

# To lose one set of data may be regarded as misfortune...

Working towards a compliance oriented architecture

Clive Longbottom,  
Service Director, Quocirca Ltd

# Data Leakage – it's in the news

Telegraph.co.uk

Home News Sport Finance Lifestyle Commen

UK World Politics Celebrities Obituaries Weird E

Election Results Map UK Political Database Political Pa

HOME > NEWS > NEWS TOPICS > POLITICS

## Hundreds of laptops owned by Whitehall departments lost or stolen in two years

Hundreds of laptops owned by government ministries have been lost or st

*Privacy and Security*

Tuesday, July 20, 2010

### Massachusetts Facility Reports Data Breach of 800,000 Records

On Monday, officials at South Shore Hospital announced that the personal information of a individuals could be missing after an off-site for destroying the computer files did not receive *Boston Globe* reports.

## UK headed for data breach disclosure law within four years

Europe working on legisla

Post a comment

By Nick Heath, 16 July 2010 15:5

## Skipton faces fine for serious data breach

Jeff Prestridge, Financial Mail  
30 January 2010, 12:00am  
Reader comments (6)

Skipton Building Society faces a heavy fine from the **Financial Services Authority** after a serious breach of data security procedures that resulted in more than 3,000 savers receiving financial details about other customers of the **mutual**.

## Three local authorities lose sensitive data on children

ICO raps Barnet, West Sussex and Buckinghamshire for cavalier attitude to data protection

Dan Worth

V3.co.uk, 08 Jul 2010

## Regulator to impose data breach fine

Neil Hodge, Financial Director, 24 Mar 2010

New powers will see financial penalties in an effort to reduce serious data breaches. **Neil Hodge** reports

**The UK's data regulator** will have new powers from April which will allow it to issue fines of up to £500,000 for serious breaches, as well as enabling it to conduct compulsory audits in central government departments where breaches may have occurred.

We are being told we must....



Information Commissioner's Office



... And punished if we do not



## Apple throws out more stats on enterprise uptake of iPhone, iPad

By Eric Lai | July 22, 2010, 3:52pm PDT

### Summary

*Enterprise uptake for the iPad, iPhone continues to grow, Apple COO Tim Cook said this week.*

**How 'bout dem Apples?** More for or evaluating the iPhone and evaluating the iPad, said the company, despite the IP reported stellar revenue and

For comparison, the 80% of iPhone is up from 70% six m

[Home](#) > [Mobile and Wireless](#)

### Opinion

## Increased mobility, increased risk

By Kathleen Else

June 30, 2010 12:18 PM ET

[Comments \(1\)](#)

[Recommended \(3\)](#)



Share

[Where am I?](#) > [Home](#) > [In-depth](#) > [Analysis](#) > [Privacy & Data](#)



Mark Zuckerberg

## Facebook: 500 million reasons to be cheerful

Social networking site hugely popular despite lingering privacy concerns

David Neal

and remote-access boom is technology powered and midsize businesses (SMB) increasingly them rebound in 2010, improved mobility

## Twitter usage boosts customer trust

June 29, 2010

With more than 100 million consumers using the social networking site, [Twitter](#) represents a huge market of potential customers that businesses can engage. A new study conducted by Fleishman-Hillard has found that not only can companies use Twitter to promote their products, but it also boosts consumers' trust in a brand.

 E-mail |  Print |  BOOKMARK   ... |  Take Us With You |  Buzz up!

## Employees Influencing Enterprise IT

Demand for consumer-oriented devices in the workplace causing IT leaders to rethink how they procure and secure technology, a new survey finds.

By [Mathew J. Schwartz](#)  
InformationWeek

July 22, 2010 01:05 PM

## Ignore Consumerization of IT at Your Own Peril

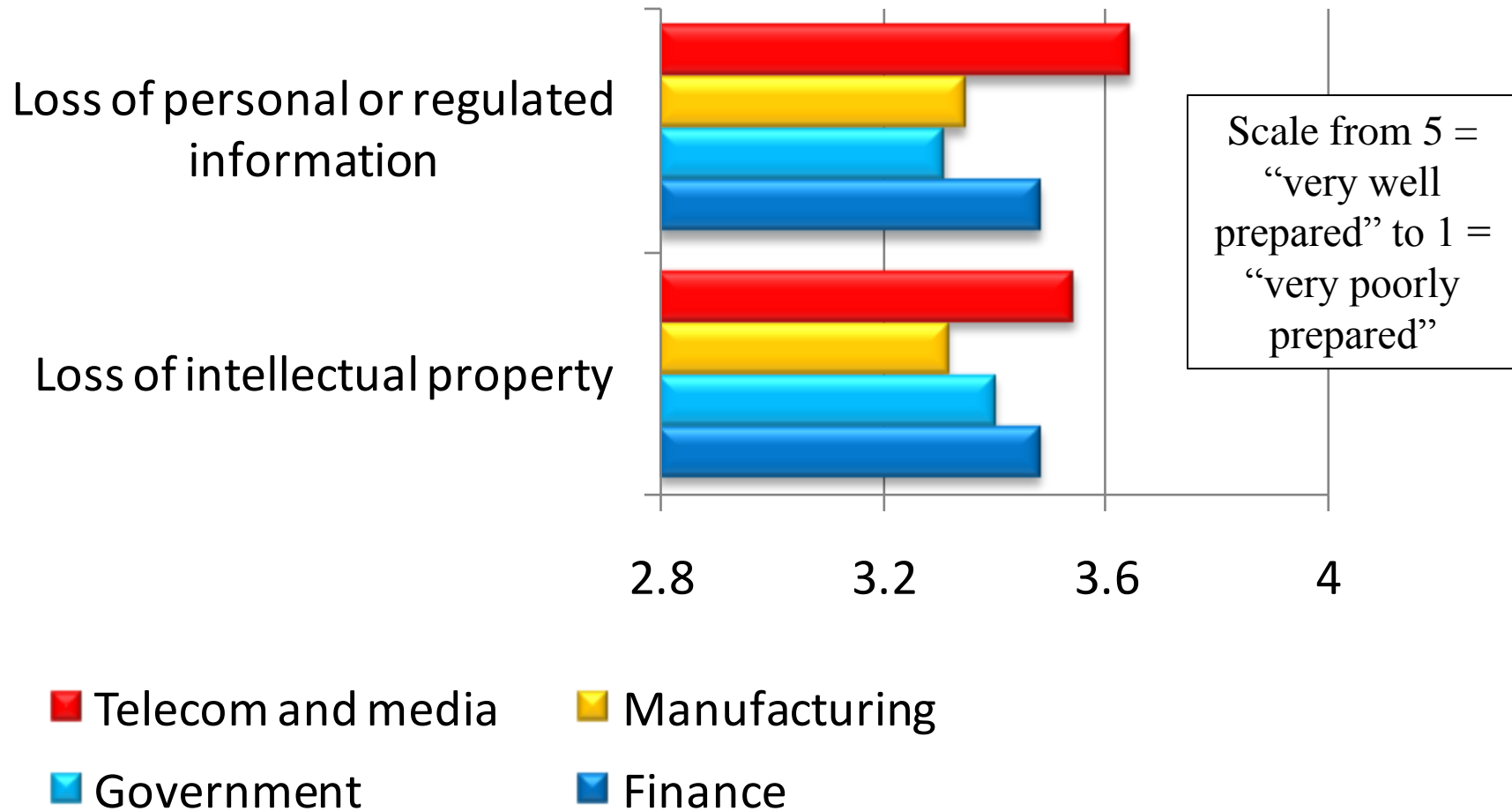


Posted by [Michael Vizard](#) 30-Jun-2010 12:37:28

# Quocirca Research Findings

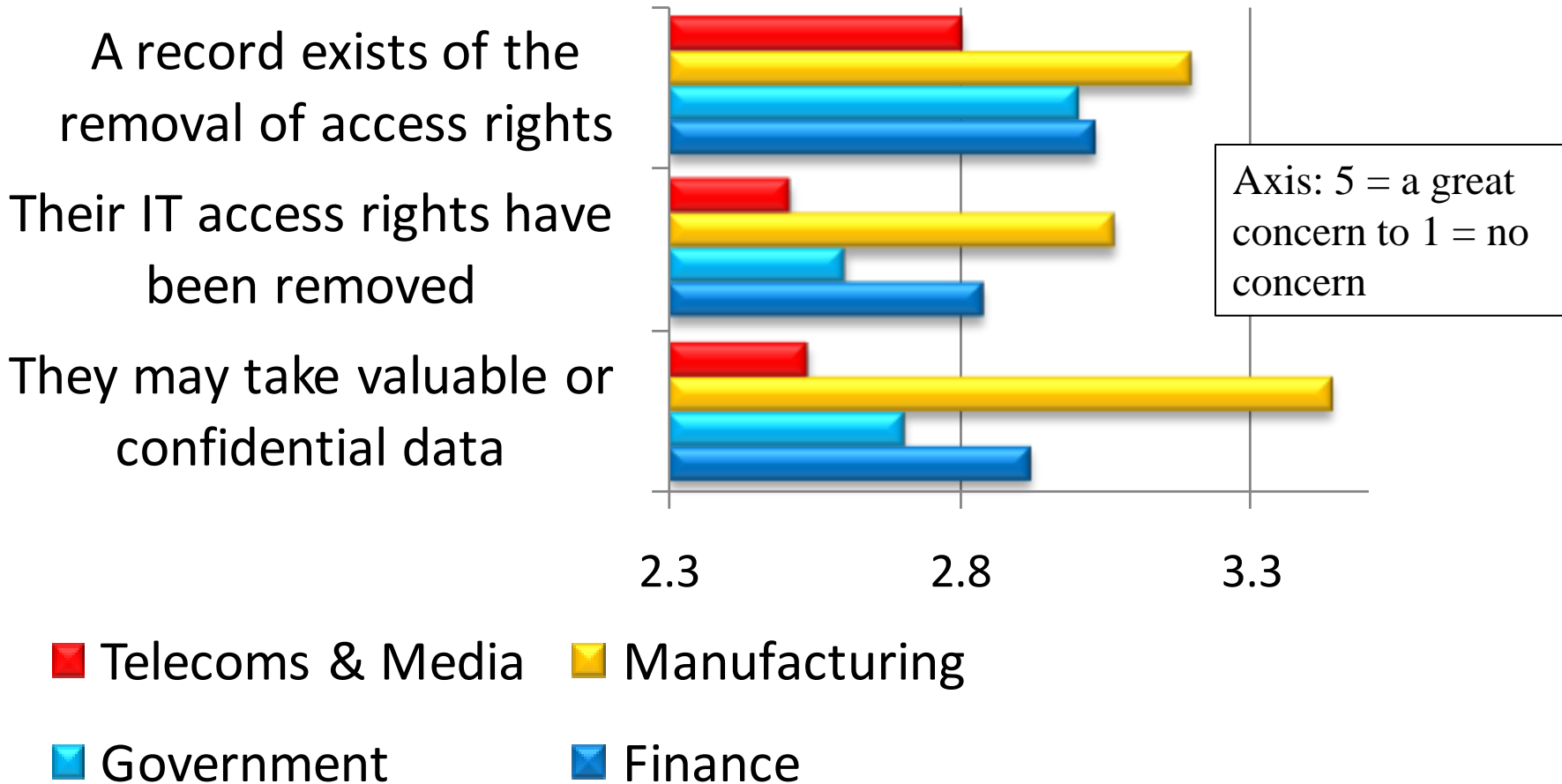
Based on 270 telephone interview in June 2009  
Research conducted for CA Technologies, Inc.

# How well prepared is your organisation to protect against the following risks?



Manufacturing organisations worry about *intellectual property*  
Governments worry about *personal information*

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



The worry manufacturing has about IP is reflected in the way they worry about loss of confidential data – and in removal of access rights

Security Needs



Content



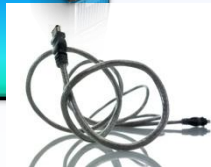
People



Hardware




Network

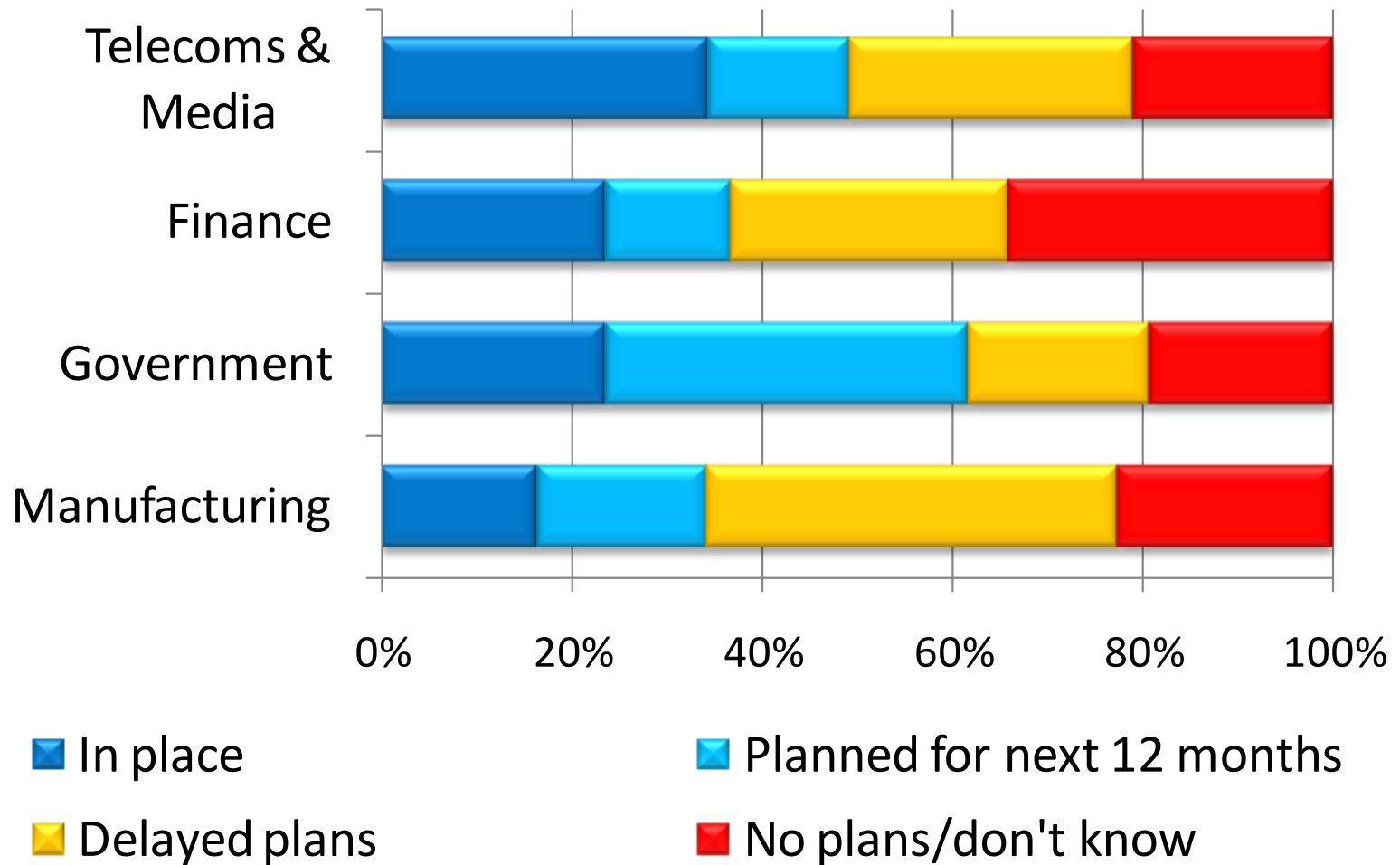


Time

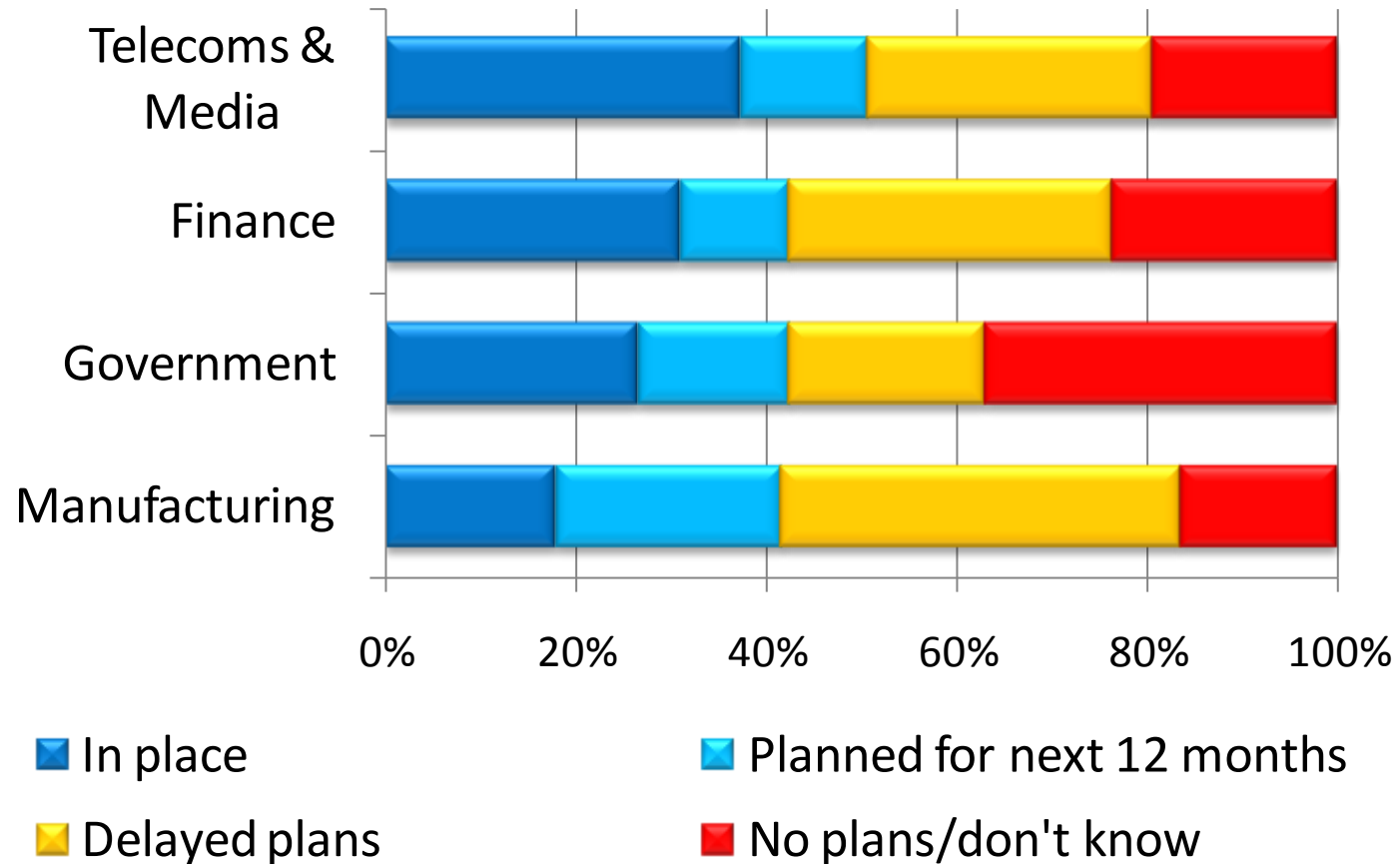
- A compliance oriented architecture has three critical components:
  1. A full identity and access management systems (IAM) that encompasses the whole value chain
  2. The capability to search and tag data, both stored and when in use
  3. The ability to link people to data and define policies about usage
  4. The capability to encrypt data, both at rest and on the move

- It's not focused on the hardware
  - It's not focused on the network
  - It's not focused on the application
- 
- It *IS* focused on information and data in context with the time and place of access by a specific person or role
    - i.e. it is about intellectual property and data privacy – the lifeblood of today's organisations

# Has your organisation deployed a full identity access management suite?



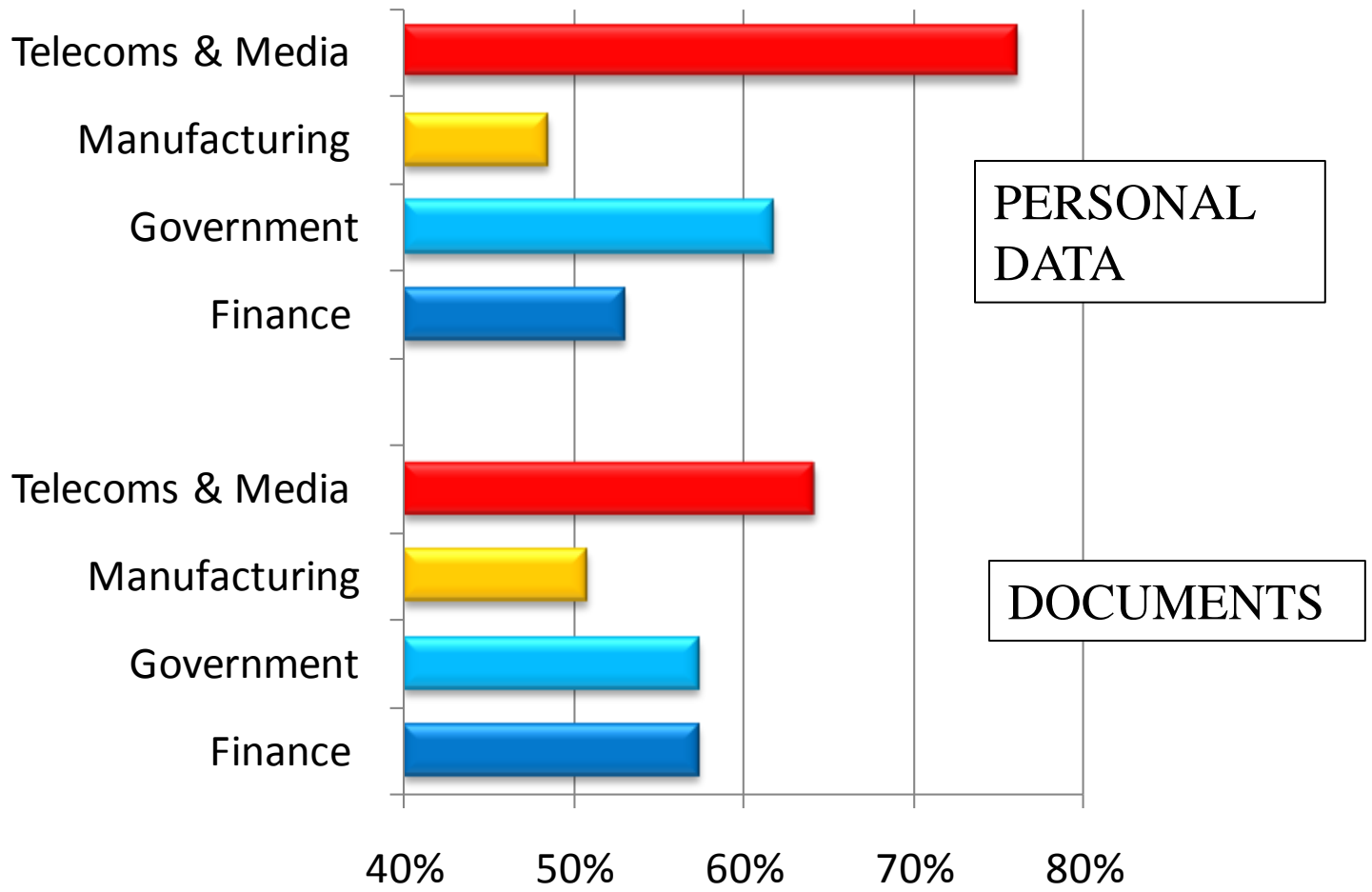
The majority of organisations do not have full IAM, and many are delaying plans due to the recession



DLP is only deployed by about 25% of organisations.....

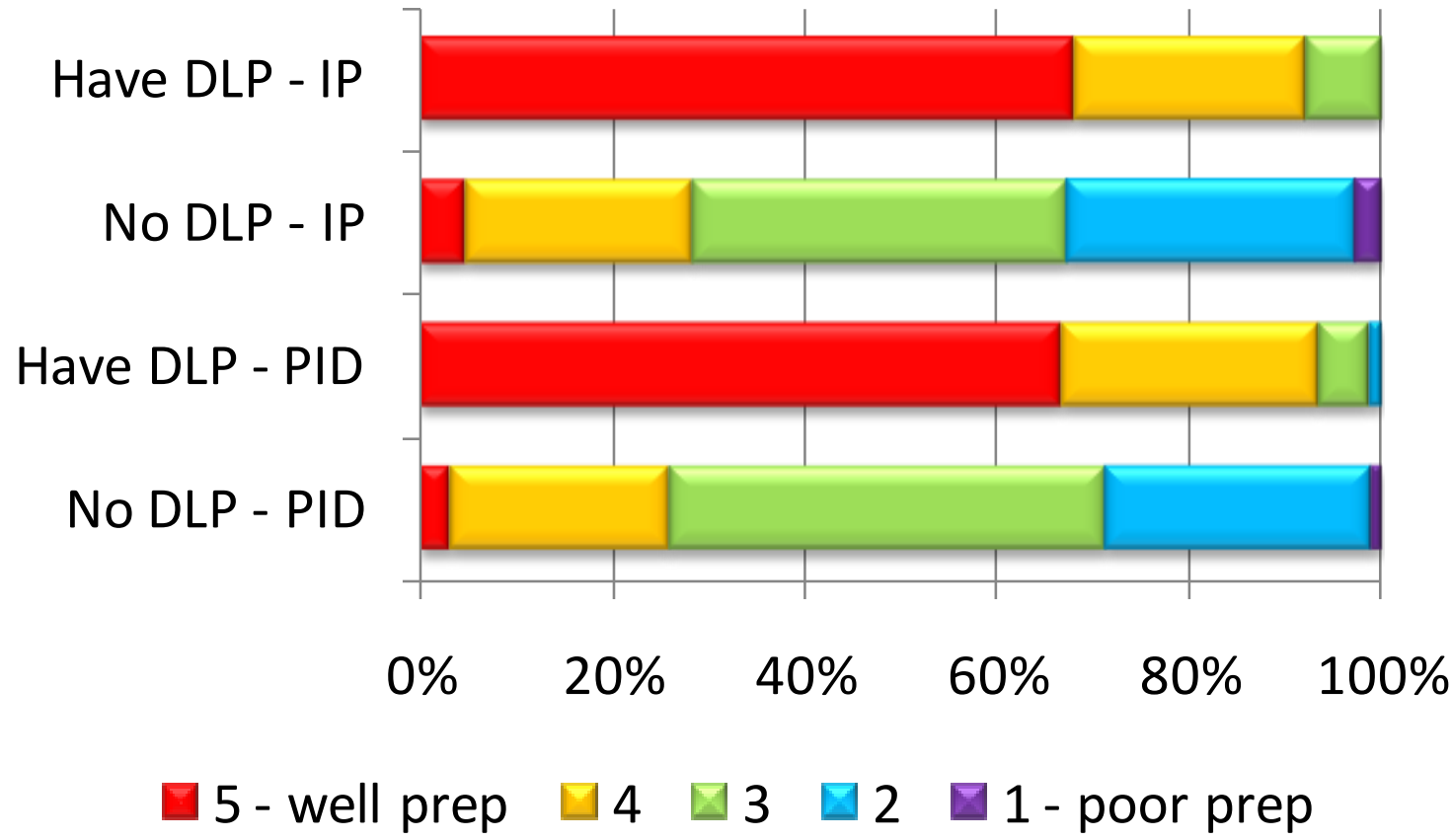
# Do you have a system for indentifying and classifying the following types of data?

Percent already having system in place

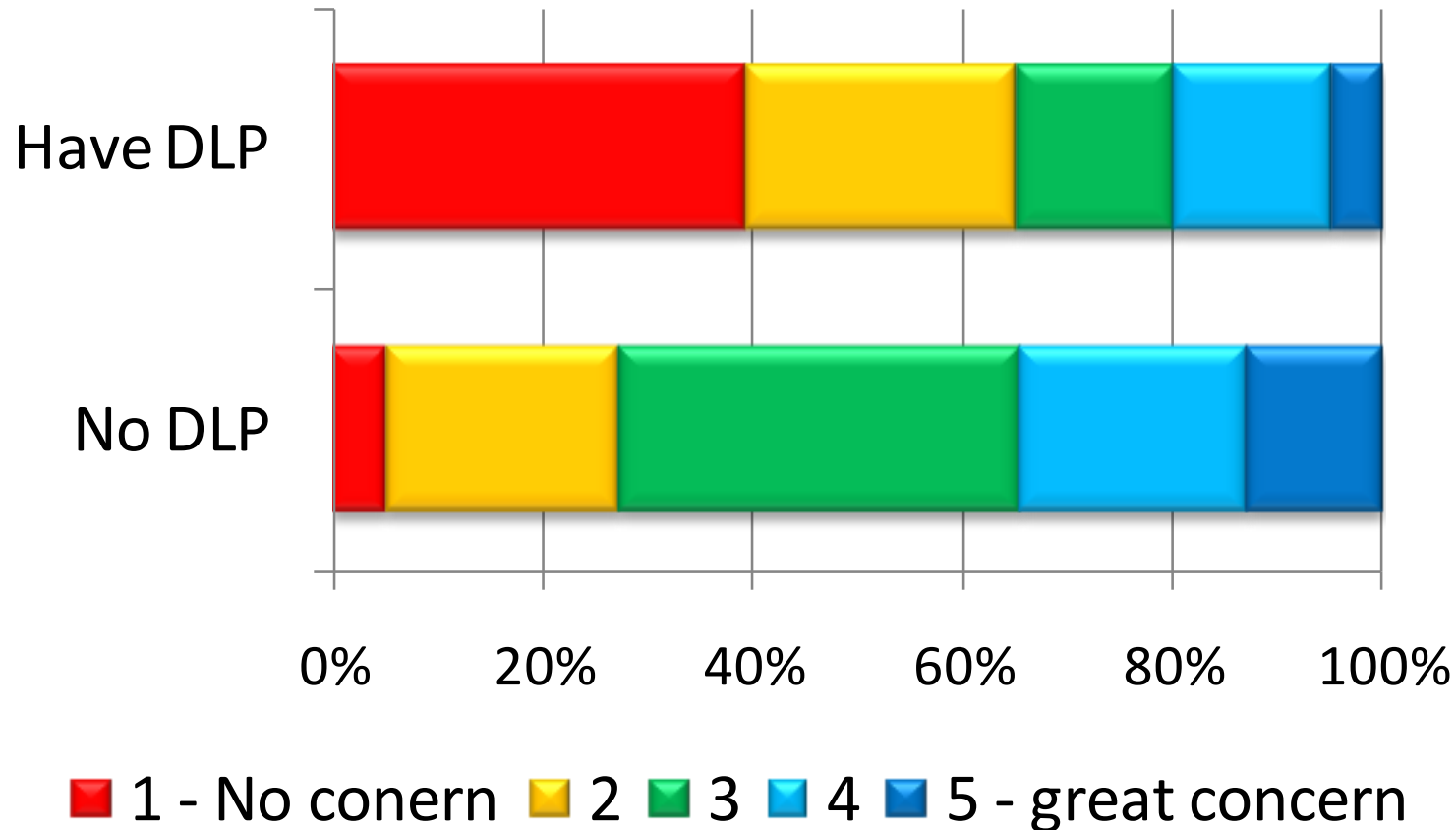


Many organisations have limited capability to classify data.....

# Use of DLP coloured by confidence to protect IP and personally identifiable data



....they should, the evidence is clear data classification as part of *DLP protects IP and personal data*



....they should do – the evidence is clear  
*DLP protects data from employees intentional or deliberate actions*

- Start with the data:
  - Is it formalised (in a database)?
  - Is it ad-hoc (stored on file and print servers, or elsewhere)?
  - Is it “clean”?
  - Is it classified and tagged?

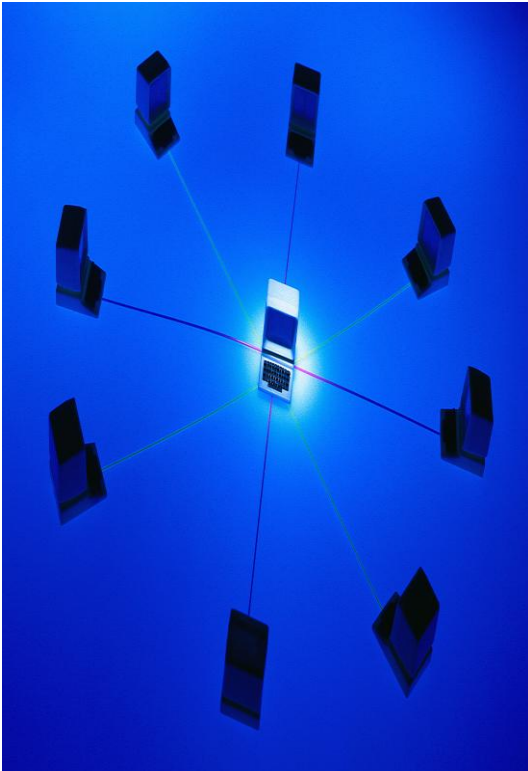


- Start with high level deduplication
  - Rationalise all multiple copies of the same file
- Rationalise data stores
  - Having multiple databases with the same data in them is not a good start
  - Use master data management to provide optimised data
- Ensure that data is valid
  - Use full data cleansing technologies to ensure e.g. names, addresses, telephone numbers are all validated – and that duplicate customers/suppliers are identified and rationalised
- Look at full deduplication
  - Block level dedupe adds a layer of security

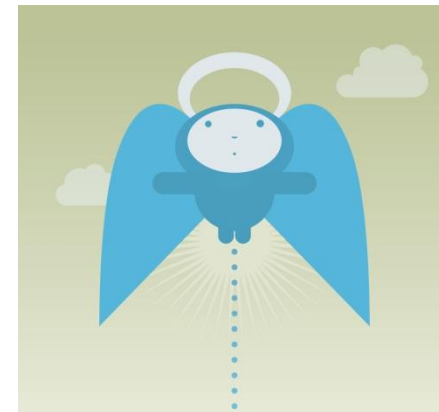
- Develop a company policy on information
  - Who can see what, when and where
  - Create basic templates for basic classification
    - Public, private, classified, for your eyes only
  - Use meta data wherever possible as classification tags
  - Use automated data classification combined with manual tagging



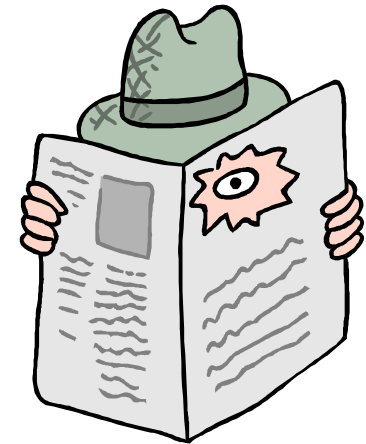
- In-organisation networks
  - Use data bridging to keep data within certain parts of the network, if necessary
  - Use roles and individual identities extensively
- Edge of network inspection
  - Use deep packet inspection to “see” what is being sent
  - Use common sense and blocking to prevent certain data types going off site
    - E.g. IF <task worker> then block, ELSE IF <Exec> then warn, ELSE raise malicious event with IT



- The who, where and when...
  - Who by role and individual
  - Where by fully controlled, partially controlled, open
    - Office is different to home is different to Starbucks
    - Employee is different to contractor is different to supplier is different to customer
  - When by is this possible?
    - Last known network contact from New York, 5 minutes later from Moscow...



- Use encryption
  - Use public/private pair keys
  - Ensure public key delivery is secure
- Ensure policies and contracts are solid
  - No access details sharing, full disclosure of individuals joining and leaving the external
- Full audit
  - What was (attempted to be) accessed , when, from where, by whom, and what was done with it?





- Centralise data wherever possible
  - Minimise the amount of data on the device
- Encrypt data on the move and at rest
- Ensure all devices can be micro-managed
  - Block and delete if lost/stolen
- Ensure policies in place for all removable media
  - Full disk/device encryption
  - Biometric or changing key tokens

- The IT platform is just that – a platform
  - IT equipment should have no inherent value above the purchase price
- All value is in the data and information
  - This is the organisation's intellectual property and basis for revenues
- Everything is about the who, what, where and when
  - Nothing else really matters
- Enforcing security around the data and information makes compliance, audit and governance easier – across the whole of the value chain