

Data Security – Data Loss Risk Reduction

Many companies are now completely reliant on the data stored on their network servers, PCs, laptops, and mobile devices. Some of this data is likely to contain either personal information and/or confidential company information.

Here we look at some of the issues to consider when reviewing the security of your computer systems, and how to minimise the risks of data loss.

There have been many high profile incidents of data loss – where large volumes of personal information have found their way into the public domain.

Examples of this sort of information include health records, financial records and employee details.

A commercial organisation also faces the additional risk of data being lost to a competitor.

Obviously, the larger data losses from government and corporations hit the headlines.

However, any company, however large or small can suffer data loss unless sensible precautions are taken.

Whilst there is some data loss from manual/paper records, the most significant losses have been from lost or stolen PCs, Laptops, USB devices, and CD/DVDs.

An increasing risk is also emerging from the latest generation of mobile devices – which can run applications, link to corporate servers and can receive emails with corporate and personal data in the form of attachments.

There are usually two ways in which data can go missing:

- an employee accidentally or deliberately loses or discloses personal information, or
- the data is stolen through physical or electronic penetration.

Audit use and storage of personal data

Just think for a couple of minutes about the kind of potentially sensitive and confidential data which is stored by your business –

- Staff records with date of birth, salary and bank account details, sickness/absence etc
- Customer and Supplier records with bank/credit card account details, pin numbers, passwords, transaction information, discounts and pricing, contracts information
- Financial and performance data and business plans

Confidential data is not always conveniently stored in a 'secure' database. Often employees create spreadsheets and other documents to make their jobs easier, but this is quite often done at the expense of data security.

Find out what is happening to data and what controls are in place to prevent accidental or deliberate loss of this information.

Risk analysis and risk reduction

So the first key question is - If all or some of this data is lost who could be harmed and in what way?

When that is known, then steps to mitigate the risks of data loss must be taken.

So here are some steps which should be undertaken to reduce the risk of data loss –

- take regular backups and store backup data off-site
- review the type of data taken/sent offsite on laptops, mobiles or other media and
- find out how much of this data actually needs to go off-site, and if it does the most appropriate level of data security which should be applied.
- Review the use/availability of USB devices and other writable media such as CD/DVD's within the company and
- think about restricting access to these devices to authorised users only via appropriate security settings and physical controls.
- Ensure that company websites which process online payments have the highest levels of security. This means adopting SSL encrypted transmissions, and also testing for vulnerabilities from XSS (cross site scripting) and CSRF (cross site request forgery) attacks.
- Have a procedure for dealing with sensitive information and its secure disposal once the data is no longer required.
- Train staff on their responsibilities, the data security procedures and what they should do if data goes missing.

Security breach

As well as risk reduction, it is also good practice to have procedures in place in the event a security breach occurs.

This should concentrate on four main areas –

1. A recovery plan and procedures to deal with damage limitation.
2. Recovery review process to assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen again.
3. Notification procedures – this includes not only notifying the individuals who have been, or potentially may be, affected but the breach may be serious enough to have to inform the Information Commissioner (ICO) but only if the breach involves personal data; other regulatory bodies; other third parties such as the police and the banks and the media.
4. Post-breach – ensure that appropriate measures are put in place to prevent a similar occurrence, and update procedures and train staff accordingly.

How we can help

Please contact us if you require help in the following areas:

- performing a security/information audit
- training staff in security principles and procedures

For information of users: This material is published for the information of clients. It provides only an overview of the regulations in force at the date of publication, and no action should be taken without consulting the detailed legislation or seeking professional advice. Therefore no responsibility for loss occasioned by any person acting or refraining from action as a result of the material can be accepted by the authors or the firm.