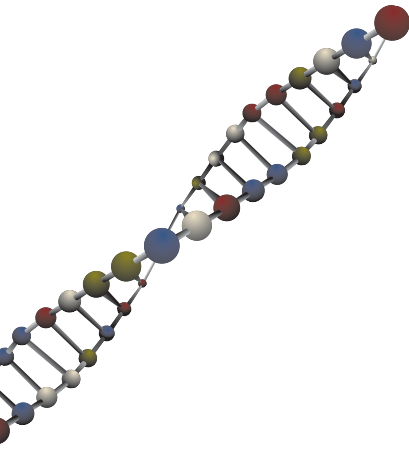


Information security breaches survey 2004

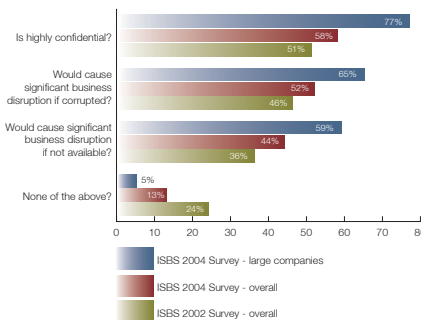


Backups and recovery

Increasing dependence on data

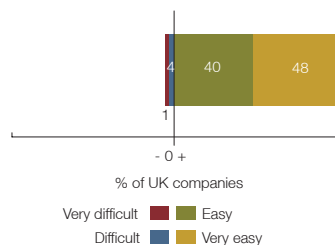
Information is widely regarded as the life-blood of modern business. This survey shows that UK companies continue to be increasingly reliant on the confidentiality, availability and integrity of their data. As you might expect, government, health and financial services companies are most concerned with confidentiality, while the agriculture and manufacturing sectors are least concerned. Availability appears to be a fairly consistent issue for all sectors.

What proportion of UK businesses have electronic data that:



Given this reliance on data, it is unsurprising that UK businesses are prepared to spend money to protect this information. A massive 88% reported that they find it easy or very easy to justify the cost of backups and disaster recovery facilities.

How easy do you find it to build a business case for expenditure on backups and disaster recovery?

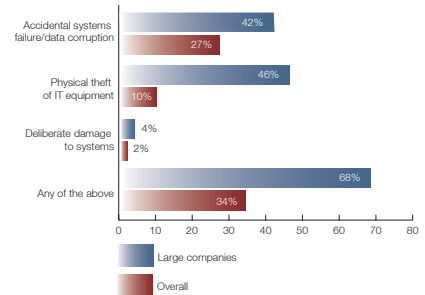


As a result, 95% of companies have some form of backup or disaster recovery facilities in place. However, as we will see later, their effectiveness and reliability vary considerably.

Many cases of data corruption or loss

Roughly one third of all UK businesses and two-thirds of large businesses had a security incident that involved loss of data (excluding viruses). A quarter had accidental systems failures, of which more than half (55%) had more than one such incident. Systems failure was most frequent in financial services and technology companies, and occurred least in small retailers.

Frequency of incidents likely to require access to backups



Physical theft of computer equipment was a particular issue for large companies in all sectors. Many of these had experienced several such incidents, some with more than a hundred separate thefts. The loss of data normally outweighed the monetary cost, which was typically a few thousand pounds per breach.

Thankfully, very few companies reported deliberate sabotage of their data or networks by their employees.

14% of companies that had any type of security incident identified systems failure, data corruption or physical theft as their worst incident. Three-quarters said the incident was serious. Some (7%) had significant permanent data loss as a result of the incident. Manufacturing companies had the most incidents.

61% of companies took more than a day to recover from their worst systems failure. These delays inflicted major disruption to business operations in roughly half the cases. Some reported disruptions that lasted a month.

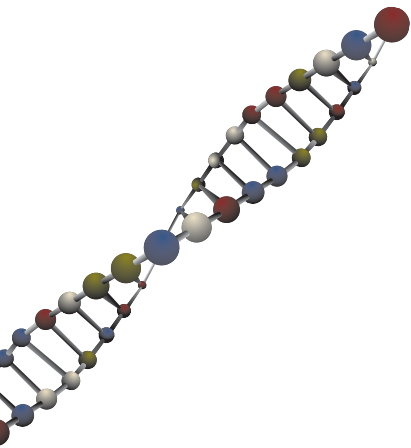
DTI recommends

- Identify what data is critical to your business and where it is stored.
- Make regular backups of this critical data.
- Make sure that you can recover this data in a timely fashion - this is a key step in recovering from most types of information security incident.
- Test your recovery processes regularly.

For more information, please see www.dti.gov.uk/industries/information_security

in association with:





The information security breaches survey has over the last decade formed an integral part of the DTI's programme to help UK businesses address the issue of information security.

The survey takes place every two years and involves telephone interviews with 1,000 businesses of all sizes across all areas of the UK, plus a series of face to face interviews.

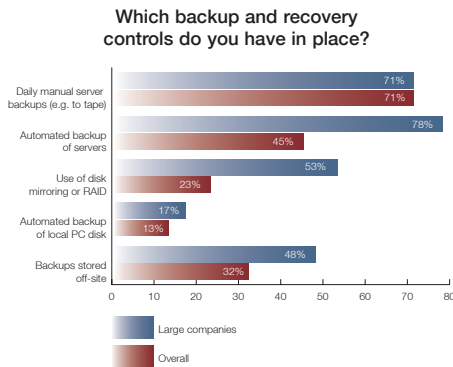
Based on the total sample of UK businesses in this survey, we are 95% confident that the margin of error for our sampling procedure and its results is no more than +/- 3%.

For more information, please refer to the Information Security Breaches Survey Technical Report (URN 04/617). This is available from 27 April 2004 and can be downloaded from www.security-survey.gov.uk



Backup processes vary

Given the increasing reliance on data, one might assume that businesses have comprehensive processes to perform and test their data backups on a regular basis. In practice, these vary a lot.



Businesses continue to rely heavily on tape storage for their backups, despite the well-known reliability issues of tapes.

A large UK financial institution had to recover from backups after the failure of a core business system. However, due to slow tape drives, the backups had been scheduled to kick off each day before processing was complete. As a result, the backups were useless.

Worryingly, only a third of businesses store their backups off-site (rising to half of large companies). Companies that have suffered computer thefts have also often lost their backups because they were stored next to the computers that were stolen.

An increasing trend is the use of automated backups, with 45% of UK businesses reporting some use of automated server backups, and 13% having an automated backup process for their local desktop PCs. While these percentages are higher than ever before, when was the last time your laptop or desktop PC was backed up?

What are the barriers to businesses taking effective backups? After all, the cost of storage media (e.g. tapes and discs) has dropped sharply over the past decade. Many businesses do not realise the value of their data until it is too late. Others think that they have good backups, only to find them unreliable when needed.

Responsibility for decision making relating to data backups is often not clearly defined. IT staff are sometimes not aware what data is critical and hence worthy of being backed up. Business staff frequently assume that backups are being made when actually they may not be.

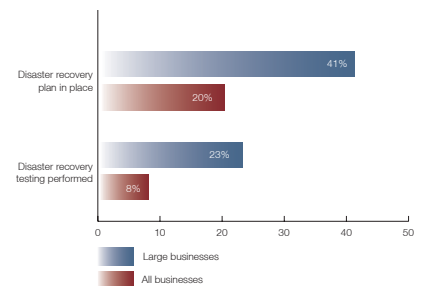
Once bitten, twice shy

Hindsight is a wonderful thing. Only when problems strike do businesses realise the value of their missing data and the cost of trying to recover it, re-create it or do without it. By this stage it is often too late to avoid significant downtime and the associated opportunity cost or embarrassment.

A lot of businesses interviewed reported security breaches which could have been mitigated by effective backups and recovery plans.

23% of respondents reported that better backup and contingency plans would have helped to prevent their worst security incident in the past year, and 15% have now made changes to these processes as a result of this incident.

Are disaster recovery plans in place and testing performed?



20% of companies have a business continuity or disaster recovery plan in place, rising to 41% for large companies. However only 8% have actually tested these recovery plans to give comfort that they would actually work in practice.

This report is printed on Mega Matt paper which is made from 50% recycled and 50% chlorine-free pulp from countries that operate strict reforestation policies.

Department of Trade and Industry. April 2004. URN 04/610

ATTIX⁵

Attix5 is a leading provider of automated online data backup and recovery solutions to blue-chip companies and SMEs across industry. Attix5 technology offers clients highly secure and fail-safe protection against loss of critical business information while reducing cost and risk normally associated with legacy backup solutions. Attix5 Backup Professional is a fully automated solution which can backup data wherever it resides.

To find how Attix5 can help you improve the speed, reliability and control of your data backup and recovery processes please visit our website at www.attix5.com