



March 7, 2008

Backing Up Your Data - The Key To Safe Computing

Sean Sweeney

Here's a data loss-prevention exercise that any organization can run immediately at little or no cost except, perhaps, to some egos. Simply ask for some critical data to be restored from backup. Accept no excuses. If the exercise is successful, great. But the chances are very good that it won't be. In fact, there are long-time IT consultants who have often asked but never seen data successfully restored from backup.

Organizations underestimate the length and fragility of the backup chain. First off, the data has to exist in a form that can be backed up. The backup hardware and software must be functioning correctly, and the media must actually capture the information. Somebody must cause the backup to be performed and the backed-up data must be, ideally, properly documented and moved to an off-site location. Finally, the data must be restored in a timely manner, so everybody can get back to work.

The list of things that can go wrong in that chain of events is almost endless. Ironically, the biggest enemy of regular, properly executed backups is the reliability and efficiency of today's IT systems. That dependability means that restoring data from backup is rarely necessary. Unfortunately, systems that are seldom used tend to fall into decay and that is where the danger lies.

So, if nobody takes excuses from you, you can't accept excuses from anybody else. If you have the responsibility for keeping systems up, running and productive, plain, old-fashioned fire drills are the only answer.

Copyright 2008 Fortress Data Vaulting. All Rights Reserved.