Problem:
The loss of a corporation’s production data can impact the state of operations to the point of crisis. Almost everyone is aware of the more spectacular threats to corporate data: viruses and worms, natural and human-made disasters. Non-malicious, inadvertent user error is an even more common cause of lost data. Whatever the cause of data loss or corruption, a swift, reliable data backup-and-restore operation is your first line of defense against the problem.

Solution:
Restoring files to how they were before disaster (large or small) strikes helps put you back on track for business as usual. Routine backups are a solid business practice, because in an age where data fuels business, you can’t afford to “run on empty” for very long.

Things to Consider:
How and how often you back up data, the systems and media on which you store the back-ups, and how you plan to restore lost data all depend on your specific business needs.

- Consider the type of data and its value to your business.
- Scope the impact of data loss or temporary unavailability to this data by core business functions.
- Consider data volume and anticipated increases in data volume.
- Understand how much the data changes over time.
- Some organizations back up all their data weekly and perform incremental backups of the changed data nightly.
- Organizations with a need for up-to-the-minute data do real-time backups.
- For some applications, it makes sense to back up onto tape and conduct restores manually.
- Critical applications might back up onto large-capacity disk, which can enable faster recovery.
- Backups can be done over the network, or they can be done via a SAN, freeing valuable bandwidth on the network.

Within an organization, the various types of data and needs for data availability may require more than one type of backup. Sometimes, stopgap or local solutions have been put into place, leading to inefficiencies and unnecessary costs. For maximum cost effectiveness, companies should seek to design and implement an integrated backup and recovery strategy that matches the backup procedures, systems, and media to both IT operational and business needs.

Why Dell:
Dell’s approach to backup takes into account your business needs, the value of your data, and your existing infrastructure. We can help you build consolidated backup and recovery solutions that can save not only your data, but your time and money as well. We consider the amount and type of data to be backed up, and expected data growth; the window of time you have available for backups without impacting daily business; as well as security and regulatory requirements. Whether your goal is to extend an existing infrastructure or build a new one, we can help you envision, architect, validate, build, and deploy a backup and recovery strategy that meets your data availability needs, within the requirements of your operations and budget. Through training, certification, and support services we can help you keep your new backup and recovery systems operating smoothly. Dell’s storage portfolio includes Storage Area Network (SAN) and Network Attached Storage (NAS) products, tape, and emerging technologies like disk-based backup. Our expertise in the full range of backup solutions lets us match data protection technology to your specific needs, for scalability, simplicity, manageability, reliability, and cost-effectiveness.

Customer Testimonial
“We needed to simplify our back-up processes and make operational cost savings. Standardizing our infrastructure and working with Dell have ensured that we’re in a strong position for the future with an IT environment on which we can depend.”
Patrick Bygraves, IT technical support manager Bedfordshire Police October 2005

Sources of Data Loss or Downtime

- Human Error 26%
- Software Corruption 9%
- Computer Viruses 4%
- System/Hardware Malfunction 56%
- Natural Disasters 2%
- Other 3%

Source: Ontrack Data Recovery
www.ontrack.co.uk/understandingdataloss