



COMPUTER DATA SAFETY - NIGERIA AS A CASE STUDY

By Engr. Samson Ojo Ogunlere
Lecturer at Babcock University, Ilishan-Remo,
Ogun State, Nigeria
Email: ogunlere@yahoo.com

Data safety in a computer environment is often misused or miss-understood and majority of computer users do not have clear cut differences with the following terms:

- Data Security
- Data Integrity
- Data Validity

Their differences can be conceptualised as follows:

Data Safety - This is making sure that data is always intact (always available for use as at when needed) and not deleted or erased.

Data Security - This is making sure that only the people who should have access to the data are the only ones who can access the data and also keeping straight who can read the data and who can write data. This is an assurance that your data is safe from unauthorized access (requires username, password, and cannot be viewed by anonymous users and/or users with incorrect authorisation).

Data Integrity - This is making sure that the data is correct and not corrupt. This is also an assurance that the input is correct (correctly formatted, free from errors). Pure integrity of data refers to the property which determines that data, once stored, has not been altered in an unauthorised way -- either by a person, or by the malfunctioning of software or hardware.

Hardware wise, Cache designs have provisions to eliminate invalid data in system memory caused by write operations. This happens when busmaster devices or processors write data to memory locations which have previously been copied to the cache. All data, wherever located in the system, has to be valid. This is known as **data coherence**.

Also Bus snooping monitors memory accesses made by other busmaster devices. When data in the cache has been changed (dirty bit is set), data must be written back to main memory before the busmaster can access them. If data in the cache has not been changed but the memory location is overwritten, the corresponding cache line will be marked invalid. Note that in systems with multiple processors cache coherency is much more complicated, hence **MESI** (Modified, Exclusive, Shared and Invalid) protocol is designed to handle it.

Data Validity - Data validity has to do with determining if the data itself is valid. The context here plays a critical role. For example, one would not expect a name to contain the characters #, @, or %. It can be said with reasonable safety that such a name is invalid (thus no data validity).

Note that in some instances it is possible for data validity and integrity to fail on the same piece of data. For example, because of a hard disk crash, a person's name may change in such a way that it now contains the character '%'. Thus the integrity and the validity have been compromised.

Data Validity Errors caused due to incorrect data entry are probably the most common data-related errors in a computer environment. These errors are also the most difficult to detect in the system. Data validity errors can be reduced by the use of data validation rules in the data fields. For example the date field in a database uses the DD/MM/YYYY format. A developer can incorporate a data validation rule such that DD does not exceed 31 and MM does not exceed 12. Note that in many cases simple field validation rules are may not detect data validity errors. In such cases, queries can be used to validate data fields. For example a query can be written to compare the sum of the numbers in the database data field with the original sum of numbers from the source. A difference between the figures indicates an error in at least one data element.

Having explained the differences between these often confused, misused/misunderstood computer terms, it is time to focus our attention on the article of this paper which is **computer data safety -Nigeria as a case study**.

To understand this from a computer point of view, the following concepts need to be understood:

- Power supply
- Backup
- Redundancy
- Archiving
- Electrical Storms (Lightning and thunder)
- Fire
- Flooding

Power Supply

It is worth noting that good clean power free from failure/spikes/surges/brownouts or inconsistent frequencies are the first level of defense against data loss. Is this the case in Nigeria? Is the country free from power failure/spikes and surges? Your guess is as good as mine. For this reason alone, computer users in Nigeria will continue to be experiencing data

lost or data insecurity either from constant power failure/spikes/surges and brownouts due to constant power outages, low voltages and over voltages.

Remedies

- i. The use of a stavol- motorized stabilizer or automatic voltage regulator with an on-line UPS (Uninterruptable power supply) is one of the surest ways in protecting data lost against power failure, surges and spikes. *(These types of AVR's have quick speed in dynamic response, low distortion, high adaptation to overload and high resistance to electromagnetic interference. They can properly absorb and control the noises and peak voltage of electrified wire netting).*
- ii. Another way of achieving data safety as a result of power failure or fluctuation is the use of an on-line (automatic) inverter which can be powered on automatically when there is power failure. The advantage of being sychronised with the main helps in eliminating spikes/surges/brownout or transient spikes during change-over which often play significant role during computer system hard disk head seek (during read and write operation).

Generally speaking, the more expensive and higher-wattage the PSU/Generating sets/Inverters/UPS and Stabilizers - the better it is likely to handle systems and be free from spikes/fluctuations/surges and brownout (but not necessarily on failure!). It is advisable to check the voltage/wattage load of the computer systems to that of the PSU efficiency before making a purchase or commitment. The load efficiency should be between 70 and 80% loads capacity of any proposed PSU (PSU or otherwise should be able to holdup efficiently and effectively).

Backup

If there's one important task computer users regularly ignore, it is backing up of data, including important items like office documents, music, videos, and photos etc. Things go wrong sometimes: Computers may get viruses, hard drives may fail, fire, thunder/lightning and flooding may happen (normally refers to as act of GOD - Natural disaster). This happens all over the world but most prevalence in Nigeria due to lack of proper planning, ignorance and computer technology awareness.

Backing up data is a time-delayed replication of data, or should be. If it is instantaneous, it is useless. The entire point of backing up data is so that, if, in any moment, one accidentally deletes a file or develops system corruption, then the data is present elsewhere. If backing up is instantaneous and not time-delayed, then any changes such as a file deletion or otherwise are reflected in the backup, rendering it useless from a data recovery perspective.

The particular time-delay to choose for backing up data varies. Most businesses backup once a day, but for home users once a week is usually sufficient. That way if you lose a project during the week it's always there on another machine. Better backup systems allow multiple time-save-points, so that changes to data can be easily tracked and fixed if required.

One of the biggest reasons people forget backing up is that they don't know where to start, what tools to use, or how to go about it. The process is relatively simple these days and often completely automated if one really knows what to do and how to do it. Hence one needs no excuses when vital documents or records are all gone or missing due to none backing up. The following tips are ways and methods of effective back up.

i. Network Attached Storage

NAS, or Network Attached Storage, are autonomous storage devices that sit on a network outside of the PC remotely connected via Wi-Fi or wired network. This technology is a tool of businesses that is more prevalent for personal use as the number of household PCs and file sharing networks increased.

In many ways, the computer treats a NAS device like any other hard drive. It will show up as a separate disk in 'My Computer' or as an icon on the desktop which could be accessed just as one would on any drive (external or otherwise). Since it's not directly attached to a PC, it can easily be accessed by several computers at once for sharing files. Even better, consumer-oriented NAS boxes often come packed with additional features that make them an incredibly attractive choice for data storage, such as the ability to automatically back up data on a regular schedule (usually every night while asleep). And since a NAS device sits on a network separately from the PC, it should still be safe even if something disastrous happens to the entire computer.

NAS is still viewed as one of the best and most versatile method for data storage and backups but not often used in Nigeria, probably because of lack of awareness and the difficulty in setting them up than a USB hard drive.

ii. External hard drives with backup software

The most common method for backing up data in the world which is also prevalent in Nigeria is the use of an external drive, like those from LaCie which come pre-packaged with software for easily duplicating files. Many drives come with a one-click solution, meaning one can press a button on the front of the drive or the desktop to begin an automatic backup. Any other backup software such as Acronis True Image, Time Machine, or the built in Windows backup tool are also used.

Other devices in this category that are often used for backing data are; the USB Flash Drives, blank CD/DVD, Tape streamers, Blu-ray media and drives. These devices come in different shapes and sizes. They are light and can easily be carried about with lots of stored information.

iii. Online Option

Online file storage solutions are an excellent option, especially if one wants to share files between several PCs or save data for future use. Some Internet storage solutions are used without ever leaving the Web browser, while others add themselves to 'My Computer' like they're just another hard drive. Still others install small apps that work in the computer's background, syncing data to the Web without the user ever having to do a thing.

This option is becoming more popular in Nigeria as the most common method of data backup begins to fail and computer users become more aware of the importance of securing their vital information. This off-site method of backing up data has been proven as one of the safest way in keeping the computer data/information safe. This is true even in times of flooding or fire incidents, the data is safely kept on-line.

The only disadvantage in this method is the risk of hackers that may cause harm to the data being stored which may sometimes affect data integrity, rendering the data invalid.

Whichever backup method one chooses, it is important to separate the Power for the main machines and backup machines. This doubles the chances of data protection in the event of a surge/spike/blackout/brownout; ie. if power protection on one setup fails, the other may have survived, but if they are both on the same channel, both may burn. Actually though, the best thing to do is to keep the backup physically disconnected from power when not being used.

Redundancy (RAID)

RAID is an acronym for Redundant Array of Independent Disks first described in a University of California at Berkeley paper entitled "A Case for Redundant Array of Independent Drives," published in 1987. The purpose of RAID is to set **fault tolerant and extremely fast disk arrays**. It is known as the **easiest set and forgets method**. Redundancy is not the same thing as backing up data. Redundancy is instantaneous - backing up is time-lapsed. They serve different purposes, but both within the context of data loss. Generally within computers a certain level of redundancy can be achieved by having 2 or more drives in a RAID 1 (*uses two identically sized disks to make two copies of all data, or "mirroring/Duplexing"*). As a result of the duplication of all data, available disk space is 50%.

When more than two disks in an array are mirrored, data are not only mirrored but also are striped. This method is called RAID 1+0 or RAID 10.

RAID 5 configurations which are also known as DDG (Distributed Data guarding) requires a minimum of three drives. In RAID 5 configuration, parity data is not stored on a dedicated drive but is distributed evenly across all drives.

The Advanced Data Guarding (ADG) RAID delivers higher fault tolerance similar to RAID 1 while keeping capacity utilization high. This configuration protects data from multiple drive failures while only requiring the capacity of two drives to store parity information. This higher level of protection is ideal where large logical volumes are required.

By writing everything on the computer to both disks at the same time, a *RAID array* ensures that even if one of the hard drives fails, the computer will operate normally as long as the other still functions. That means, any RAID configurations adopted covers against one of the drives dying or crashing. However, if one accidentally deletes a file or experience file-system corruption, redundancy does not help. That's where time-lapsed inter-computer redundancy (ie. Backing up) helps.

Archiving

Archiving achieves the safe storage of non-active data or projects. It can be regarded as separate from backing up as it is predominantly for non-active as opposed to active data, so the storage methods can be permanent (ie. read-only like CDR/DVDR) if desired, and once-only as opposed to recurrent. This form includes optical disc storage (cd/dvd/blu-ray), tape storage (though less common nowadays) and external computer/hard drive storage. Generally if the data is important, a mixture of two or more forms of archival is good for data safety purposes. This achieves a certain amount of redundancy and also allows for more safety where one particular media might be faulty or have a shorter life-span. For proper safety, it is advisable to keep some of these storage devices far away from the computer building where

the data saved is in use. More often than not, the NAS and Online options mentioned earlier have more advantages than the archiving.

Electrical Storms

Electrical storms are composed of **lightning and thunder**, typically accompanied by heavy precipitation. Each storm forms in large cumulonimbus clouds (thunderheads) stretching one to five miles in diameter with a height of about 25,000 feet.

Electrical storms are an amazing phenomenon. Although lightning can instantly destroy any object in its path, it is not considered a very dangerous natural disaster. It is a very isolated event as each lightning strike only affects a minimal area and rarely kills or injures humans and animals. Lightning does contain a significant amount of power, reaching temperatures hotter than the surface of the sun, and creating shockwaves that is known as thunder.

Electrical storms are very common in Nigeria as they are very devastating to computer/communication equipment (most especially during the raining season period, between the months of March to November – Though global change effect may affect this statistic) as most computer users play ignorance thereby blaming nature (Act of God) for their inadequacies or proper preventive planning. When lightning or thunder strikes in an area that computer buildings are not well grounded or protected with lightning and thunder arrestors, computer equipment could be damaged, that may result in huge data loss. This is prevalence in Nigeria.

Electrical storms can also cause power failure/spikes/surges/brown or inconsistent frequencies which are the first level of defense against data loss. Therefore, the best prevention to life and property (most especially to computer data loss) is adequate provision and protection against these natural disasters by installing powerful anti-thunder/lightning gadgets in all computer/communication buildings. This should be done or carried out by professionals in their chosen carrier.

Lightning is the leading cause of forest fires, igniting trees and burning entire forests in most advance countries like America and Australia thereby endangering human life and other properties if adequate protection is not in place.

Fire

Fire disaster is another impediment to computer data loss and life endeavour. The rate of fire accidents in Nigeria, where hundreds of lives and property worth billions of naira are lost annually to fire disasters, has become a subject of concern among the citizenry. Fire incidents have contributed more than 25% death to life and properties (including computer systems) in recent time in Nigeria. This is especially so considering the use and storage of fuel and other explosives in houses and office buildings to operate power generating sets. Other causes that may have resulted to the various fire disasters in the country include accidents and carelessness, faulty wiring, reckless use of electrical appliances and heating gadgets, unattended stove and gases, children playing with matches among other causes.

For instance, an estimate of 7,129 fire accidents, about 990 lives are lost annually in the country; while the United States Fire Administration (USFA) statistical analysis showed that there were about 3,320 deaths and that 17, 000 fire-related injuries occurred in the year 2008

(quoted Abubakar Jimoh- Sunday Tribune, 08 January 2012). This statistic has been on the increase in recent time.

Electrical appliances are other serious reasons for fire outbreaks in office buildings in Nigeria, destroying and damaging vital documents and information. An Indian safety expert, Srinivas Katta (2011) identified such electrical conditions that can be fire hazards to include damaged electrical conductors, overloaded sockets and extension cords, faulty wirings, blown fuses, low quality electrical equipment, malfunction of electrical devices, loose electrical connections, and lack of clearance between electrical heating devices and combustible materials.

For office buildings where computer/communication and other valuables are stored, powerful fire alarm systems should be installed to forestall any ugly fire outbreak that may threaten life and properties. Also, at the strategic places, standardized fire extinguishers in home, office and public auditorium should be installed. The use of wrong fire extinguishers should be avoided. Mostly, fires are extinguished by water or sand. Special foam chemicals are used in case of oil fire; electric fires are extinguished by switching off electricity and using carbon-dioxide gas to extinguish the fire.

Early detection of fire is a very crucial step in fire protection and this should be ensured through individual alertness, fire safety awareness, volunteer system and automatic fire detection systems (such as fire, smoke, heat of rise, halogen gas system, audible and visual alarms on anticipated fire).

Flooding

The effect of flooding on computer data and computer equipment in general, life and other properties cannot be over emphasized, and Nigeria in this regard is no exception. In recent times, most big cities in Nigeria have witnessed serious flooding due to blockages of drainages (gutters canals) resulting in the destruction of life and properties. Hence it is advisable to have a raised floor built in swamp areas as well as low level areas in computer installation rooms or better still, avoid installing computer equipment in the basement and ground floor. This will forestall flooding.

A flood is caused by excess water surpassing the limits of its confines. A flood can happen during a myriad of events, including heavy rainfall and overflowing river banks. Floods present a significant danger with enough force to sweep away massive objects such as building, cars and trees, even human being etc.

Floods make an enormous impact on the environment and society. Floods destroy drainage systems in cities, causing raw sewage to spill out into bodies of water. Also, in cases of severe floods, buildings can be significantly damaged and even destroyed, affecting office equipment. This can lead to catastrophic effects on the environment as many toxic materials such as paint, pesticide and gasoline can be released into the rivers, lakes, bays, and ocean. Floods may also cause millions of dollars worth of damage to a city, both evicting people from their homes and ruining businesses.

Nigerian should be grateful to God for not, encountering some dangerous natural disasters like Hurricanes, Tornadoes, Volcanoes and Earthquakes at least for now because such happenings can be very devastating to life and properties due to lack of adequate preparation

for emergency response. In fact, the country's emergency response is zero judging from past occurrences (from various road accidents, Bombing incidents, plane crashes, building collapsing, and many more).

Like the saying goes, prevention is better than cure. Early preparation and prevention by creating flood plains and winding streams are two of the best ways to hinder the accumulation of water by providing a route for the drainage of water. Constant clearing of drainages (gutters and canals) is another way of preventing flooding in our environment. The protection of wetlands also helps to maintain a natural drainage system to provide a place for the excess water to gather. Such devices allow the water to evaporate before it can accumulate.

References:

- [1] HyperOffice, "Data security and integrity" - [http://faculty.ksu.edu.sa/ALFURAIH/Computer Security/Hper_Office.pdf](http://faculty.ksu.edu.sa/ALFURAIH/Computer%20Security/Hper_Office.pdf)
- [2] WikiAnswer, http://wiki.answers.com/Q/What_is_difference_between_data_integrity_and_data_security
- [3] Compaq Training manual, "Compaq systems products architecture", Vol. 2 – Server Technology, sysparch 2002 - Revision 2.11
- [4] Oracle thinkquest education foundation, " effects of flooding/ electrical storms" <http://library.thinkquest.org/03oct/00758/en/disaster/flood/effects.html>
- [5] Abubakar Jimoh- "Averting fire disasters in Nigeria", Sunday Tribune, 08 January 2012, <http://www.tribune.com.ng/sun/opinion/6034-averting-fire-disasters-in-nigeria>
- [6] www.comberton.cambs.sch.uk/Curriculum/.../Security_Integrity.ppt