Why backup?

Increasing amounts of data to protect
Businesses of all sizes are witnessing an explosion in the volume of data. Whether it is the result of the Internet, e-mail or increasingly heavy and media-rich application software, there is a massive growth in the volume of data all around. Conservative estimates from IDC place data growth at approximately 80% per year. This data is a key asset of any company, and losing this data would cause severe damage.

Data under threat
Even with the most reliable computer hardware and software, there is always the possibility of something going wrong. A study by Ontrack in 2002 showed the following to be the most common causes of data loss:

The cost of data loss
Losing critical data can be a costly business. According to a study by Ontrack in 2002, the cost of recreating just 20MB of data can be expensive and varies by business function:

Sales & Marketing	19 days	$17,000
Accounting	21 days	$19,000
Engineering	42 days	$98,000

However, the full financial impact is likely to be more dramatic. The full picture includes loss of revenue, loss of customers, low productivity, legal action and worse, possibly your entire business. The ability to recover from critical data loss can mean the difference between business survival and closure. According to the National Archives and Records Administration:

Eighty percent of companies without well-conceived data protection and recovery strategies go out of business within two years of a major disaster

Statistics from Boston Computing Analysts in 2003 show that 93% of companies in the US that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster. Moreover, the National Archives and Records Administration reports that 50% of US businesses that found themselves without data management for the same period filed for bankruptcy immediately.

Compliance with Government regulations
Recent world events including acts of terrorism, natural disasters and large-scale company fraud have resulted in a new raft of legislation designed to protect company data from loss or corruption. This legislation includes:
- Sarbanes-Oxley Act,
- Graham-Leach-Bliley Act (GLBA),
- USA Patriot Act,
- Health Insurance Portability and Accountability Act (HIPPA)

- European Union Data Protection Act

Compliance with any or all of this legislation means one thing; organizations are required to store, manage and safeguard a lot more data than they might otherwise feel compelled to on their own. This, in turn, has lead to the need for more storage capacity and more efficient methods of backing up, retrieving and archiving data.

Data Protection for SMBs

Little wonder then that it is predicted that annual world-wide spending on data storage hardware, software and services by SMB companies will undergo phenomenal growth, more than quadrupling by 2006 according to a report by Access Markets International (AMI). The report concludes that worldwide SMB storage spending will grow at a compound annual growth rate of 43% over a 4 year timeframe to 2006.

The key to successful disaster recovery and data protection is regular backup within the structure of a robust disaster recovery plan. This plan should include secure off-site storage and regular testing and evaluation of backup procedures, hardware, software and personnel.