

A compliance oriented IT architecture for financial services organisations

Bob Tarzey

Analyst and Director, Quocirca Ltd

Dec 7th 2011

Financial regulators

GLOBAL



EU



NATIONAL



Non-financial regulators



Information Commissioner's Office



DATA PROTECTION ACT 1998



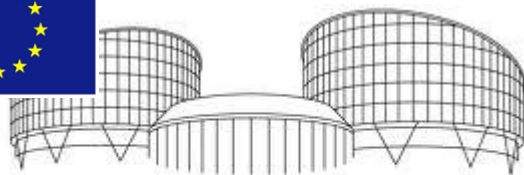
Regulation of Investigatory Powers Act 2000

USA PATRIOT ACT



Sarbanes-Oxley

Financial and Accounting Disclosure Information



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME



PCI DSS V2.0 Requirement 8

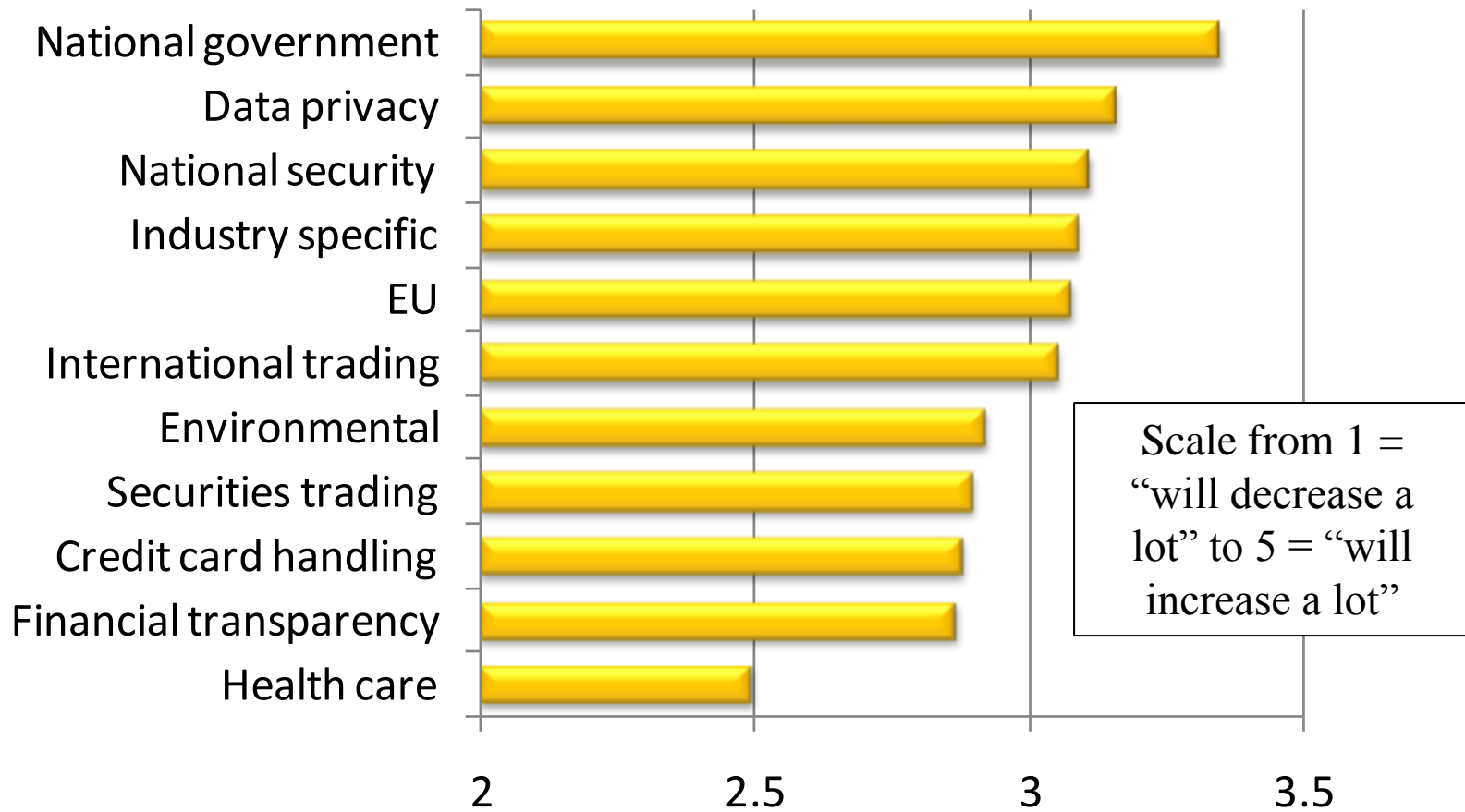
“Assign a unique ID to each person with computer access”

“ensures that each individual is uniquely accountable for his or her actions”

UK DPA

“Only allow your staff access to the information they need to do their job and don’t let them share passwords”

How do you see regulations in the following areas affecting your organisation over the next 5 years?

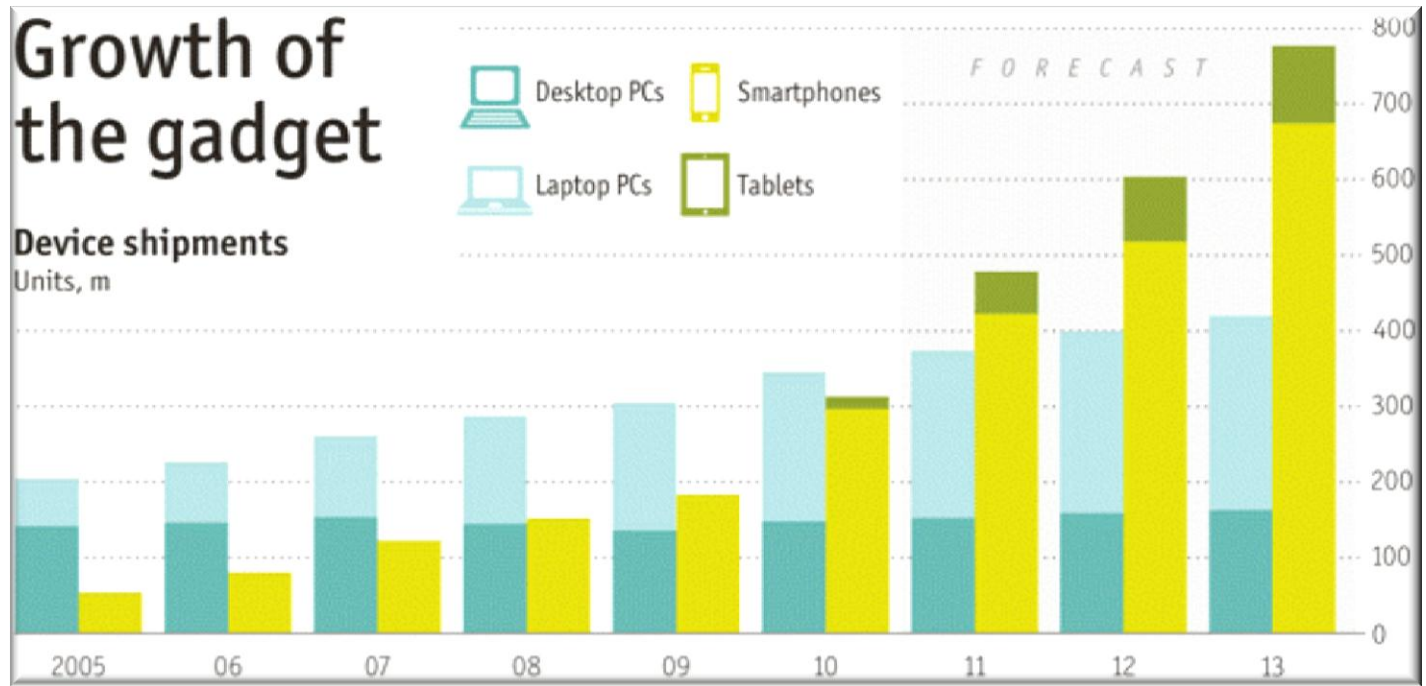


Life is not going to get easier, regulations are expected to increase in all areas

Source, Quocirca "You sent what?", 2010

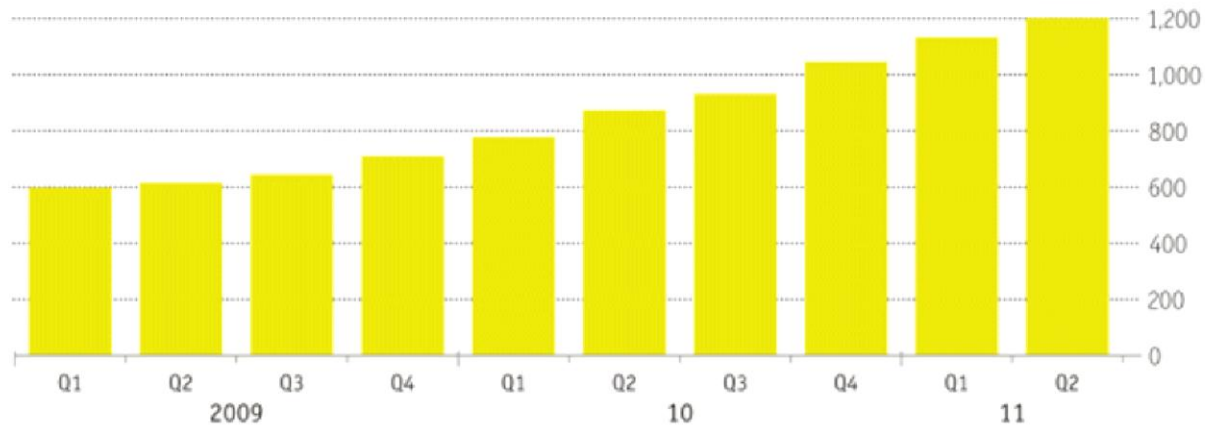
Growth of the gadget

Device shipments
Units, m



Sneaky geekery

Unique pieces of mobile malware, cumulative total

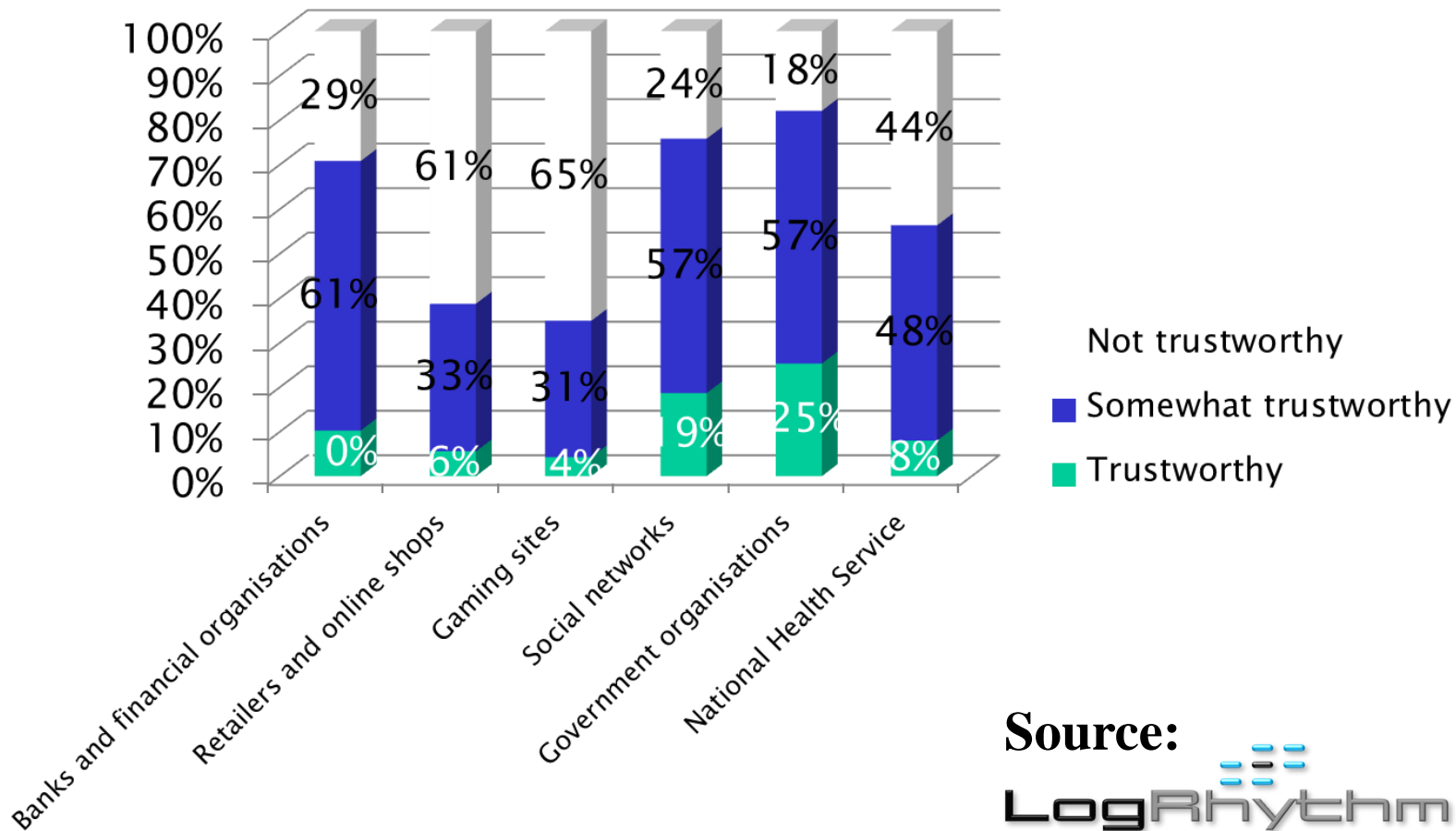


Source: McAfee

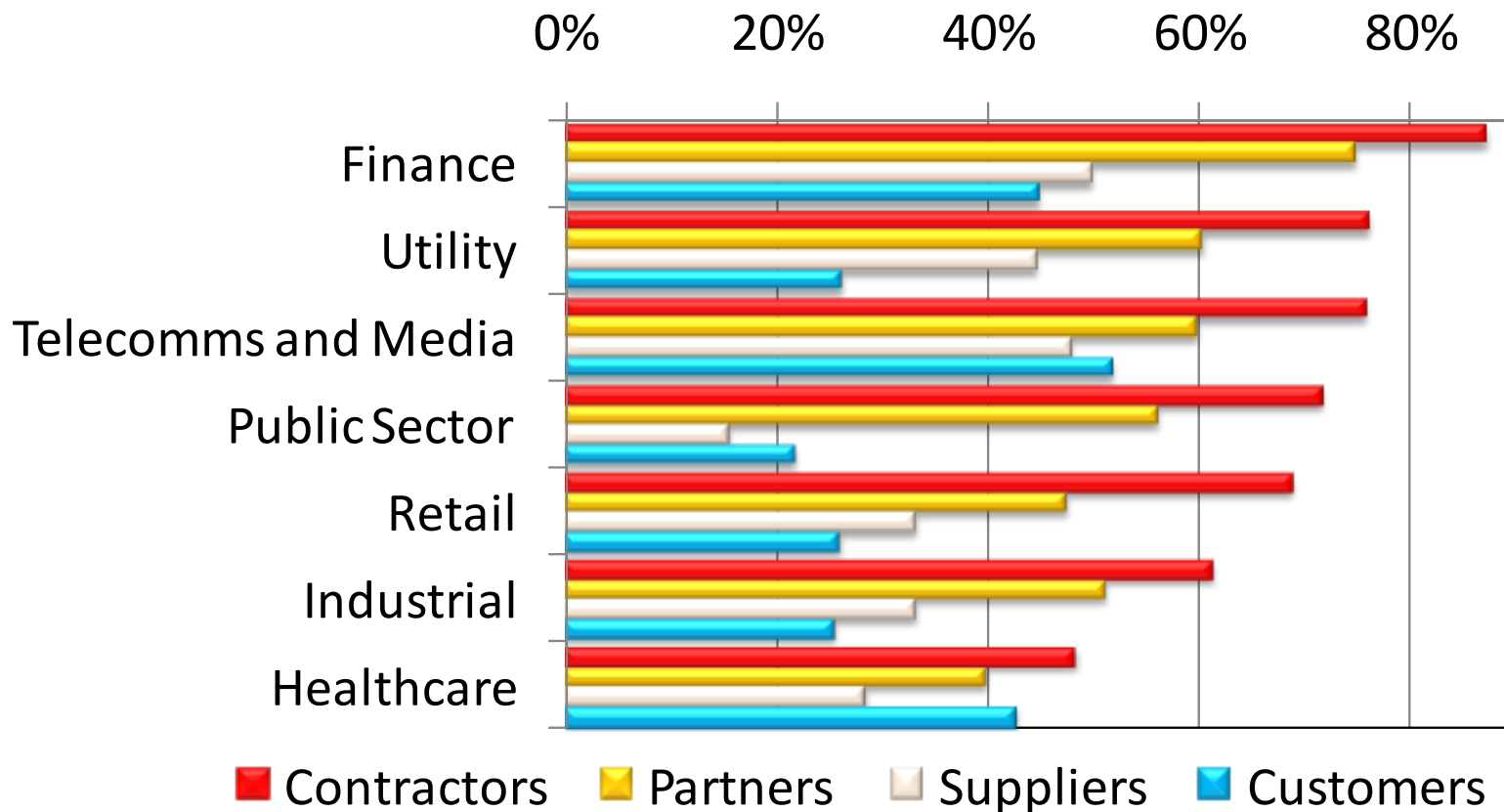
**Source:
Economist
Beyond the
PC
Oct 2011**

The court of public opinion

In terms of keeping your records safe, how trustworthy do you feel the following organisations are?

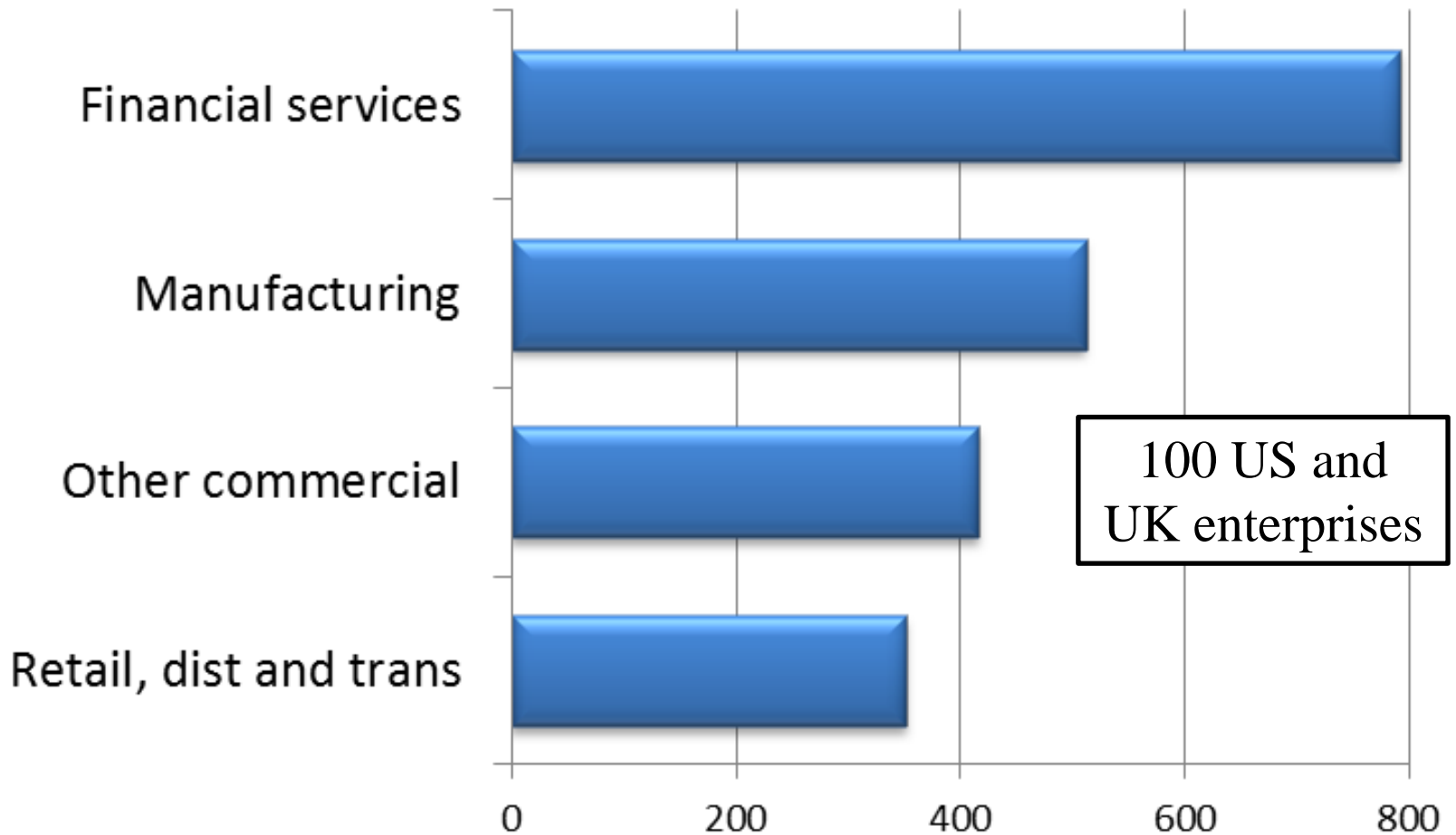


Percentage saying external users are provided access to internal systems



Source, Quocirca, The Distributed Business Index, March 2008

How many mission-critical applications does your business track? (average number of applications)



New Quocirca research sponsored by Veracode (full report in Jan 2012)

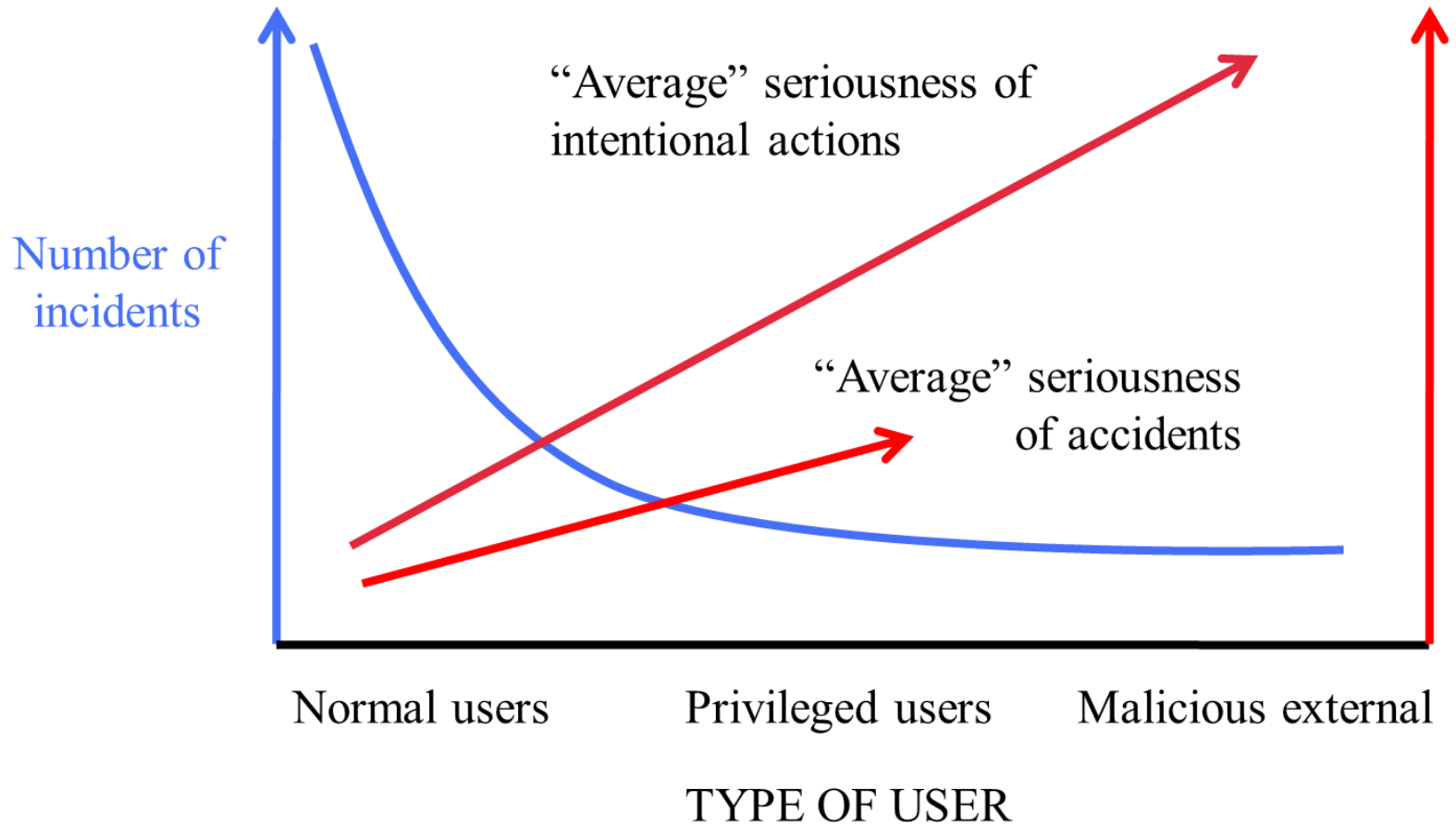
VERACODE

The IT burden in financial services

- Delivering financial services is all about data
- Much of the burden for providing the information for proving compliance falls on IT departments
- The need to be able to prove who has been doing what with data over time
- Includes:
 - Normal users
 - Privileged users
 - External users

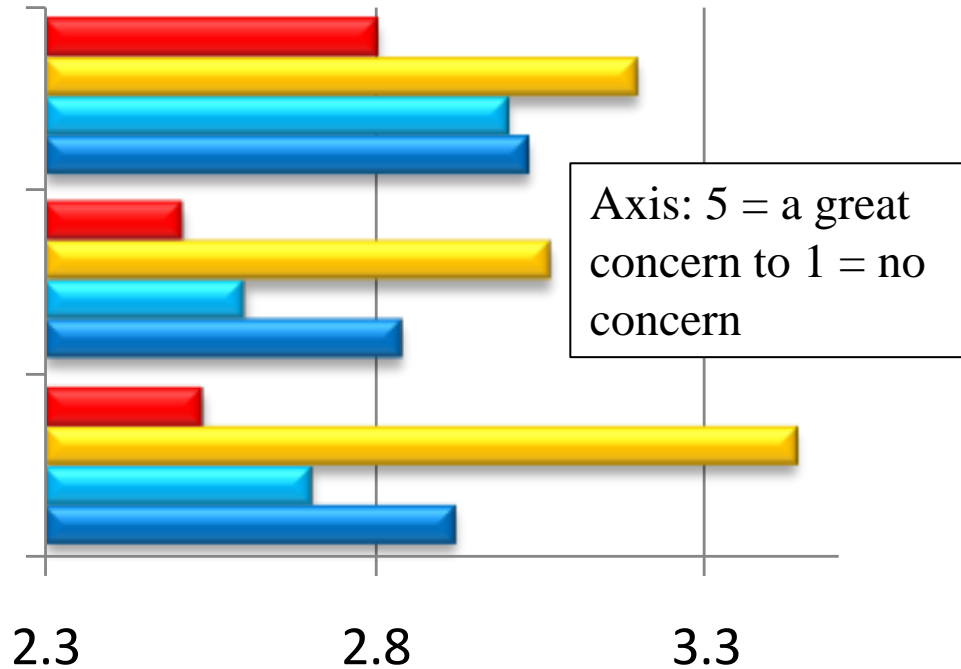


Relative user risk



When your employees leave your organisation, how much do the following concern you?

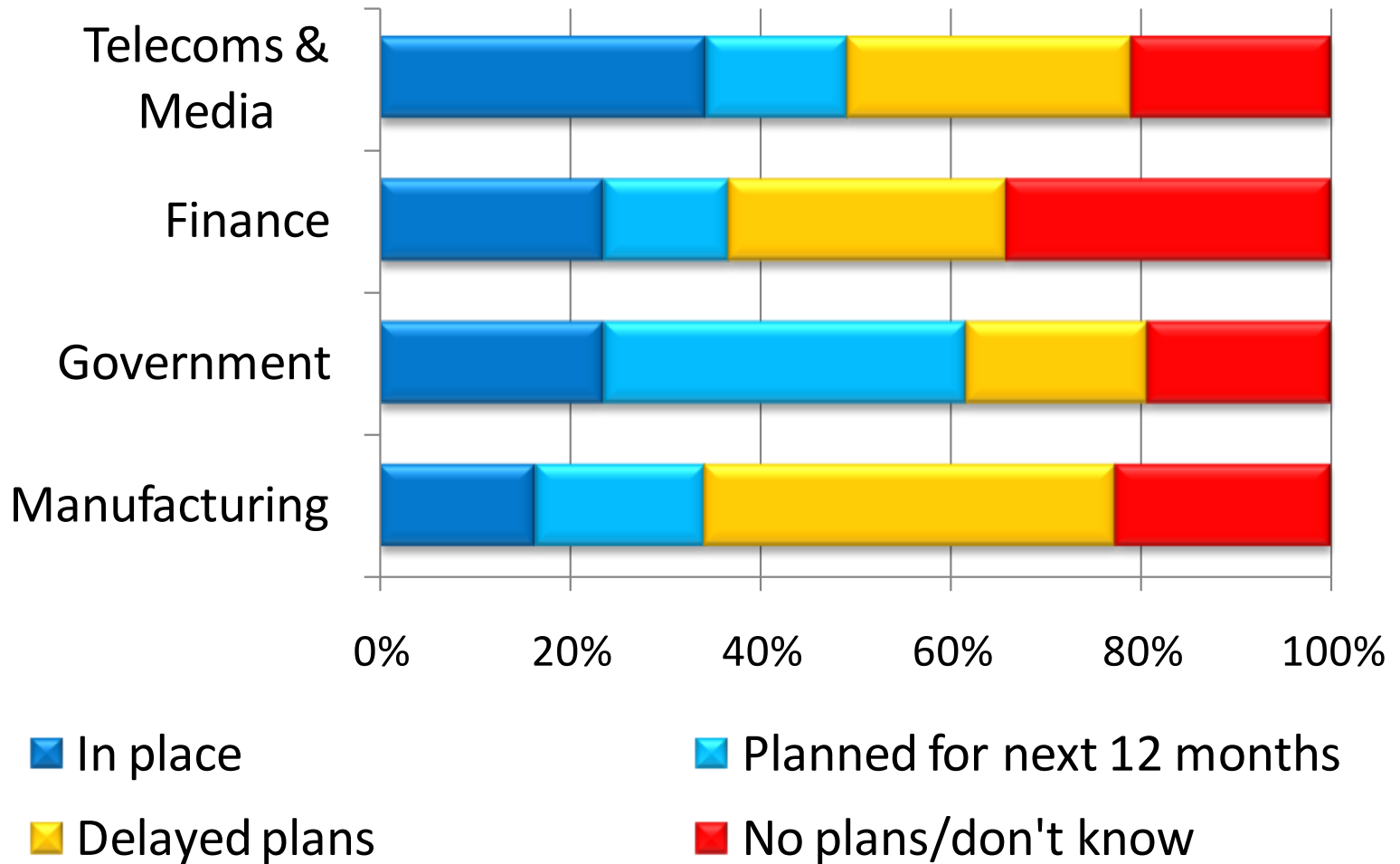
- A record exists of the removal of access rights
- Their IT access rights have been removed
- They may take valuable or confidential data



- Telecoms & Media
- Manufacturing
- Government
- Finance

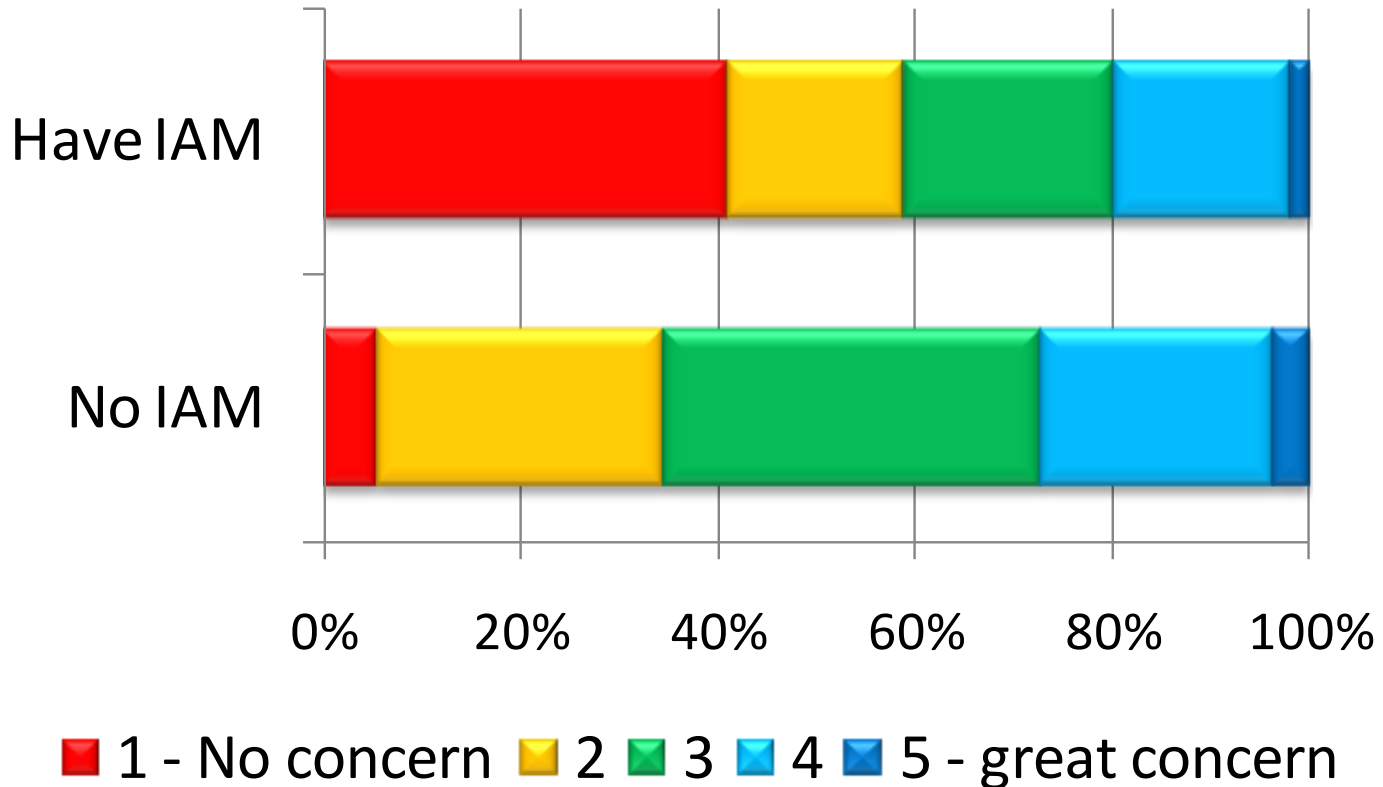
Source, Quocirca
“You sent what?”, 2010

Has your organisation deployed a full identity management suite?



Source, Quocirca
“You sent what?”, 2010

Use of IAM coloured by concern over managing access rights of departing employees



....they should – the evidence is clear
IAM enables safe management of access rights

Nearly all businesses use Microsoft Windows Server

For the majority it is their main server operating system

So, nearly all business have and use Windows Server Active Directory



It makes sense to use Active Directory for centralised identity management



Identity Commandments



Standards provide a basis for building a compliance orientated architecture that includes identity and access management based on Active Directory

THANKYOU

www.quocirca.com

bob.tarzey@quocirca.com