

Levels of Choice for Implementing a Data and System Protection Plan

This document describes, considering specifics and a big picture view, the main components of a simple, but well designed and implemented System and Data Protection plan. Each specific component of data and system management is evaluated in terms of pros and cons, and associated costs and complexities.

For each component and each level of implementation options will be provided. These options fall mainly along the following divisions:

- Is the system realized manually or automatically?
- Is the system on-line or off-line (i.e does the system require some sort of backup server or secondary computer, or can it be completely realized on a single computer?)?
- Is the system testable or non-testable?
- Is the system free or low-cost, or more expensive?
- Is it implemented through software or hardware, or some combination?

Only divisions that are absolutely resolved for specific components are listed in the general description.

In addition each component will be evaluated for:

- Required technical proficiency and behavioural capacity of person(s) using and/or responsible for maintaining the system
- Complexity to set up, maintain, and scale system
- Reliability
- Dependencies created between Data and System Protection Plan and other systems

1. Basic Data and System Backup achieved through Redundancy

Data Backup and System Fault Tolerance are achieved primarily by copying all data and all system files and configuration information to a separate physical device. By having an independent copy of the entire system and all the data if the primary system fails or data is lost or corrupted on the primary system the secondary system can be quickly implemented to replace the primary system or lost data recovered from the secondary system.

The problem with this sort of very basic system is that if data is lost due to corruption of the primary system it is very likely that this corruption also exists in the secondary system, and therefore in the data. This most basic level of system and data protection only protects against hardware failure. However, as hardware failure is the most likely spontaneous cause of system or data loss in many cases this level of backup and recoverability is sufficient.

We can implement basic data and systems backup at different levels.

Level 1 - Mirroring

This level is implemented transparently with hardware and can, with many current or new PCs, be implemented immediately or with some moderately complex reconfiguration.

Basic Level 1 is: automatic, on-line, and implemented almost entirely in hardware

Basic Level 1 is: potentially complex to set up, but requires very little technical competency to use or manage, requires no specific behavioural changes to use, and has no dependencies with other systems

A second hard drive is set to automatically receive an exact copy of the data on the main drive. This is called mirroring or RAID0. If you do not already have two hard drives and a RAID controller in the computer you wish to protect the purchase of a second hard drive and special disk controller card will be required (\$200 - \$400). To convert a system to use mirroring will take a few hours of work may require a reinstall of the operating system. Once set up this system will work transparently until one or both drives fail or the disks fill up.

This level of recoverability only protects you from the failure of a hard drive, the most likely cause of spontaneous data loss. It can be modified to provide some level of data or system recovery, but if this is a main requirement different strategies need to be implemented.

Pros: protects against most likely cause of data loss, can be very inexpensive, requires very little technical knowledge to use and maintain

Cons: no useful recoverability or protection against theft, fire, malware, viruses, etc., may require additional expense and reinstall of operating system, little to no system protection from software failure, doesn't protect against data loss due to inherent file corruption or intentional or accidental file deletion, reduces the total storage capacity available on your system

Level 2 - Manually Copying Data and/or System Configuration to a second hard drive

Basic Level 2 is: manual, on-line or off-line, and is implemented through hardware and specific learned behaviours

Basic Level 2 is: very simple to set up, inexpensive, relatively easy to maintain but will become difficult to scale if amount and types of data become too complex, depends critically on how well the system and data are organized and maintained and therefore requires the person using the system to take complete ownership of their data and the backup procedures

In the level 2 version of the basic strategy all identified system data, software of value, and client-generated data of value is manually copied to a second internal or external drive, an Internet storage site, another storage device (even an iPod will do) or to another computer on the network.

Note: CDs and DVDs are not recommend for backing up at this level as they degrade with time, have limited storage capacity, are easily lost or broken, and rapidly become a management headache. CD's and DVD's serve mainly for archival purposes or for a second or third level of backup, such as creating offsite backups.

This strategy can be automated with software or operating system tools (advanced level) but if your technology and data world is relatively simple and you are less than comfortable with acquiring the technical understanding required to maintain and trouble-shoot an automated system, whether or not money is spent, it is often simpler and more reliable to simply doing the same thing manually.

The value of learning about your own technology immediately translates into peace of mind concerning the safety of your most valued data and the usability and reliability of your technology.

Pros: cheap and encourages you to know where and what your data is, and how to organize this data, allows you to exploit your network, the Internet, or older PCs proactively, can provide any level of backup including off-site and version control, is very flexible and adaptable to changing needs

Cons: Only as reliable as the person(s) doing the backing up, can become a management nightmare and cause data bloat, may not protect against theft, fire, etc., provides only limited system recoverability unless client has a very high level of understanding of what to back up and when, requires knowing where and what your data and software is in detail, also requires having detailed knowledge of the hardware and software in your systems and how it is configured and accessed.

2. Advanced Data Back Up and System Recoverability

In the advanced approach to data backup and system recoverability (fault tolerance) the process of duplicating data and the system is accomplished mostly automatically. However, the system still needs to be monitored manually and recovery is always a manual process requiring some basic level of understanding of your system and some technical expertise.

Traditionally, large-scale backups are accomplished using dedicated backup servers that copy data to external magnetic tape devices. These systems are highly problematic, expensive, and require a high level of technical expertise and maintenance if they are to work reliably. Additionally, unless a complete data management strategy is in place with sound policies enforced for creating and storing data this type of back up system may continually need to be upgraded to keep up with data bloat. For individuals or small to medium sized organizations or businesses there are simpler systems that can be implemented. However, a key part of any system of this sort is the provision of custom training to all people using, maintaining, or relying on the system to facilitate the acquisition of the knowledge, understanding, and behaviours required to support and use the system.

Level 1 – Combined Recoverability and Backup using external storage devices and Disk Imaging or Backup Applications

The simplest, most versatile, reliable and cost-effective method for directly achieving all aspects of data and systems recoverability and backup is to use a disk imaging tool (software) with a large capacity external drive, possibly in conjunction with a second internal drive, or second computer on the network or Internet (a 'server').

Advanced Level 1 is: half manual and half automatic, on-line or off-line, testable, requires investment of time and money for software and hardware, and is implemented through the use of

hardware and software, with some behavioural change required, specifically complete ownership when backups are run.

Advanced Level 2; requires greater technical ability to implement, but less to maintain and use, can be easily scaled and reconfigured for changing needs but only so far, is very reliable, and allows recovery to be facilitated automatically and relatively simply, even by non-technical users with basic training on use of the system.

Disk imaging is the process of copying all or part of the contents of a hard drive or partition at a very low-level, which makes it fast and simple.

Partitioning (creation partitions) is just a way of creating separate but virtual storage areas on the same physical hard drive. It is essential that you understand the difference between a partition, a hard drive, and what a drive letter represents if you wish to have a reliable system and data protection plan.

A hard drive, or any portable storage device (including i-devices, cell phones, cameras,, USB keys, etc., must be, when it is connected to a computer, represented by a unique drive letter. Most physical storage devices can be configured to have one or more partitions, each requiring a unique drive letter, although for most devices other than internal or external storage devices (true disk drives) this is unlikely. The important point is that we can't assume that different drive letters mean different physical devices, nor can we assume the same devices will always get the same drive letter. In most case all the internal devices get the same drive letters every time the computer boots while external device are assigned the next free letter when they are actually connected.

Imaging works by copying at the level of the actual one and zeroes on your hard drive, the bits and bytes (bits being 1 or 0, bytes being a fixed number of bits, usually 8). This creates a single, very large, but compressed file. This image file can be restored in whole or part, or even browsed by using tools that come with the imaging software.

Imaging a whole partition or drive can take a long time if there is a lot of data so it is best to set up imaging on a clean system where the important data is very well organized, or even better, separated from other extraneous stuff.

Again, if a storage device has been configured with multiple partitions it will show up as more than one drive letter. You can not assume that each drive letter implies a different physical device. This may only indicate more than one partition exists on the same physical device. If you use a different partition on a single drive to back up data you are simply copying the data to a different place on the same storage device. This is not a very useful sort of back up. You must have some comfort level with using your operating system and systems tools to determine how many different physical storage devices are actually connected, internally or externally, to your computer.

At this level one simply runs the imaging tool, or backup application manually whenever the need for a system or data backup presents itself.

Pros: Less maintenance, decision making, and user intervention is required than manual copying of data and system information, many applications can be configured to back up system and application settings and user data, backups and recovery may be simplified through automation, many free applications are available, having access to a database of files backed up makes finding

specific files to be recovered easier, only expense is external storage device, allows old hardware to be re-deployed, takes advantage of free Internet services, provides some protection against fire, theft, data corruption, or malware by having data stored on different physical device, doesn't slow down your system or create dependencies with other automated task such as software or operating systems updates.

Cons: only as reliable as person maintaining the system, data created since last backup is not protected, needs to be tested to ensure it will work when required, more technical understanding is required to back up system than simply copying data manually

Level 2 - Automatic Backup of Data and System to external storage device with imaging tools

The strategy of copying system information and data manually to a different physical storage device can be automated but experience shows that for basic needs and simple systems this sort of approach can be more problematic and liable to fail than needs be, whether or not money is spent, than simply doing it manually.

More completely automated methods need to be used in multi-user environments involving dedicated and shared data servers, if you use more than one computer or device with data storage capacity, if you generate large amounts of data or many different kinds of data, if you want the highest level and most foolproof security for your data due to its value, if you need version or auditing control, and, most importantly if you and the other people using the system value and are willing to learn how to use and manage the system at the level you need it to work.

At this level a disk imaging/backup application is used to image the entire hard drive for system recoverability, a separate system backup image (to supplement the basic recovery image, and one of more daily, weekly, or monthly back ups of the data customized for the type of recoverability required and the complexity of the data.

Advanced Level 2 is: automatic, off-line, testable, requires investment of time and money for software and hardware, and implemented through the use of hardware and software, with some behavioural change required

Advanced Level 2; requires greater technical ability to implement, but less to maintain and use, can be easily scaled and reconfigured for changing needs, is very reliable and provides a high degree of control and sophistication in terms of what gets backed up where, when, and how, and allows recovery to be facilitated automatically and relatively simply, even by non-technical users with basic training on the use of the system. This level does create many potential dependencies with other aspects of your overall system that need to be considered and managed, specifically it is best to have a well designed data management strategy already in place for best results

a) System Recoverability

The simplest and most effective method for providing system protection and recoverability is to take a complete disk image of your computer with a freshly installed and updated operating system with all the applications and peripherals in place, but without any data. This facilitates two essential kinds of recoverability; recoverability initiated due to system hardware or software failure, or recoverability initiated to maximize system performance.

By taking a complete image of a data-free system you can restore a near complete and optimally functioning system without the need to input licence keys, reapply patches and service packs, and will only have to update software that has changed since the last system image was taken. Additionally, if your data is clearly organized restoring the data independently from the system gives us the greatest flexibility and simplifies the restoration process making it more user-friendly and reliable.

If you use your system daily, place great demands on it and need to regularly remove and install applications, or create lots of resource-intensive data your system performance may degrade more quickly. By being able to quickly (2-3 hours) restore a complete working system and data you can keep your system running as smoothly and securely as possible without having to do reinstalls from scratch. In addition, if your system is compromised by a particularly nasty virus or malware it is often simpler and quicker to restore the entire system than to try and repair the damage.

Taking a complete image of a system is also a useful method for recovering data from a damaged hard drive or unbootable operating system.

Starting an operating system rebuild from scratch can take 2-3 days and cost \$75 -\$400 if you have to pay someone else to do it. With a pre-configured image and disk imaging tool recovery takes an hour or so, and doesn't have to cost you a penny more than the imaging tool, storage space, and time. If the system is well designed, documented and maintained even someone not very comfortable with technology can accomplish a complete system and/or data restore.

New complete restore images can be taken periodically, with or without data, after major upgrades or system changes, assuming your systems is still running well. You can keep any number of images as long as you have storage capacity and the energy to manage them. Ideally it is best to keep a basic clean install recovery image and take a new complete image at least every other month.

If these images are complete and include data they also serve as failsafe backups. However, as taking an unlimited number of complete images is not really sustainable this is not how the tool is normally used to back up data.

This sort of recoverability can be automated, involves software and hardware, is testable, can be on-line or off-line, and costs money (\$200 minimum).

It can be implemented on an internal drive or over a network on another computer but the simplest and most flexible method to setup and manage uses an external USB drive. Current USB drives can be purchased with RAID0 (mirroring) built in. This kind of drive is recommended so that your images and backups are themselves automatically duplicated (external drives are more prone to failure because they are portable and tend to get abused). At this point archiving images and data offsite, annually or semi-annually, would give you a system that would allow you to quickly recover from even the most catastrophic and unlikely series of events!

Pros: if you are willing to invest the time, money, and energy into having the system set up and learn how to manage and use it there is nothing better for recoverability and backup. It will save you time, money, and frustration in the long term and give you peace of mind as soon as it is implemented.

Cons: You may have to reinstall windows or clean up your data if your system is not running optimally or is disorganized with large amounts of data (anything over 50 GB can be problematic for imaging for recovery depending on what condition your operating system and data is in).

b) Data Backup and Recoverability

The same tool that is used to back up and restore your system can also be used to back up and restore data. Current disk imaging tools also function as simple but sophisticated back up tools. They can be used to create images that only contain the files or folders you indicate and you can selectively browse for and restore only the data you need, not the whole image.

In addition to basic data recoverability you can use different kinds of backup techniques; full, incremental, or differential, and other features of the software to provide version or auditing control (seeing earlier versions of files that are constantly changing, or confirming times and dates of creation and modification) and provide many windows into the past to allow for many possible scenarios of data recovery. You can also automatically and easily manage back up sets and archiving of data to make the system as seamless as possible.

All that is required is that you check in on the system once a month (this can be automated using email) to ensure that it is functioning normally and that back ups aren't getting too big too fast.

Pros: You will never lose data again, including application data such as bookmarks or contacts, implementing a recovery and back up plan forces you to take ownership of your data, you can simplify your operating system and turn off a whole bunch of resource intensive system tools that slow down your computer and cause bloat, protection from viruses and malware becomes less of a concern and it becomes easier to secure your PC and your sensitive information, recovering from system failure is much easier and cheaper, you won't be beholden to technical experts

Cons: You will have understand at a basic metaphorical level the system and technology in order to use and maintain it, implementing a recovery and back up system forces you to take ownership of your data, you may need to start with a freshly installed operating system, time and money is required to initially create the system (\$200 to \$600)

Every backup and recovery system is a unique creation based on the individual needs of the specific customer and comes with training and customized documentation as required. Only what is sufficient for the requirements of the client and their level of comfort with the technology need be implemented and can be reconfigured by the client themselves as situations evolve.