

# **The Real Problem: Humans in the Loop**

## The Real Problem: Humans in the Loop

Industry analysts report that a whopping 80% of unplanned downtime is caused by people and process issues. Clearly, the real problem is humans in the loop. To achieve reliable results, processes need to be automated wherever practical.

This adage applies strongly to your disaster recovery strategies, as well. Many of the most commonly used methods for backing up and storing critical data rely upon frequent human interaction along the way. Reducing the human factor in your data backup and recovery processes can dramatically increase the reliability of your methods, and thus the security of your valuable data.

One highly effective option is disaster-proof disk technology. A true alternative to tape and online strategies, this technology combines reliable disk-to-disk backup with the added benefit of disaster protection and physical security. As a bonus, disaster-proof disk technology can cost significantly less than tape solutions and eliminate the human-induced risk of transporting the data to an offsite facility. In addition, disaster-proof disk technology won't saturate precious WAN bandwidth and remains a viable recovery strategy even if the office connection is severed.

### Why "the human touch" isn't necessarily a good thing

In many facets of life, "the human touch" is synonymous with superior value or benefit. When it comes to data backup and recovery, however, the human touch is to be avoided as much as possible.

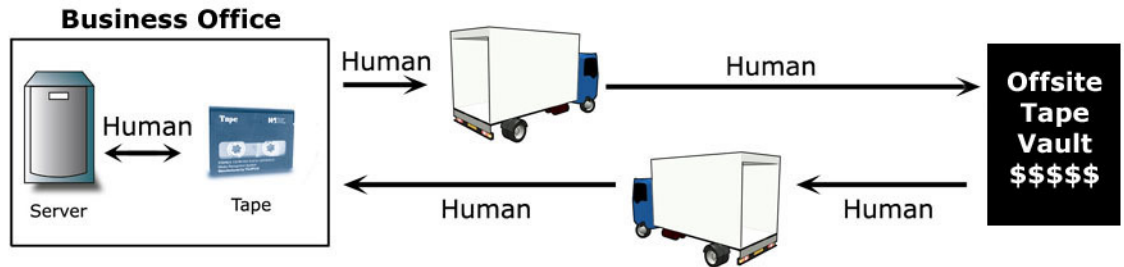
The more you can automate your data backup process – eliminating the need or ability for a person to intervene – the more overall reliability you can achieve.

Consider tape backup as an example. Tape has become common for data backup because it's simple and familiar. Companies can schedule daily (or more frequent) backups of recent data, moving the tapes to a "safe" location and rotating new tapes for the next day's backup.

Unfortunately, this seemingly simple operation is fraught with potential reliability problems, in large part because tape backup depends on human intervention throughout the process.

Relying on humans to perform mundane backup tasks is a mistake

People must install the tapes, initiate the backups, remove the backed-up tapes, load them onto a vehicle, drive the tapes to the off-site storage location, unload the tapes at the storage site, and reverse the entire process everyday.



Millions of personal data records have been lost due to human error.

Each one of these human touch points presents opportunities for mistakes and problems. It's easy to forget to change backup tapes, especially if the person charged with this task is busy with other responsibilities (a common situation in nearly every organization today). Tapes can be damaged in a hot truck environment and become unusable. They can be dropped during transit or misplaced at the offsite facility. They can even be stolen or destroyed by disgruntled employees. Real-world problems such as these are a daily pain point for IT organizations across the country.

Wells Fargo, Citibank, and Bank of America have all had to publicly disclose data loss due to missing tapes. Over the years, the personal information of millions has been compromised due to humans attempting to "protect" critical data by transporting the data offsite. A public relations nightmare for companies, such mistakes are nearly impossible to avoid when relying on the human touch.

### **Tape – A necessary evil?**

With such notoriously unreliable media, it's no surprise that up to half of all tape restorations fail – and you're unlikely to know they've failed until you try to restore data following some kind of disaster. As a result, disk backup continues to become more popular.

**Disk is best for operational disasters such as server failure, file deletion, and virus corruption.**

Disk backups bypass the human interaction required for tape backup and vaulting, and they do not suffer from the bandwidth limitations of online backup methods. Because the backup is onsite, the data stays on your LAN. Of course, everyone knows that reliance on “normal” disk backup can leave crucial data unprotected during disasters that affect the physical location where the disks are located, including fires, floods, earthquakes, or explosions.

Consequently, many companies have chosen disk backup to protect from operational disasters (server failure, virus, etc.) and tape backup for natural disaster. Disk-to-disk-to-tape (D2D2T) strategies improve reliability of recovery from operational issues. Unfortunately, tape is still stubbornly part of the strategy. A human-managed tape solution is still used as the last line of defense against natural disaster, resulting in risky security practices as a side effect.

### **Online backup – Recovery is the problem**

Today’s increasing data storage requirements might demand the capacity and speed of tape or disk. If your business is lucky enough to have so little data that an online backup solution is sufficient, you should consider this approach.

The key to a successful online strategy is not the backup so much as the recovery process.

If your business or branch office is in Omaha and your backup is in California, your data might be somewhat hard to get to when disaster strikes. Recovering individual files is probably easy. Recovering your entire server image might be faster if you FedEx the data back rather than trying to trickle the data across a T1. Moving 500 GB via a 1.5Mb T1 connection might take up to month to retrieve. If backup images are large, online recovery is hardly acceptable for bare metal server restoration.

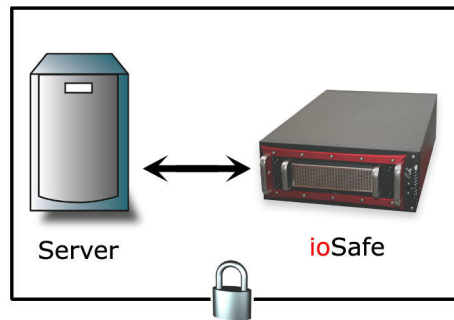
In addition, your particular disaster might involve losing your Internet connection. In cases where this is true, it is important to realize that you have lost not only your ability to recover but also your ability to backup.

**Recovery Time Objective (RTO) is the key when evaluating online backup solutions. How fast can you recover?**

## Disaster-proof disk – an aircraft black box for your business data

An important new approach to data recovery is available: Disaster-proof disk storage is an emerging technology meant to provide simplified server protection and disaster protection in one box.

Disaster-proof hardware technology can provide all the advantages of “normal” disk backup – e.g., reliability, convenience, automation – with the added advantage of an enclosure that is built to survive disasters: fire, flood, vandalism, theft, building collapse, and more. It’s analogous to having an aircraft black box for your digital data.



By automating the data backup process, disk-to-disaster-proof-disk technology can significantly boost the reliability and security of your data recovery following a disaster. It’s easy to see how such a one-step process, combined with a disaster-proof enclosure, eliminates most of the risk caused by human interactions.

Disaster-proof hardware, like any single solution, is not without pitfalls. Humans will still be required to configure the devices. Errors in setting up the LAN might make the data available to the outside world. Errors in executing viable backup jobs can also occur if recovery is not tested.

While the data might not be permanently lost, rare building quarantines might make the data inaccessible temporarily. If during quarantine an Internet connection is still available, the data residing on the disaster-proof hardware could still be reachable via a VPN connection. If the building is truly quarantined, you’ll need to cope with the reality of having your entire office stuck in the parking lot while the building is under lock down. Even if the data were accessible, people might not have desks, phones, or workstations to utilize in a quarantine situation.

**Disaster-proof hardware: like an aircraft black box for your business.**

**Quarantine scenarios involve major business continuity issues no matter what backup strategy.**

**Insurance can replace almost everything except your data assets.**

**94% of businesses that experience catastrophic data loss go out of business. (Univ. of Texas Study)**

## **Final thoughts: Data insurance and the “real problem”**

Realistically, you should implement multiple techniques to protect your data against disaster. For example, you might use disaster-proof storage in conjunction with weekly or monthly tape backup for long-term archival. This is both more reliable and less expensive than daily offsite tape vaulting. Another valuable option is to combine online backup for the most critical data with a disaster-proof solution to achieve point-in-time recovery for your server.

The goal of disaster recovery and business continuity (DR/BC), ultimately, is to minimize business losses. Calculating business loss can be very complicated and is different for every business. The money spent on DR/BC in some ways should be thought of as insurance. Too much or too little insurance can be very bad for your business. Optimizing your protection by spending money where it matters most is the key to minimizing business loss. It’s important to recognize that your data asset is the one asset that insurance can’t replace.

Give your business the best chance of recovering quickly and completely from disasters, whether they’re related to weather or human error, either accidental or malicious. The more you can automate your data backup processes, the more you can eliminate the risks involved in human intervention – and the more likely you’ll be in a position to retrieve and recreate your data, when you need it. An added benefit is that a sound data recovery strategy will help significantly with regulatory compliance, which is becoming an increasing burden on organizations of all types and sizes.

Desks, computers, building, etc. can be replaced. But once the data is lost, it’s lost for good. By automating the process of data backup and recovery with disaster-proof disk technology, you greatly diminish the chances of human error. In addition, your staff is relieved of the burden of spending valuable time checking, logging, and verifying tape backups. The result is lower cost, higher reliability, and better productivity.

Every business can gain by properly applying all technologies to protect your company. You will be in a far better position to recover from disaster by planning in advance – before the fire or the server crash. Proper application of backup technology will maximize profits by allowing humans to get out of the backup loop and let them solve the “real problem” – growing the business.