Simmers & Co
Chartered Accountants

[FACTSHEET]

Data Security - Data Loss Risk Reduction

Many companies are now completely reliant on the data stored on their network servers, PCs, laptops, mobile devices or 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 that covers some additional considerations for those with data in the cloud or using 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. These 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 departments and corporations have hit the headlines. However, any company, no matter its size, could suffer a data loss unless sensible precautions are taken.

During 2021 some 39% of UK businesses have experienced some sort of security breach or cyber attack, according to research commissioned by the Department for Culture, Media and Sport (DCMS). The report can be found at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022.

Audit the use and storage of personal data

Consider the potentially sensitive and confidential data that is stored by your business:

- staff records with date of birth, medical information, salary and bank account details etc
- customer and supplier records with bank/credit card account details, pin numbers, passwords, transaction information, contract information, discounts and pricing
- 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) that 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 which controls are in place to prevent accidental or deliberate loss of this information.

Risk analysis and risk reduction

The key question is - if all or some of this data is lost who could be harmed and how?

Once that question has been answered, steps to mitigate the risks of data loss must be taken. Here are some steps that should 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 that is stored on all devices (including laptops, mobiles, tablets etc) that are used off-site. If such information contains personal and/or confidential data, 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. In addition, implement appropriate security controls to restrict the type of data that can be stored on such devices
- ensure that company websites that process online payments have the highest levels of security available such as using the latest versions of SSL for data transmission. If you are not passing the process of payments to a payment gateway service, and will be storing any credit card information, either on disk or in memory on your own servers, you will need to comply with the Payment Card Industry Data Security Standard (PCI DSS)

- 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 and consider hiring penetration testing firms to conduct these tests on your behalf
- have a procedure for dealing with sensitive information and its secure disposal once the data is no longer required, this should also include the disposal of print outs
- have a procedure by which any personal/corporate data stored on mobile devices can be deleted or access removed
- train staff on their responsibilities, the company's data security procedures, and what they should do if data goes missing
- train staff to identify rogue emails, ransomware, malware, and other potential threats as well as the procedures that 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 need to be informed
4. post-breach - ensure that appropriate measures are put in place to prevent a similar occurrence, 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.

Simmers and Co Chartered Accountants and Registered Auditors
Albany Chambers, Albany Street, Oban, Argyll PA34 4AL

Phone: 01631 562169 | Fax: 01631 565959 | Email: mail@simmers.co.uk

www.simmers.co.uk

Partners: David A McGregor | Jacqueline M Hoey