SURE!

The Balmori Software Newsletter

The IT Resource for SMEs

No. 0307.2a

Causes of data corruption, and how to protect yourself

In our 20 years as a software developer, by far the single leading reason why our customers come to us for technical support has been data corruption. Your data can get corrupted or lost in several different ways; and each one brings with it it's own implications and repercussions.

COMPUTER VIRUSES

For our present purposes, computer viruses are typically small programs designed to disrupt your computing by corrupting or erasing your data, or by preventing your access to your data. Computer viruses are written by computer vandals desiring to demonstrate their cleverness, by computer criminals with more complex and sinister motives, and by employees of intelligence agencies of various countries targeting the military computers of their enemies. Computer viruses are a given in the world of computing as we know it today; so we'd better learn to live with them and deal with them.

Protecting yourself: To protect your data against viruses, the current state-of-the-art responses are as follows:
Deploy anti-virus software, such as Trend PC-Cillin, McAfee, or Norton, *and update the virus patterns religiously.* Because new viruses are being written everyday, your anti-virus software should be kept up-to-date on the latest virus going around. Get the latest virus patterns from your vendor; he will usually e-mail it to you. Your anti-virus software is useless if it protects you against all the viruses in existence in the history of the world as of last Sunday but not against the 15 written and disseminated since then.

- Deploy a firewall if you use your computer to surf the Internet, and especially if that computer is part of a Local Area Network.
- A better, but probably unpopular, idea: disconnect your Internet-surfing computer from your LAN to minimize the possibility of Internet-borne viruses getting onto your network.
- If you are using a particular computer to maintain sensitive company data (such as SURE! GL or SURE! Insurance Brokerage System or SURE! ISARAP), avoid using that computer for Internet-surfing to begin with.

ELECTRICAL POWER PROBLEMS

- Power fluctuations. The electricity coming out of your wall outlet may be less or greater than the rated output. A 220-volt outlet could be actually at 175 volts, or 260 volts, for significant stretches of time. These may be respectively too low or too high to provide the correct power to the power supply unit in your computer, and by extension, to the many chips on your motherboard and peripherals. Without the correct power, your data could get corrupted.
- Power failures. Brownouts happen less frequently in this country than in the infamous years of 1992-93, but they still do occur. Furthermore, somebody accidentally kicking out the power cable from the wall socket has the same effect. When your PC suddenly loses electrical power, any data that is undergoing processing at the time of power loss is irreparably damaged.

Protecting yourself: Install an Uninterruptable Power Supply (UPS) unit. A good quality UPS smooths out power fluctuations so that appliances attached to the UPS are getting the stated electrical voltage at all times. This function implies that you will benefit from a good UPS even if you never experience another brownout in your life. A good quality UPS also protects against sudden electricity loss by continuing to provide the correct power even as the power grid dies.

But it is important to note that most UPSs are *not intended to let you work through a brownout.* By continuing to keep your PC on and working through a brownout, you will be taxing the lead-acid battery in the UPS. Eventually, that battery will fail, and you are right back where you started, losing data. UPSs are best used as a way to power down in a calm, correct manner when you are hit by a brownout, or when someone kicks out the cable from your wall outlet. And speaking of lead-acid batteries, these are similar to car batteries. We all know that car batteries have to be checked periodically, and that, despite the best care, they die and need replacement within two to three years. UPS batteries also require periodic checking and maintenance; and they will also eventually die. Therefore, if you are wise, have your UPS checked every few months; and accept that, like all things, it will eventually die. And incorporate these realities into your budget planning.

> After six months of using a software application, your accumulated data is probably worth more than the software you're encoding it into.

Another point to consider is the load capacity of a UPS unit. Common capacities are 350W and 500W. A UPS unit marked 500W has a maximum capacity of 500 watts. This means you should not plug in more than 500 watts worth of computer hardware and peripherals to it. In fact, you should allow for a 30% margin for best performance. Thus, the most you should load onto a 500W UPS unit is

350 watts worth of computers and peripherals [500 watts x (1 - 30%)]. To determine the total wattage load on a UPS unit, check the back of each component plugged into the UPS. Each component will have a wattage rating marked on a metal-colored plate or embossed in the plastic housing in the back of it. For example, you will typically have a monitor, a computer CPU, and a printer all attached to the UPS. Returning to our example of a 500W unit, the total wattage of all three aforementioned components attached to the UPS, if we observe the recommended margin of safety, should not exceed 350 watts.

BAD HARDWARE

Perhaps this is a problem only in the Philippines and other developing countries, where people often still rank price above performance as a purchase criterion. More sophisticated cultures will have the longer view and will see that the more reliable, better performing component is in fact the cheaper in the long run. Actual experience, both our own direct experience and that of our customers, has shown that there are bad brands, acceptable brands, and excellent brands for every major PC or LAN component that you can name. In a LAN, your hubs, switches, network interface cards, and cabling are potential data killers, if you bought the bad stuff. Frayed, kinked, or poorly routed cabling is another data corruption cause. There is a reason why even among clone brands, there is a price difference between the cheapest brands and the most expensive. In general, you get what you pay for. If you are running a mission-critical application, do not be scrimping on the hardware.

Protecting yourself: After six months of using a software application, your accumulated data is probably worth more than the software you're encoding it into. Whether you like it or not, whether you realize it or not. Avoid the heartache of data corruption from bad hardware by doing your homework. Learn what the IT community considers to be good, bad, or indifferent components. Ask your IT department, if you have one, or a knowledgeable outside consultant. When buying components for your computers or LAN, shop performance and quality first, price second. (Balmori Software has a list of minimum-acceptable-quality specs for PCs that we can fax to readers upon request. Request your copy by calling or e-mailing us.)

SABOTAGE

This sounds melodramatic, and is fairly uncommon; but it does happen.

Disgruntled employees are the most likely perpetrators of this behavior, for the simple reason that in all likelihood, your ordinary blue-uniformed security guard is already successfully keeping outsiders away from your computers.

Protecting yourself: Limit access to sensitive company information in your computer or LAN. If you have a LAN, have the System Administrator control the access of authorized employees to various company data. (And don't forget: Who will guard the guardians? Have someone you trust be ready to take over from your current in-house IT expert or System Administrator. After all, *he's* not immune to disgruntlement.) Have your lawyer draw up a form whereby employees acknowledge that they could be prosecuted for willfully damaging company records, including electronic records. (And actually file cases against miscreants, to show the rest that you're serious.) Have your System Administrator enable user-tracking features in the LAN operating system to record evidence in case of deliberate data destruction

CONCLUSION

There are at least four ways you can lose data through data corruption. In order of frequency of occurrence, they are: computer viruses, electrical power problems, bad hardware components, and sabotage. Protecting yourself successfully against them requires two things: know-how and discipline. You should do your homework, and get to know thine enemy. Then, with the knowledge gained, implement the indicated countermeasures in a methodical, systematic, consistent, sustained manner; i.e., with discipline. Welcome to the computer revolution. *RSR.* Note: Read our related article entitled "Backing up: the most basic things you should know" (Balmori Software Bulletin No. 0307.2)

What is an archive?

We create archives and we make back-ups in exactly the same way, using exactly the same procedures. So you could say that the two expressions mean one and the same thing. But there is a slight difference. Their *intended use* is different.

Archives. Archives are permanent records of data. Someday we may need to view our old data, or reproduce reports from them. We can only do this if we have archives.

Archives, once created, should not be "freshened" with new data; the new data may have changed. Freshening the archive would in effect destroy the original archives (the original permanent records).

Back-ups. We have a slightly different, more defensive, motive for making back-ups. We wish to protect our *current* data against loss or damage from electrical power problems, computer viruses, or sabotage.

If any of our current data is destroyed and we do not have back-ups, our only alternative is to re-input data. Therefore, we create back-ups in order to avoid having to re-input lost or damaged data. Because of the nature of their mission, back-ups can safely be "freshened" with ever-newer data. We do not worry about overwriting the old data in back-ups, because we have our permanent archives.

Conclusion. Despite their strong similarity, archives and back-ups have different uses. We should therefore create both archives and back-ups for ideal data security.

(For a more detailed discussion of data back-up issues and concerns, see our newsletter No. 0307.2, "Backing up: the most basic things you should knowf.")

Balmori Software. We make it simple.

Balmori Software Inc. Tel.: +632-890-1977 TeleFax: +632-890-1976
2/F, Delben Building E-mail: balmori@balmorisoftware.com
1090 Chino Roces Ave. Website: www.balmorisoftware.com
Makati City 1231, Philippines