

Five Steps to Security

MAKING ORACLE WORK FOR YOU

T 0870 11 22 000
F 0870 11 22 001
www.teamsolve.co.uk

ORACLE CERTIFIED ADVANTAGE
PARTNER


teamsolve

Five Steps to Security

Contents

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

Five Steps to Security

1. Background

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

Over the last couple of years a number of massive data protection lapses hit the headlines – affecting millions of people across the UK.

Further to this, Information Commissioner Richard Thomas stated that several other organisations came forward on a confessional basis in light of these developments.

The general public found it almost impossible to swallow, but it has served as a rude awakening for organisations operating across all industries – not only those serving Central Government.

In all the above cases, the finger of blame has been pointed at inadequate or non-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 last two years.

What all 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 and front line staff alike.

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?

Five Steps to Security

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

Over the last couple of years, too many organisations have been caught out by transferring sensitive data by hand – via transferable media. CD's, Flash Drives, USB pens etc. The moment the data leaves the relative protection of the data centre, you're opening Pandora's Box.

Even with an advanced level of encryption, it could take as little as a few minutes to a few days for a hacker to decrypt the data in to a useable format.

By designing and building systems that provide access controls to those that need it – at a sufficient level - you can remove the need to use these transfer methods. These controls need to be backed up by robust policies and procedures that are strictly monitored, enforced and educated.

Five Steps to Security

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.

Alongside the hardware, 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** are Oracle's most recent entries into the security and data management space. It should be high on the list of security considerations for many organisations as 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 businesses.

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

Five Steps to Security

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

For the most sensitive database, it may be beneficial for your organisation to look at tightening Application Security. It's possible to enforce IP level allowances, meaning that a username and password is not enough to grant access – it must be coupled with the correct IP address.

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 strategic “buy-in” from a senior level to champion security issues, establish it of business-critical performance and instil it as a culture throughout the organisation.

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, the picture is not quite so ‘secure’ elsewhere.

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

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

Five Steps to Security

6. Minimise Your Risk

The Resource and the Technology does exist 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 clients in the UK. From SME's to Enterprise we have the experience and skills base to provide a secure framework in which to manage and transfer your data.

Contact us today to find out how we can help your organisation to keep its data secure and available to the only the right people:

T: 0870 11 22 000

F: 0870 11 22 001

E: info@teamsolve.co.uk.

www.teamsolve.co.uk

We have offices in both Derby and London and have clients all over the UK and world. Contact us today for details of how Teamsolve can help you to improve your business productivity, streamline your IT procedures and boost your service levels.

Copyright © Teamsolve 2009

All Trademarks are hereby acknowledged

MAKING ORACLE WORK FOR YOU

T 0870 11 22 000
F 0870 11 22 001
www.teamsolve.co.uk

ORACLE CERTIFIED ADVANTAGE
PARTNER


teamsolve