Data Security - Data Loss Risk Reduction

Nunn Hayward

FACTSHEETS

01753 888211
www.nhllp.com

Many companies are now completely reliant on the data stored on their network servers, PCs, laptops, mobile devices or in the cloud. 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. We have a related factsheet which covers some additional considerations for those with data in the cloud, or use some form of outsourcing.

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 have included 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 departments and corporations have hit the headlines. However, any company, no matter how large or small can suffer data loss unless sensible precautions are taken.

In the past year alone, according to recent research commissioned by the Department for Culture, Media and Sport (DCMS) some 45% of small/micro businesses have experienced some sort of security breach or cyber attack in the 12 months. The small/micro business survey results can be found here

The full report encompassing all company sizes can be found here

Over all sizes of business, the most common types of of breaches were - fraudulent emails (72% of all breaches), viruses and malware (33%), organisational impersonators (27%) and ransomware (17%).

Audit the use and storage of personal data

Consider the potentially sensitive and confidential data which is stored by your business -

- staff records with date of birth, salary and bank account details, medical information 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 need to create and circulate ad hoc reports (using spreadsheets and other documents) which are usually extracts of information stored in a database. This sort of data retrieval is quite often done at the expense of data security - as the database itself invariably will have access controls, but these ad hoc reports usually do not.
- 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 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. Here are some steps which can be undertaken to reduce the risk of data loss -

- Undertake regular backups and store backup data securely off-site
- If high risk data is stored in the cloud understand what security mechanisms are in place and how you can retrieve all of this data if necessary
- Review the type of information which is stored on all devices (including laptops, mobiles, tablets etc) which are used off-site. If such information contains personal and/or confidential data

01753 888211
www.nhllp.com

try to minimise or anonymise the data. Ensure that the most appropriate levels of data security and data encryption are applied to this data

- If mobile devices are permitted to use company facilities ensure there is an active Bring your own Device (BYOD) policy in place, and appropriate security controls to restrict the type of data that can be stored on such devices
- Ensure that company websites which process online payments have the highest levels of security. This means adopting SSL encrypted transmissions.
- Review the use/availability of USB, and other writable media such as optical devices within the company and think about restricting access to these devices to authorised users only, via appropriate security settings, data encryption, and physical controls
- Ensure that company websites and networks are tested for vulnerabilities from attacks
- Have a procedure for dealing with sensitive information and its secure disposal once the data is no longer required
- Have a procedure by which any personal/corporate data stored on mobile devices can be wiped
- Train staff on their responsibilities, the data security procedures and what they should do if data goes missing
- Train staff to identify rogue emails, ransomware and malware, and other potential threats, and the procedures which should be followed.

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. If the security breach involves loss of personal data then the Information Commissioner (ICO) should be informed. There may be other regulatory bodies and other third parties such as the police, the banks and the media who may need to be informed
4. Post-breach - ensure that appropriate measures are put in place to prevent a similar occurrence, and update procedures and train or re-train staff accordingly.

Useful resources

National Cyber Security Centre (UK) www.ncsc.gov.uk/guidance

The cyber threat to UK business www.ncsc.gov.uk/cyberthreat

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.