7 Shortcuts to Losing Your Data

(and Probably Your Job)

UNITRENDS

7 Technology Circle
Suite 100
Columbia, SC 29203

Phone: 866.359.5411
E-Mail: sales@unitrends.com
URL: www.unitrends.com

7 Shortcuts to Losing Your Data (and Probably Your Job)

This tongue in cheek white paper explores data loss from a contrarian point of view - exploring the top 7 shortcuts you can take to ensure that you lose your data. And since a fundamental responsibility of any information technology professional, as well as any C-level executive, is to ensure that the data upon which any company is created is protected - scrupulously following these shortcuts should also ensure that you lose not only your data but your job as well.

What Are the Consequences of Data Loss?

The consequences of data loss are dire; here is a sampling of just a few statistics related to the impact of data loss on business:

- 93% of companies that lost their data center for 10 days or more due to a disaster, filed for bankruptcy within one year of the disaster. 50% of businesses that found themselves without data management for this same time period filed for bankruptcy immediately. (National Archives & Records Administration in Washington)

- 94% of companies suffering from a catastrophic data loss do not survive - 43% never reopen and 51% close within two years. (University of Texas)

- 30% of all businesses that have a major fire go out of business within a year and 70% fail within five years. (Home Office Computing Magazine)

- 77% of those companies who do test their tape backups found back-up failures. (Boston Computing Network, Data Loss Statistics)

- 7 out of 10 small firms that experience a major data loss go out of business within a year. (DTI/Price waterhouse Coopers)

- 96% of all business workstations are not being backed up. (Contingency Planning and Strategic Research Corporation)

- 50% of all tape backups fail to restore. (Gartner)

- 25% of all PC users suffer from data loss each year (Gartner)

2

What Causes Data Loss?

In order to understand shortcuts to losing your data, the first thing we need to do is understand the most common reasons that data is lost.

The primary causes of data loss are:

- Human failure
- Human error
- Software corruption
- Theft
- Computer viruses
- Hardware destruction

The results of the two best studies regarding data loss in the real world are depicted as follows:

Root Cause	**Incident %**
Hardware failure	40%
Human error	29%
Software corruption	13%
Theft	9%
Computer viruses	6%
Hardware destruction	3%

Source: David M. Smith, Ph.D., Pepperdine University

Root Cause	**Customer Perception**	**Actual Incident %**
Hardware or system problem	78%	56%
Human error	11%	26%
Software corruption	7%	9%
Computer viruses	2%	4%
Natural disasters	1%	2%

Source: Kroll OnTrack Data Recovery Services

Each of these together form the foundation for our advice on the most effective path for you to lose your data - the 7 shortcuts that are discussed in the next section.

UNITRENDS

7 Shortcuts to Losing Your Data

In this chapter we're going to explore the 7 shortcuts to losing your data one-by-one. We're going to do so by discussing each of these causes of data loss from the perspective of paths. In each section, we'll first discuss the path associated with the shortcut to losing your data. As illustrated in the picture to the right, this shortcut is designed not only to facilitate your losing your data - but to put you on the fast track for early retirement.

After the shortcut to losing your data is explored, we then describe taking another path - one in which you don't lose your data and don't put your job at risk. This path, depicted at the bottom left of this page, is of course the one we recommend.

Ignore Hardware Failure

Shortcut to Losing Your Data

Hardware failure is the leading cause of data loss; thus ignoring hardware failure is the most important shortcut you can take in order to lose data. You have several choices with respect to taking this shortcut. The most straightforward technique to lose your data is to simply ignore that hardware failure can occur and simply not backup your systems and data. Of course, that's a bit crass - there are more subtle ways to ensure data loss.

Another age-old option to help you lose your data is to use tape as your backup medium. With the high failure rates associated with tape, sooner or later you're assured that you're going to need to recover your data and not be able to do so.

A creative technique to ensure you will eventually lose your data is to use your SAN or NAS storage device as both the source of the backup and the target of a backup. Note that I'm not referring to snapshots in between physical transfers of data off the SAN or NAS; I'm talking about using your SAN and NAS for primary storage and for backup storage exclusively.

Taking Another Path

To protect yourself from hardware failure, you have to move your data from primary storage to a completely separate secondary storage. That secondary storage can be (and should be) less expensive than your primary storage, but it has to have RAS (Reliability, Availability, Serviceability) characteristics that are as good or better than your primary storage. Those requirements rule out tape as well as ruling out partitioned primary storage (SAN or NAS) - although SAN and NAS snapshotting may be used between primary backup protection. The best approach is some type of D2D (Disk-to-Disk) backup. The advantage to D2D backup is that you are using secondary media with higher reliability characteristics than tape while still insuring that you have a physically separate secondary storage set so that you can survive hardware and system failure.

Trust Your Fellow Coworkers to Follow Policy

Shortcut to Losing Your Data

Human error is the second leading cause of data loss. Human error ranges from accidental deletion of files and records to ignoring policies regarding data to rebooting systems without proper shutdown procedures. Blind belief and trust in your fellow coworkers to not only follow policy but to not make any mistakes at all are fundamental to using this shortcut to its fullest potential in losing your data.

Taking Another Path

There are two fundamental reasons for human error: ignorance and arrogance. Attempting to change human nature is the height of arrogance. People have a tendency to be incredibly poor at following policy. Thus specifying that all "important" data will be stored only on centralized corporate servers and storage tends to fail as soon as a C-level executive loses the data on their notebook. But even when people try their best to follow policy, accidents such as file and record deletion will occur.

The best defenses against human error are automation and retention. Automation allows policies and procedures to be created and automatically executed. Retention allows recovery of data even when the data loss isn't noticed for some period of time.

Retention is one of the fundamental differentiations between backup and simple high availability (which is typically achieved with some type of replication) - high availability handles hardware failure well but does a poor job of handling logical failures such as those caused by human error - because logical failure is simply replicated in highly available systems. Of course, protecting against hardware failure using high availability and against all types of failure using backup is a common technique for protecting data and systems.

Previously, we described why D2D is such an important component of protecting your system. When we discuss any type of logical failure, including human error, another important concept is to protect your data using a superset of D2D which is called D2D2x (Disk-to-Disk-to-Any.) D2D2x simply means that you have longer-term strategies for backups to either on-premise rotational archiving media (disk or tape - although tape has the risks we've discussed previously) or to a private or public cloud.

Disregard Software Corruption

Shortcut to Losing Your Data

Software corruption is the third leading cause of data loss. Anyone who has lived through a BSoD

(Blue Screen of Death) in Windows understands the concept. Of course, software corruption is caused not only by software defects but through the chaining of errors in systems as well. It's important to ignore software corruption in order to increase your odds of losing your data.

Taking Another Path

Software corruption, like human error, is another type of logical (as opposed to physical, or hardware) failure. The primary differentiation with respect to data loss is that software corruption can occur and remain undetected for days, weeks, months, or years. Thus automation for strict adherence to policy and retention are incredibly important techniques for protecting your data against software corruption.

Rely Upon the Honesty of Others

Shortcut to Losing Your Data

Theft is a another cause of data loss. Theft manifests itself either via a "data spill" in which data isn't lost but instead made available to third-parties for whom the data wasn't intended or in outright destruction. For the purposes of this paper, we're going to limit our discussion to outright destruction of data.

The destruction of data is rarely performed by a relatively disinterested "hacker"; instead, it is most often performed by a disgruntled employee or ex-employee. It is incredibly difficult to prevent; although precautions should be and most often are taken particularly around the involuntary termination of employees.

Taking Another Path

The first step to avoid malicious destruction is to create policies which make your primary data more difficult to destroy. These include strict policies and procedures associated with not only involuntary but voluntary termination as well and on taking steps to secure your environment from external access.

From the perspective of data protection, theft is largely indistinguishable from human error in terms of the tools and techniques that must be used to protect your data - the only difference between the two is motive and motive isn't really a factor in terms of this type of logical failure. Automation and retention again are the most important strategies for ensuring that you can survive this type of threat.

Pay No Mind to Computer Viruses

Shortcut to Losing Your Data

Computer viruses range from the annoying to those that threaten not only the systems of your organization but your organization's reputation as well. The easiest way to lose your data with respect to computer viruses is to not install a firewall and anti-virus software. In addition, make sure that all of your systems operate using Windows - not just your PCs but your servers and your backup servers as well. That way you insure 100% infection when a virus occurs.

Taking Another Path

In order to protect your data you will of course have a firewall and install anti-virus software. From a backup perspective, the important thing here is to operate your backup and disaster recovery software on a non-Windows platform.

Vendors ship their backup software on Windows platforms for one reason - they can make the most money with the least expense because Windows is so ubiquitous. If you take a step back and think about it, however, it just doesn't make sense to run your "protection" software on the same operating system that is relentlessly under attack by malicious people.

Play the Odds on Disasters

Shortcut to Losing Your Data

Disasters are not a leading cause of data loss by any means. From the charts discussed previously, you can see that data loss due to disasters occurs no more than 1% to 3% of the time. In order to take the shortcut to losing your data, you should focus on the relative rarity of disasters and ignore the severe consequences when a disaster strikes.

Taking Another Path

Why don't people walk around outside in thunderstorms? The odds of getting struck by lightning are pretty low. The National Weather Service estimates that the odds in any given year are 1 in 500,000. The reason of course is that the consequences of being struck by lightning are very high. The odds of death are 1 in 10; the odds of disability approach 9 in 10.

The odds of data loss due to a natural disaster are relatively low; however, the consequences are severe. In order to safeguard your data, you need to have a disaster recovery plan for your environment. A major part of that disaster recovery plan is protecting your data. There are two basic schemes for this: tape-based rotational archiving and electronic-based replication of data to an off-premise site.

We advise looking at vendors that support an integrated D2D2x approach whereby you can use disk, tape, or electronic replication concurrently to optimize your overall spending in support of true disaster recovery.

7

Take Recovery for Granted

Shortcut to Losing Your Data

All of the previous shortcuts we've discussed were derived from the tables of statistics depicted previously which illustrated the reasons for data loss. However, this shortcut - concerning losing your data by taking recovery for granted - applies to all of those reasons for data loss. This one is pretty simple - simply assume recovery will work.

Taking Another Path

The picture to the left illustrates the age-old saying concerning what happens when we assume. It is particularly apt when discussing recovery. Don't assume anything!

Regardless of the technology that you use, it's important that you periodically test your recovery. Don't assume because you can write to tape that you can read from that tape. Don't assume because a dashboard shows you a successful backup status that you can recover that backup. Be paranoid and test. And then test again.

About Unitrends

Unitrends offers a family of affordable, all-in-one on-premise backup appliances that support virtual and physical system backup and disaster recovery via disk-based archiving as well as electronic vaulting to private- and public-clouds. Unitrends is customer-obsessed, not technology-obsessed, and is focused on enabling its customers to focus on their business rather than on backup.

For more information, please visit www.unitrends.com or email us at sales@unitrends.com.

7 Technology Circle, Suite 100 Columbia, SC 29203

Phone: 866.359.5411
E-Mail: sales@unitrends.com
URL: www.unitrends.com

UNITRENDS