

Basics of System and Data Management

The first part of this document provides a high level and understandable view of how and why you need a simple, testable, and reliable Backup/Recovery and Data Management Strategy to protect not only your valuable data but also to ensure the uninterrupted, safe, secure, and smooth operation of your system.

Your system is not limited to just your computer and interface-able devices (iPods, cell phones, Xbox's laptops, almost any newish technology). Your system includes all the thought, time, energy, and money that was, and is, put into installing, configuring, and updating the operating system, all your peripherals, your network, your Internet connection, your entertainment system, your communication devices, and all your software. In addition, your system now includes another layer of tools, hardware and software, for tuning and securing your computer from all the well-advertised risks and the unavoidable random software and hardware failures, or acts of God that might befall it.

Yikes!

On average people replace their PCs every 3-4 years and their laptops every 2-3 years. The reality is that for many users who don't need the latest on-line or PC games or run high-end video, sound or graphics editing programs, or other resource intensive programs (if you don't know what they are you don't use them) a well maintained and protected computer can easily last 7 years or more and a laptop 5 years or more with a couple of inexpensive upgrades and all without a severe drop off in performance.

But not the way things are done now!

The problem is simple. If you rely too heavily on others to maintain your system and data for you, or do not understand what you need or don't need to do, or why you do or don't need to do it, then all that ends up happening is that your valuable data and personal information either becomes lost in an ever growing sea of superfluous data, or exposed for everyone to see or steal, and your system quickly becomes compromised in performance and security; primarily by all the junk that was supposed to prevent this from happening in the first place.

This happens mainly because your many service providers feel forced to work at odds with each other, and by not owning any responsibility beyond what they see as the ends of their own involvement, create redundancies and gaps that they aren't aware of, or won't admit to. This problem also exists within businesses between and even within IT departments and often extends outside to their relationships with their customers.

The central belief of most technology vendors is to assume that the customer does not want to, need to, and is not capable of understanding or making truly informed decisions about their technology.

The central belief of many users of technology is to be afraid of, or to feel personally challenged in the use of their technology and to simply adapt a 'make it work, now, and I don't want to know why or how' philosophy.

This gap is made worse by the software and hardware engineering premise that assumes that if you design perfect technology all people will be able to use it intuitively with little or no need to understand the design parameters that were used to create the interface in the first place.

These beliefs are not sustainable and they inevitably lead to behaviours that put vendors and service providers at odds with their customers, thus creating a high probability of recurring system failures and data loss and exposure, and promotes collective behaviours that are wasteful and unsafe.

And no one wants to accept any personal or collective responsibility, and everyone wants to blame someone else.

If you send a 6 year old into a forest with a chain saw whose fault is it if something bad happens?

The computer is the most powerful and sophisticated tool humans have ever devised and we have set it free in the world to be used by both problematic ends of the spectrum. The professional who think he or she knows it all and the customer who doesn't want to, and thinks they can't.

At PIN Marketing and Technology we ask every client to make an agreement before beginning training in which they declare:

- 1. I am willing and recognize the need to take responsibility for my technology use and for the use of technology by any groups or institutions that I serve. I recognize that to do this I must acquire some basic high-level understanding of technology at the level of metaphor (i.e relating what I don't easily understand to what I do).*
- 2. I am willing and recognize the need to abandon some old behaviours and to learn some new ones if I wish to create for myself and the world an environment in which technology is used wisely, safely, and in way that is environmentally sustainable.*
- 3. I am willing and recognize the need to stop focusing on blame and the bottom line and shift the focus to collaborative problem solving and adding value by envisioning at the level of imagination, and not at all at the level of stuff.*

The Three Goals of a System and Data Protection Strategy:

There are three main components to be considered in designing and implementing a system of technology and behaviours to accomplish a reliable, efficient and economically sustainable system for protecting your systems and data. These are:

- 1. Recoverability (Fault Tolerance)** – this is the ability to keep systems up and running up to and including 7-24 operations and facilitating system and data recovery in the event of avoidable or unavoidable events such as theft, unintentional or intentional user error, severe software failure (viruses, hard drive corruption, etc), natural disaster, etc.

Facilitating recovery includes designing and implementing solutions primarily at the level of hardware first and software second to minimize the likelihood of preventable events (proactive) and efficiently recover from events that were unavoidable even given best practices. Recoverability at this level is wholesale for both data and systems. Recoverability can be tailored to specific types of

hardware (i.e. specific brands, makes, models, and operating systems versions) to minimize recovery time and complexity or to facilitate refurbishing a system whose performance has degraded or needs to be kept running as effectively as possible (i.e systems running data or resource intensive programs and technologies need to be rebuilt more frequently

2. Backup – this is the ability to recover from system problems or data loss and to prevent system and data loss, and to a certain extent, to maintain the security of both. There are many levels of backup:

- Wholesale recovery of lost data from fatal or non-fatal systems failure
- Piecemeal recovery of lost data from fatal or non-fatal systems failure
- Version control – the recovering of earlier versions of data
- Forensic recovery – recovering data and/or meta-data for legal or financial requirements
- Archiving – the creation of off-site storage for essential data that would be compromised by theft or disaster and/or to off-load storage and prevent software and data bloat that inevitably grinds systems to a halt

Backup is implemented simultaneously at the level of hardware and software but is managed primarily at the level of software.

3. Data and System Management and Security

It is at this level that issues such as virus and malware protection, social and behavioural vulnerabilities, and operating system, data, and software maintenance are implemented. This level is achieved at the level of software and behaviour and includes acquiring the necessary skills, knowledge and motivation to take charge of adapting our computers and technology to our vision of how things should be done, rather than adapting to the computer or its software defaults.

This includes taking steps to know what data is important to you, where it is, and how to organize it, and is essential if the lower levels are to be cost-effectively implemented and to work, sustainable, and testable. It is not enough to address higher level first. We must begin at the level of our data to have success.

3b) Data Accessibility and Synchronization across Devices or Systems

This is a value added level of System and Data protection that helps with the other levels and is important to consider to eliminate the redundancies inherent in having the same data sets (such as address lists, copies of file, etc) existing in the same or different forms on different computers, websites, or personal devices such as iPods, cell phones, blackberries, etc.

By creating single silos of specific types of data (music files, bookmarks, address books, etc) we can avoid many security and performance problems as well as simplifying our entire data and systems protection plan, and ensuring long term sustainability and a sense of empowerment.

This level of data and system protection includes also includes simple behavioural based strategies for managing the ever-growing list of passwords we are expected to manage.

Completing the following set of questions will help to evaluate and design the least sufficient and most effective and efficient strategy for data and system protection.

1. If your system fails (software and/or hardware) and may take several days to fix, or require the purchase of a new system is this a problem?
2. If your operating system needs to be rebuilt to resolve a software issue or improve performance can you do this yourself or will you have to find someone else to do it (with or without expense)?
3. Do you have data that you would feel really upset about losing, or that would cost you money or hassles if you were to loss it?
4. Do you often have to recreate address lists, bookmarks, documents, etc. or recover music files, movies, or photos from other sources?
5. If you haven't complete the documents, **Questionnaire for Determining Technology Strategies and Training** or **Questionnaire to Help Design a Protection plan** list all the types of data or information on your computer or on any of your technology devices that are either very important to you or would take a great amount of time, expense, or effort to recreate.
6. Do you enjoy redoing things you have already done, but don't need to do again, or would you rather just do these things once and maintain them?
7. Do you want the ability to recover lost, corrupted, or accidentally deleted files or system settings and software?
8. Do you want the ability to recover earlier versions of software, systems or files? If yes, how far back, and how often would you want these changes captured?
9. Do you want or need a system to off-load old data or create backups of data at another location to protect against theft, fire, etc.?
10. Do you understand how to select, maintain, configure and use the tools required to protect your data and systems against malware, viruses, theft, accidents, etc.?
11. Do you have one password for every site, including your on-line banking?
12. Do you understand how to select, maintain, configure, and use the tools required to keep your technology running as smoothly as possible over its life?
13. Do you have duplication of lists or data on different devices? If yes, would it be valuable to have a way to synchronize, centralize, and back up this data.
14. Would it be useful to access your computer, data, or any resources remotely?
15. Would it be useful to share resources or peripherals for more than one device or computer?