



1. Overview

Before beginning a discussion of backup and recovery, let's look at why we go to the trouble of making backups.

Why Do We Make Backups?

System administrators must perform many tasks, including installing, configuring, and maintaining system hardware and software, adding and deleting users, monitoring disk and CPU utilization, tuning for performance, educating users, ensuring security—and making backups. The job of creating backups is often given to the most junior administrator, because it can be very repetitive and not very glamorous. Backups also consume valuable time and resources. Why suffer through all of that work?

For one thing, it doesn't take long in the IT world for things to break. Hardware fails, software becomes corrupted or has bugs, and users make mistakes. There's an old saying, "There are two kinds of motorcycle owners: those who have fallen and those who will fall." The same applies to system administrators: There are those who have lost data and those who will lose data. Preparing for "normal" failure is one good justification for backup.

What about a disaster, such as a tornado, flood, hurricane, earthquake, or fire? Next time you're in your computer room, look at the ceiling. Does it have sprinklers? What will happen to your machines when the sprinklers go off? Are you storing your backups in the same room? What will happen to those tapes? What is your recourse when the air conditioning fails on a weekend, server performance slowly degrades, and disks or equipment fail?

As disastrous as the events of 9/11/2001 were, they reminded those of us in the computer business that we also have to prepare for *man-made* disasters. The number of hackers and crackers trying to get to your data has been increasing steadily. Other dangers include acts by malicious ex-employees and really egregious user mistakes (e.g., `rm -rf *`, or `DEL /F /Q C:*.*`).

Administrators may also face external requirements for record retention, such as a state or federal agency that requires you to keep documents of a certain type for n years.

It is your job to be able to recover from any type of problem and return your systems to full functionality. Just as we all carry insurance for our houses, health, cars, and life, we should make sure we've done what we need to do to be able to recover our sys-

2 / Overview

tems in time of disaster. This, of course, requires a disaster recovery plan. One of the essential pieces of a disaster recovery plan is a solid, well-tested backup and recovery system. The remainder of this booklet focuses on creating such a system.