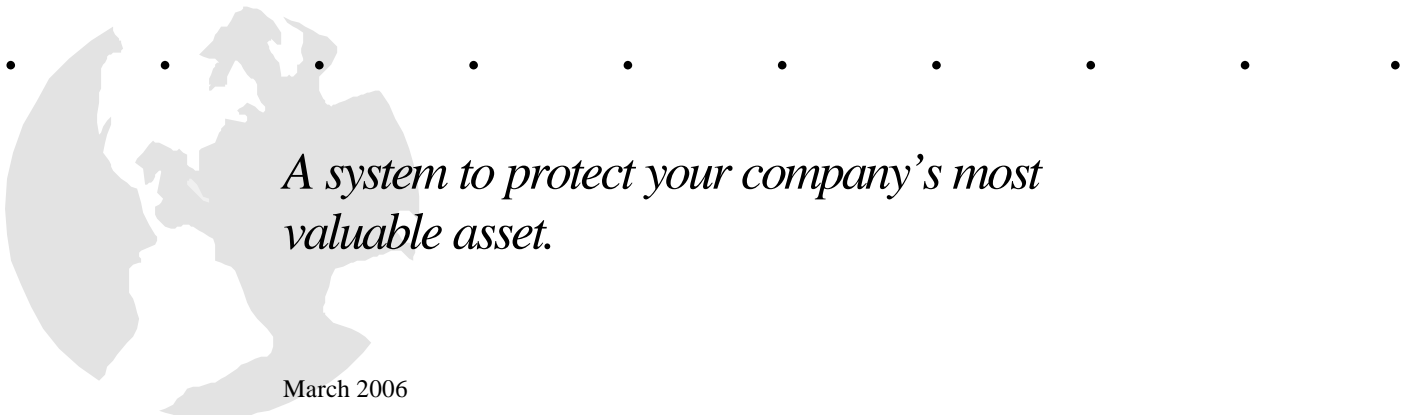




Datatrieve Ltd
(T) 0845 838 6027
(F) 0871 251 5447
www.datatrieve.co.uk
sales@datatrieve.co.uk

Datatrieve Ltd

Online data backup



A system to protect your company's most valuable asset.

March 2006



Introduction

About this document

The aim of this document is to introduce you to the online data backup system supplied by Datatrieve Ltd, and to highlight the benefits in terms of both simplicity and cost of using an online backup system compared to a more traditional backup system.

We also want this document to prompt you into considering the robustness of your existing backup systems, and whether or not they can be guaranteed to protect your data should disaster strike. Businesses also need to consider their legal requirements in terms of data protection and contingency planning.

About Datatrieve Ltd

Datatrieve Ltd is a UK-based provider of secure online data backup and retrieval services. By subscribing to our services you will protect your valuable data through the regular backup of files to our remote server facilities.

The company was incorporated in 2003 by its founder, Dr Neil Peacock, and is based in Colchester, Essex. Our system has been developed almost entirely in-house, and has been thoroughly tested over the course of the last 2 years to ensure that the final product delivers a safe and reliable alternative to more traditional backup systems.

Our online backup system is currently being supplied through a nationwide reseller network, including a major ISP. It is also available for purchase directly from Datatrieve.

Data security

Security risks

The DTI Information Security Breaches Survey¹ published in 2004 revealed that 87% of UK businesses are now highly dependent on electronic information, compared with 76% in 2002. The survey also revealed the following startling facts:

- The average UK business now receives roughly twenty viruses a year.
- Large businesses are attacked more, receiving on average one virus per week.
- Two-thirds of UK businesses had a premeditated or malicious incident: one quarter had a significant incident involving accidental systems failure or data corruption.
- The average UK business now has roughly one security breach per month.
- Virus infection and inappropriate usage of systems by staff were the cause of most of the incidents. Viruses also caused the greatest number of serious incidents.
- The average cost of an organisation's most serious security incident was roughly £10,000, rising to £120,000 for large companies.

Security policy and legislative requirements

The root cause of most security breaches is human error, and so it is more crucial than ever for organisations to adopt a security policy to make staff aware of the risks and their responsibilities when dealing with IT systems and data. Only a third of UK businesses have such a policy in place.

Certain industries, such as the financial services sector, also have a regulatory requirement to protect their clients' data. The fact that three-quarters of financial services companies have a security policy in place reflects this.

However, the vast majority of businesses across all sectors are subject to the requirements of the Data Protection Act 1998 when dealing with sensitive and

¹ Department of Trade and Industry and PricewaterhouseCoopers, April 2004, URN 04/617.

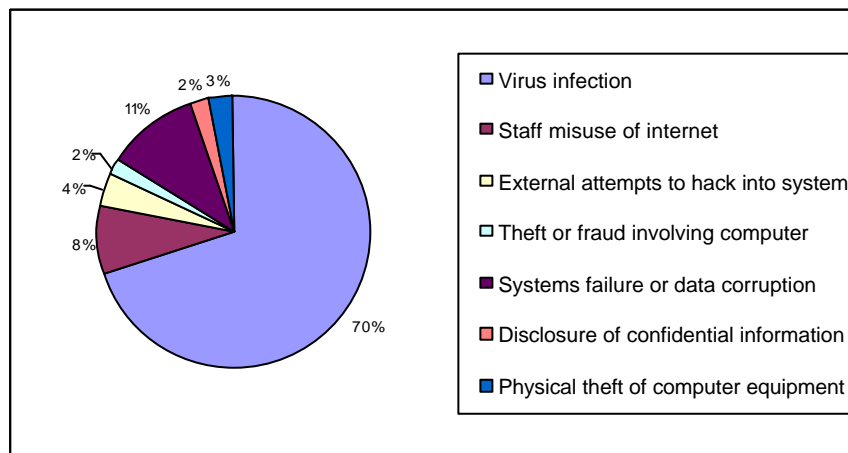
personal data. In spite of this, only 44% of businesses actually have documented procedures in place to ensure their compliance with the provisions of this Act. Principle 7 of the Act requires businesses to keep personal data secure – this means protecting it from unauthorised access, as well as safeguarding it from systems failure.

The British Standard for Information Security Management, BS 7799 has been published for a number of years now, but only a very small proportion of companies are aware of its contents, let alone having actually adopted it. Those businesses that have adopted BS 7799 have found that it had generated real benefits, in particular minimising damage to their company from security incidents.

Even taking into account the arguments presented so far, too many UK businesses are under-investing in security.

Types of security incident

The chart below shows a breakdown of the worst security incident faced by UK businesses.



Virus infections clearly account for the largest number of security breaches, a pattern which is consistent across all sizes and types of business. Systems failure and data corruption also accounts for a significant number of breaches: the most likely causes of this are hardware failure, software bugs and power supply issues.

Impact of security breaches

Security breaches can impact a business in a number of ways, as highlighted by the DTI survey:

- Business disruption: 25% of incidents reported in the survey resulted in more than a day's disruption. In some cases, disruption was extended to more than a month.
- Incident response costs: 33% of incidents involved significant costs. Some small companies spent more than 50 man-days to address their security breach.
- Direct financial losses: mostly through fines or compensation payments.
- Damage to reputation.
- Loss of data: 5% of businesses surveyed lost significant information permanently as a result of their security incident.

Protecting your data

Enterprise security

We have seen that accidental systems failure or data corruption is a significant threat to the availability and integrity of a company's data, with potentially grave consequences for businesses that are ill-prepared. However, the DTI survey revealed that 95% of businesses do have some form of backup process in place. Unfortunately, in many cases these processes are grossly inadequate.

Historically, businesses have tended to backup their data using tape storage devices which have well-known reliability issues. Even then, only 33% of businesses store their backups off-site, often leaving them prone to the same fate as the computers whose data they were protecting.

Of course, data backup should form part of a larger security policy. Significantly, only 20% of companies have a disaster recovery plan in place and of those only 8% have actually tested that their plans would work in the event of a disaster.

Requirements for a backup policy

The first stage in implementing a backup policy is to identify what data is critical to your business, and where it is stored. This data could be stored on a central server for example, or spread across many computers in an office network. Increasingly, it is found that critical data is being stored on employees' laptops. Laptop security is becoming a real concern to businesses, with over 72,000 laptops being stolen each year in the UK.

Once the critical data has been identified, a backup policy should cover the following points:

- To make sure that regular backups are made of this critical data: the regularity could range from real-time replication of data to daily backups.
- To make sure that data can be recovered in a timely fashion: for example can the tapes storing the data be made available within a suitable timeframe?
- To ensure that the recovery processes are regularly tested.

An online solution

Introducing online data backup

The vast majority of businesses that do backup their data use some form of tape-based system, e.g. DAT or DLT. Smaller companies and SOHOs are increasingly using CD or DVD systems, or portable hard disk devices onto which copies of their critical data are made. Each of these solutions has its limitations, but all have the following in common:

- They require significant manual intervention and monitoring.
- Arrangements must be made to store media or portable devices offsite.
- They offer limited security in the form of data encryption and compression.

Secure online data backup is becoming an increasingly popular solution for both businesses wishing to protect their critical data, and home users wanting to protect valuable documents and digital photos. Datatrieve Ltd is a provider of such a service. Compared with traditional backup systems, our system provides you with a number of benefits:

- Data is immediately transferred offsite to 2 UK locations.
- Your data is available from anywhere in the world 24/7; files can be shared between staff at different offices or staff who are travelling.
- Straightforward backup of multiple desktops, servers or laptops.
- No expensive hardware or software licences to buy and maintain.
- Minimal staff intervention is required.
- No limit to the amount of storage available to you: the solution is totally scalable.
- Integrity of stored data is guaranteed.

We believe that our system offers a more robust and cost-effective solution to traditional backup systems. When considering the true cost to your business of alternative systems, you need to factor in the cost of media, staff time,



hardware, hardware maintenance and replacement, software licences and the provision of offsite storage for your media.

The Datatrieve system

Introduction

Our system is simple to install and use, making light of data backup and retrieval for systems of any size, from a collection of servers to a single laptop. It includes the following features:

- Simple web-based installation mechanism and wizard to guide you through the set-up process.
- Fully flexible local file and directory selection mechanism.
- Can be used to backup network drives and UNC locations.
- Data is compressed prior to transmission to preserve bandwidth.
- All communication with the server is performed over an SSL link.
- Data is stored in compressed and encrypted form at 2 UK locations.
- Data can be accessed online 24/7.
- Real-time monitoring of storage allocation usage.
- Logs written to HTML files and automatically sent to you by email.
- Backup history available from within the software.
- Online help pages.
- Daily scheduling of backups.
- Software runs on Windows, Linux and Mac OS X operating systems.
- Historic versions of files and locally deleted files can be retained.
- Automatic email sent if a backup has been missed.
- Optional mutual authentication using client certificates.
- Open or locked files skipped during backup to prevent errors.



Architecture

We have two sets of servers located at two separate UK locations. Your data is initially uploaded to our main data centre from where it is mirrored to our secondary data centre.

All servers run RAID arrays, providing a level of redundancy in case of hard disk failure on any of the machines. This ensures that your data is securely stored.

Security

Datatrieve takes the security of its clients' data very seriously, and our system has been designed to provide the best possible security for your data from the moment it leaves your computer:

- All servers are protected from unauthorised access from the internet by the best available hardware firewall systems.
- Data is transferred between you and our servers over an SSL link, similar to that used for online banking.
- Mutual authentication using client certificates for the SSL link is available.
- Once on the server, data is stored in encrypted form.
- The mirroring of data between our two sites is carried out over a secure VPN using 3DES encryption.
- Multi-tiered application security implemented in server software.
- Our servers are located in data centres with backup power, climate control, 24 hr CCTV and alarm systems, and 24 hr onsite security personnel.

Cross-platform backup system

Our system can be run under the Windows, Linux or Mac OS X operating systems. On Windows platforms, whether server or client-based, scheduling can be configured either from within the software itself or integrated with the Windows Task Scheduler. Under Linux, scheduling is best performed by configuring cron to run the automated backup.

By coupling the Datatrieve scheduled backup with server-side backup mechanisms integral to the operating system, it is possible to protect data from applications such as MS Exchange and SQL Server.



Data insurance for businesses

The automated nature of our system, coupled with the offsite storage of data and remote access 24/7 gives businesses peace of mind that their data is securely protected.

Datatrieve Ltd is protected by a professional indemnity insurance policy providing cover up to £0.25m.

Summary

Although 95% of UK businesses perform some sort backup, and many are increasingly making use of automated backup systems, we have seen that these processes can be seriously flawed. When was the last time that your laptop, desktop or server was fully backed up?

It is often the case that many businesses do not realise the value of their data until disaster strikes, and those that have been following a backup procedure often find that their backups are unreliable when called upon.

The implementation of a fully automated and secure online data backup system such as that supplied by Datatrieve can go a long way to addressing the issues we have been discussing with regard to more traditional backup system.

Free trial

For a free 15 day trial of our system, with no obligation, please register on our website: <http://www.datatrieve.co.uk>.