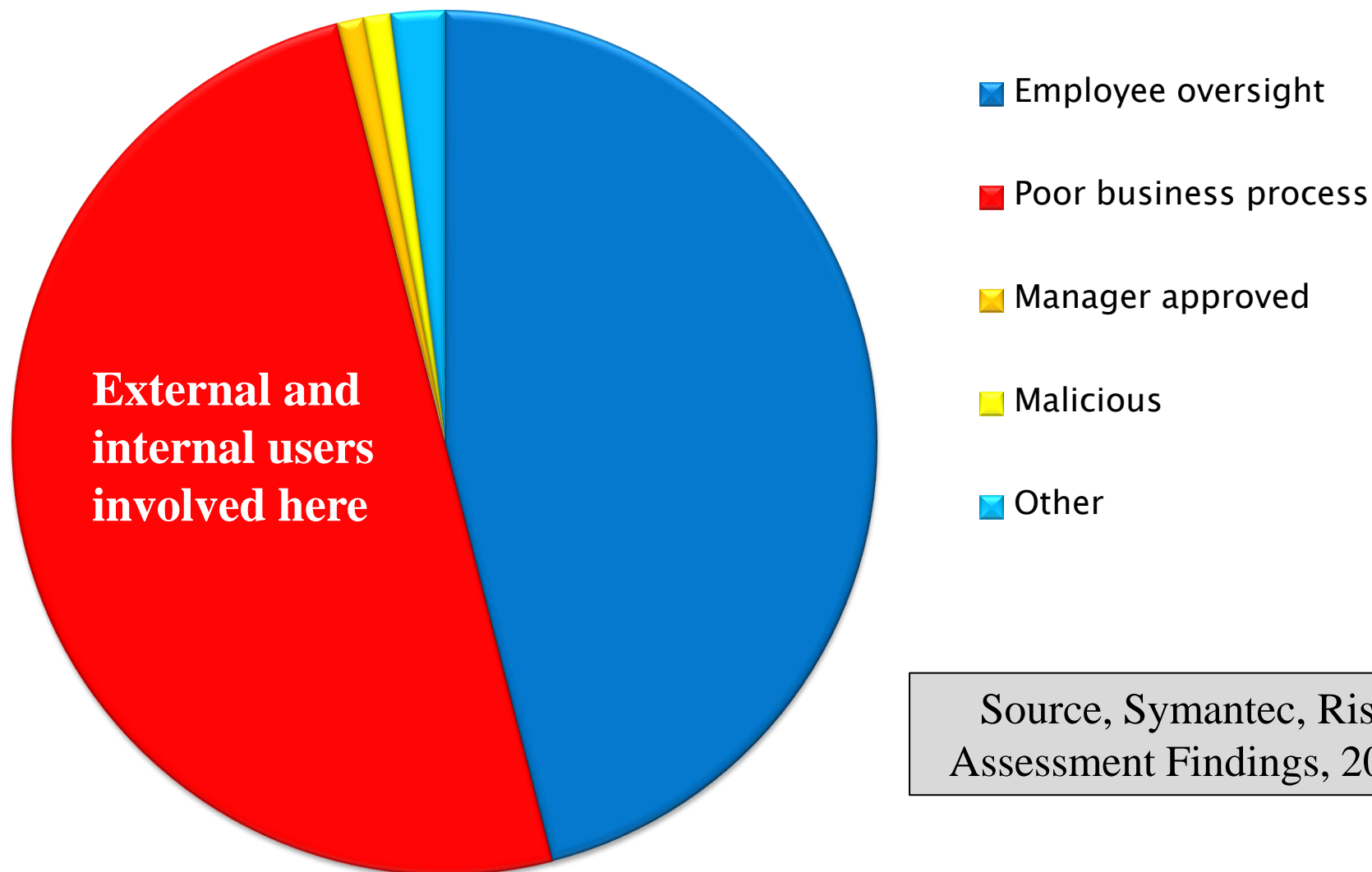
External

Who are the EXTERNAL users?

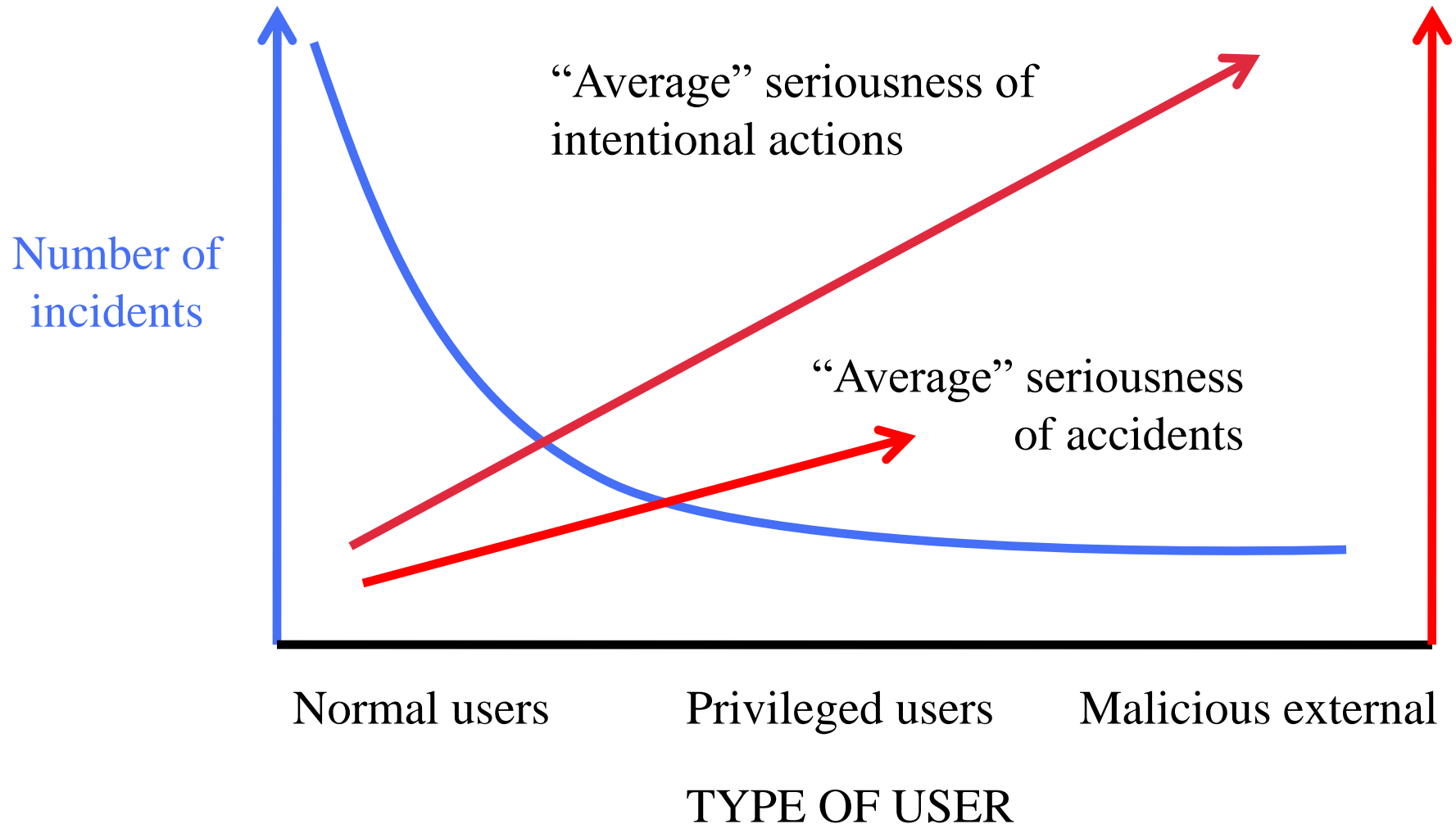


Source, Quocirca, The Distributed Business Index, March 2008

Causes of leaks

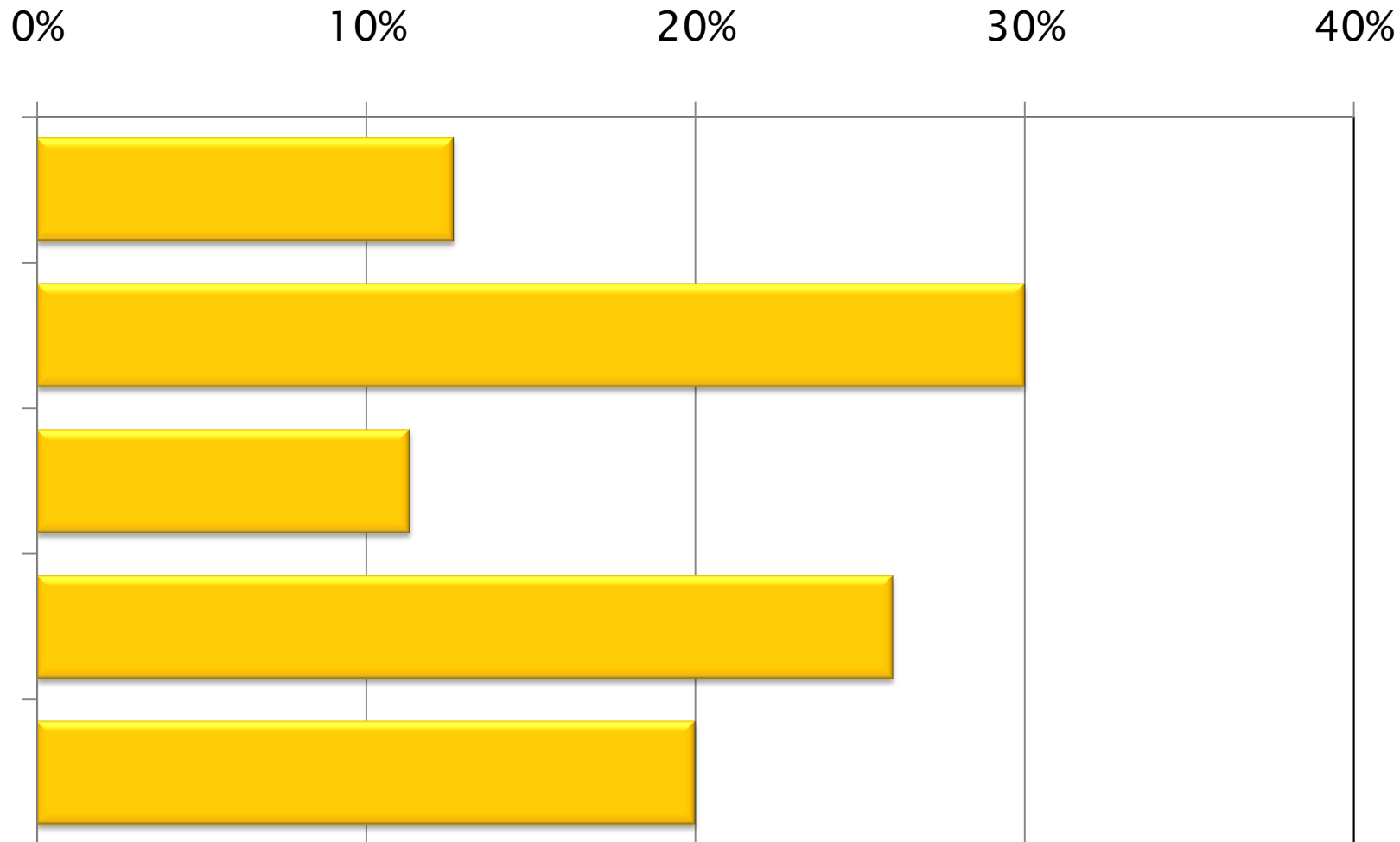


Source, Symantec, Risk Assessment Findings, 2008



- Are your users taking the security of your organisation seriously enough?
- Can you be sure that information is not being compromised through either malicious or accidental acts within the organisation
- Are the controls you currently have in place adequate enough to protect information from user behaviour, malicious or otherwise?
- Are you confident that for those users in which you place the most trust, the trust is well placed?

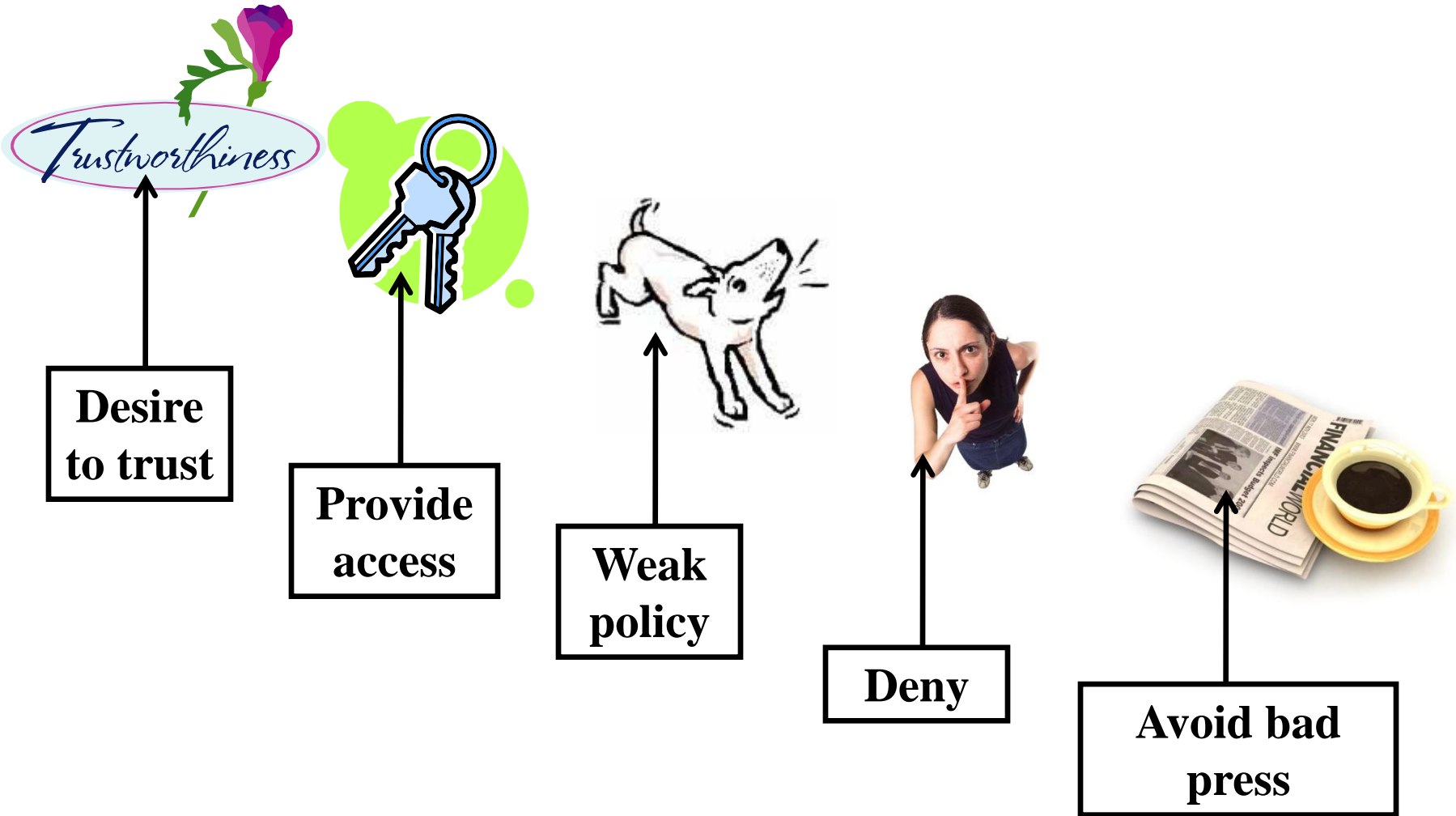
1. Malware
2. Internet
3. Internal users
4. Data compromise
5. External users
6. Use of “Web 2” tools
7. Email
8. Privileged users



Source, Superhighway at the Crossroads – Quocirca, September 2008

1. On mobiles
2. On portable PCs
3. On USB devices
4. Stored externally
5. Being transmitted

Why we ignore the insider threat



- Are your users taking the security of your organisation seriously enough?
- Can you be sure that information is not being compromised through either malicious or accidental acts within the organisation
- Are the controls you currently have in place adequate enough to protect information from user behaviour, malicious or otherwise?
- Are you confident that for those users in which you place the most trust, the trust is well placed?

- **Focus areas**

- People – normal and privileged users
- Content
- Policy

- **Tools**

- ID and access control
- Encryption
- Data loss prevention
- Privileged user management

- Are your users taking the security of your organisation seriously enough?
- Can you be sure that information is not being compromised through either malicious or accidental acts within the organisation
- Are the controls you currently have in place adequate enough to protect information from user behaviour, malicious or otherwise?
- **Are you confident that for those users in which you place the most trust, the trust is well placed?**

No as much as they worry about other things.....



Normal users



Internet



Malware



Email

- 1. Because privileged users are already under control?**
- 2. Because of that innate trust in privileged users?**

- **NO – most business do not have the tools in place for this**
- **And bad practice is common place:**
 - Account sharing
 - Default access
 - Wide ranging access
 - Generic usernames
 - Easy to remember passwords
 - Rarely changed passwords

Yes, much complacency and/or ignorance

- Privileged users make mistakes too
- Privileged users often have unlimited data access
- Privileged user can be, or turn, bad

2007 – “Low level” Database administrator stole 2.3 million credit card records from Fidelity National with the intent of selling them, he worked for a 3rd party

2008 – Soc Gen trader, Jerome Kerviel’s €4B+ banking fraud attributed to abuse privileged user access and “terrible IT security”

2009 – UK DWP reports sacking of staff for viewing celebrity tax records

Money

Coercion

Ideology

New job

Spite

Gossip

2008 – AMD Employee charged with \$1B IP theft from former employer Intel

2008 – 30 months jail for systems administrator Yung-Hsun Lin for planting logic bomb, he thought he was going to lose his job

2009 – Fannie Mae Unix engineer (a contractor) indicted for planting malicious script

1. Compliance audit failure **Misplaced?**
2. External threats
3. Loss of IP
4. Loss of data
5. Internal threats
6. IT operations risk
7. Damage to brand

- Better management of privileged users
 - They only have the rights to do the job in hand
 - An audit trail is kept
 - Unique IDs are enforced
 - Bad practice is prevented

Privileged users are protected from themselves and compliance can be demonstrated

- You can't expect any user to take "full" responsibility for the security of data
- Most organisations are not sufficiently aware of who their users are and what they get up to
- Most organisations do not have the tools in place to ensure their users are protected from themselves
- The problem is at its worst when it comes to privileged users – complacency is rife
- This makes mockery of the misplaced confidence businesses have in their ability to comply

- New Quocirca research report to be published in October
– freely available at www.quocirca.com

Thank you
Bob Tarzey
Quocirca
www.quocirca.com