

# Handling Data - in the Wake of Public Outcry

Written by: **Sanjay Mehta, Senior Technical Architect**

MAKING ORACLE WORK FOR YOU

T 0870 11 22 000  
F 0870 11 22 001  
[www.teamsolve.co.uk](http://www.teamsolve.co.uk)

**ORACLE** CERTIFIED ADVANTAGE  
PARTNER

  
teamsolve

## Contents

<b>1 - Background</b> .....	<b>3</b>
<b>2 - Introduction</b> .....	<b>3</b>
<b>3 - Measures You Can Take</b> .....	<b>4</b>
<b>3.1 - Define Your Requirements</b> .....	<b>4</b>
<b>3.2 - Think Before Putting Sensitive Data on Transferable Media</b> .....	<b>4</b>
<b>3.3 - Combine Hardware and Software Measures</b> .....	<b>5</b>
<b>3.4 - Encryption</b> .....	<b>6</b>
<b>3.5 - Network Management</b> .....	<b>6</b>
<b>4 - Get Senior Level Commitment</b> .....	<b>7</b>
<b>5 - Network Analysis</b> .....	<b>7</b>
<b>6 - Minimise Your Risk</b> .....	<b>8</b>

### 1. Background

Security and data protection within the public sector is in the spotlight like never before.

Between the 20th of November 2007 and the 17th of December 2007 4 massive data protection lapses hit the headlines – affecting millions of people across the UK.

Further to this, Information Commissioner Richard Thomas has explicitly said that several other organisations have come forward on a confessional basis in the light of these developments.

The general public found it almost impossible to swallow, but it has served as a rude awakening for all public sector organisations – not only those serving central government.

In all the above cases, the finger of blame has been pointed at inadequate or none-existent processes for the transfer of sensitive data.

### 2. Introduction

It's worth noting at this early stage that there is no such thing as 100% secure. NASA and the Pentagon, with their almost infinite levels of resource, have both been subjected to high profile security breaches over the past 12 months.

What Public Sector organisations need to ensure is that they have the best possible Security Strategy in place, with “buy-in” from all levels of seniority including, crucially, budget holders.

There's no single part of a security strategy that supersedes another. Equal importance needs to be placed on all the tools, procedures and auditing checkpoints to ensure you're doing everything that's reasonably practicable to protect your data.

How can you ensure that you minimise the risk to your organisation, whilst maintaining your auditing and compliance requirements?

### 3. Measures You Can Take

#### 3.1 - Define Your Requirements

Before you start looking at what process improvements you may wish to make, it's essential to clearly define your business requirements;

- What data are you trying to protect?
- Who are you trying to protect it from? (internal/external/combination)
- What is the level of sensitivity?
- What legislative framework are you bound by?

Once this fundamental foundation has been established, you can then start looking at more specific tools, policies and procedures.

#### 3.2 - Think Before Putting Sensitive Data on Transferable Media

Before you start looking at what process improvements you may wish to make, it's essential to clearly define your business requirements;

- What data are you trying to protect?
- Who are you trying to protect it from? (internal/external/combination)
- What is the level of sensitivity?
- What legislative framework are you bound by?

Once this fundamental foundation has been established, you can then start looking at more specific tools, policies and procedures.

### 3.3 - Combine Hardware and Software Measures

Protecting your data from internal abuse can often be controlled by looking at your hardware. Do all your End Users need CD burners and active USB ports? By eliminating the means to accommodate transferable media it can help prevent internal security breaches, or non-conformity to data protection procedures.

There's a variety of Oracle software available that can help protect your data and minimise data protection risk.

- **Oracle Database Vault** – allows for the creation and control of DBA guards. Providing an auditable trail, it has the ability to restrict which subsets or columns of data are accessible to your DBAs (financial data etc). You enable a control measure, so that if DBAs try to access unauthorised data - notification is automatically escalated to a designated security officer.
- **Oracle Identity Management Suite** is a powerful suite of applications that provide a centralised administration point for access controls. Extremely useful during “hiring and firing”, as well as providing automation for many of the day-to-day network administration tasks – it also provides a safe, efficient way to deal with the IT security implications of managing an employee from “cradle to grave”.
- **Oracle Label Security** is Oracle's most recent entry in to the security and data management space. A must for organisations in the Public Sector, it adds robust protection for information across all levels of sensitivity. It provides the intricate ability to secure data right down to individual rows in tables – such as Finance Assistants having access to 3 columns, Financial Controllers 5 columns etc. Only available for Oracle 11g Enterprise Edition, this unique bit of software addresses many of the internal and external data management threats faced in today's public-funded businesses.

**An integrated approach to planning and deploying these software options is the best way to provide maximum security.**

## Handling Data - Public Sector

### 3.4 - Encryption

Encryption of the entire database, or sensitive subsets of data can be achieved through programs such as Oracle Secure Backup. If a portion of data has to be securely transferred from one location to another, use a secure server based FTP (File Transfer Protocol) with an encryption algorithm. This will mean that the subset of data will be completely inaccessible without attachment to the rest of the database.

### 3.5 - Network Management

Encryption of the entire database, or sensitive subsets of data can be achieved through programs such as Oracle Secure Backup. If a portion of data has to be securely transferred from one location to another, use a secure server based FTP (File Transfer Protocol) with an encryption algorithm. This will mean that the subset of data will be completely inaccessible without attachment to the rest of the database.

### 4. Get Senior Level Commitment

A plethora of data management products are already on the market, and with increased importance and legislation surrounding security, the number will only continue to rise. As detailed above, there are a significant number of tools available at your disposal, but each one has a cost and resource implication that is fundamental to success. The technology exists, but it requires “buy-in” from a senior level to carry it forward and establish it as business-critical performance. How many Public Sector organisations can proudly admit to having a full time, dedicated Data Security Officer?

### 5. Regulation, Regulation, Regulation

Not all public-funded businesses are bound by dizzying levels of legal regulation – so budgets are distributed elsewhere.

Every organisation in the world wants to minimise their costs - so what do they do? Outsource. Outsourcing to UK based organisations can be a great way to offset your costs and bring in a safe pair of hands to manage your data. In the UK, organisations are bound by a robust Data Protection framework.

However, some of the most popular outsourcing destinations in the world have little to no legal regulation surrounding data at all. Take the US for example, one of the world’s most developed nations – however it has no comprehensive data protection framework. Developing nations have even less regulation to protect your investment.

That puts UK based organisations at a high risk level – given the fact that you are within the arm of the law and your offshore outsourcing partner is not.

### 6. Minimise Your Risk

The Resource and the Technology exists to keep your data secure and in the right hands. If it's not available internally, then there are specialists such as Teamsolve that can help you.

Teamsolve work with scores of Public Sector clients in the UK. From Small Universities, to large County Councils we have the experience and skills base to provide a secure framework in which to manage and transfer you data. Contact us today to find out what we can do for you. Call 0870 11 22 000, or email [info@teamsolve.co.uk](mailto:info@teamsolve.co.uk).

We have offices in both Derby and London and have clients all over the UK and world. Contact us today for more tailored information on how Teamsolve can improve your business productivity, streamline your IT procedures and boost your service levels.

**Copyright © Teamsolve 2008**

All Trademarks are hereby acknowledged

MAKING ORACLE WORK FOR YOU

T 0870 11 22 000  
F 0870 11 22 001  
[www.teamsolve.co.uk](http://www.teamsolve.co.uk)

**ORACLE** CERTIFIED ADVANTAGE  
PARTNER

  
teamsolve