



21

WORKSTATIONS

The Weakest Link

Why is it drug addicts and computer aficionados are both called users?

INTRODUCTION

—CLIFFORD STOLL

At the user end of our networks are typically workstations (or personal computers). Over the years, workstations have evolved first to supplement mainframe computer terminals (dumb terminals) and then to replace them. Few companies still employ dumb terminals. PC-based workstations, laptops, and mobile devices have become so inexpensive that they can be found all across companies performing a wide range of functions. And, from a business continuity point of view, this is exactly the problem.

Mainframe computers centralized computing power and also centralized data storage. To view data stored by a mainframe required a password, and data files had various levels of security to protect them. Important data was stored in a central location, making backing up the data relatively easy. But a problem with mainframes was that programmers could never keep up with demands for their services. Personal computers, along with their easy-to-use programs, gradually migrated this capability to the individual's desk (hence "personal" computing). As this occurred, all the environmental, electrical, and physical security protections that are provided for backroom mainframes were no longer available to these many workstations and the data residing in them. You've got a problem!

In discussing critical workstations, keep in mind that servers (specialized systems optimized for storage speed and other services) located outside the protection of the computer room are always considered critical units and must be protected as such.

RISK ASSESSMENT

As always, begin with your risk assessment. Normally workstations are listed in the departmental risk plans. Are there any critical workstations in your department? Before answering, think about what a workstation can be today. It can be a desktop unit. It can be a laptop that a manager uses at work and then carries home at night to catch up on urgent projects. It can be the smartphone or tablet carried around by the inventory manager to track shipments. In a factory, it could be a machine tool controller. In a hospital, it could a testing or monitoring device. Computing power is now everywhere!

So what to do? The first thing to do is an asset inventory. Check to see how many of each type unit you have. Categorize them by what they are (notebook, smartphone, tablet, desktop) or what they are used for. Every computer has several things in common:

1. At some point, the hardware must be repaired or replaced.
2. It runs a stored program, often from a hard disk. In some cases, the program is stored in a ROM chip and rarely changes.
3. In almost every case, it stores data.
4. It's a delicate flower adrift in a cruel world.

So let's take these one at a time. We said at some point the hardware must be repaired or replaced. Funny thing about workstations is that their usefulness fades away long before they stop working. If your processes depend on the constant availability of a specific machine, then imagine what would happen if some day it stopped working. Often you can replace it, but if the machine used an older operating system, you might have difficulty getting the old software to run on the new machine. In general, if a workstation is used in your business, it should be replaced at least every four years. If the workstation is critical, the hardware should be upgraded at least every two years. Your concern is maximum availability. If a change in hardware forces a change in the software, then at least it will be a planned event with time to address the issues that arise instead of something patched together in a crisis.

The second function common to every computer is that it is running software. This is true, even if it only runs the same software application over and over

create the same software functionality immediately. Do not wait for the other shoe to drop! If the software was purchased as a "package" from a company, periodically check with the company to ensure the software is still supported. The supplier will provide updated versions of the software that will run on current operating systems. If not, then this must also go on your controlled upgrade list. Without support, the software may not work on replacement hardware in an emergency.

By keeping your software up to date, you reduce the number of spare workstations necessary to keep onsite. If a workstation running a critical application stops working, you can quickly exchange the hardware, reload the data from backup, and proceed with your business with a minimum of downtime.

In addition, software sometimes requires upgrading. This both updates the software's function and repairs problems in the code. Unfortunately, it may also introduce new problems. Have you ever installed an operating system upgrade that killed the device it was supposed to save? Controlling versions and testing software is a subject for a data processing book. The key here is that you need to be aware of any changes to a critical workstation's software.

Always keep backup copies of critical software. The ability to restore a PC's software from a backup copy is critical to a prompt recovery.

Be sure to include on your asset list all software used in critical units to support critical business functions. When in doubt, list them.

The third function that all computers have in common is that they store data. Most data files are not worth retaining or can be lost without damage to the company. Those files are not our concern. Do your workstations hold any critical data? We will delve deeper into this subject a bit later, but as you make your asset inventory, note any critical files or general categories of files these units hold. Your list of data files should indicate:

- Size. Determines optimal backup/recovery method.
- Format. Is it in Microsoft Access? Excel? Word?
- Data Origin. Does this workstation create or modify the data?
- Volatility. How often does it change?

The fourth function that computers have in common is that environmental stresses may weaken the hardware. Always use a properly rated, functioning surge protector for your workstation and laptops. Compared to your workstation, laptops and other mobile devices have the advantage of defaulting to battery power if they lose power from the wall plug. This acts as a built-in Uninterruptible Power Supply (UPS). Critical desktop PCs also need the protection of a UPS to ensure they do not suffer a "hard stop" when losing electrical power. This reduces the likelihood of a power outage resulting in a corrupted data file. After installation, ensure your users do not burden the UPS by plugging nonessential devices into it.

In addition to clean power, workstations are designed to exist within specific temperature and humidity ranges, as established by the manufacturer. Stray outside of these and your hardware will weaken and eventually fail. A typical office environment is usually fine. But a hot, dirty factory stresses the equipment. Laptops or tablets left overnight in a car during the depths of winter can be damaged by freezing—or baked in the hot sun on a scorching summer day. Problems may not immediately appear but marginal components may begin to fail.

So far, you have identified the risk assessment from data provided from each department about its critical assets and your own asset inventory made by walking around and looking at what needs to be supported. Now, the question is: How can you mitigate the risks (or threats) to your equipment, programs, and data? The most basic step involves the physical security of these assets. As you work through these steps, keep in mind your focus is on supporting your vital business functions, but from time to time you will want to extend this to other machines as well.

PHYSICAL SECURITY

Physical security protects your unit from unauthorized access, theft, and sabotage. Sabotage can have a temporary effect if, for example, a cable is unplugged, but it can also be more devastating and permanently destroy the unit. Physical security is also important to protect software and backup files. Stolen software, which can be copied and distributed across the company, can create significant legal problems.

To prevent unauthorized access, lock the computer in a room open only to authorized people, such as a computer room or an executive's office. These are secure locations because the computer room is always locked and the executive's office is watched by the secretary or locked when not in use. Locking the room or watching the unit provides a barrier to theft and sabotage.

Other workstations in your company also require protection. One would be the workstation that controls the electronic door locks, such as in a hotel, or your employee entrances. Someone sneaking in to steal something may also steal or destroy the records of their entry into this unit. Therefore, this workstation is also normally under lock and key.

How about the workstation that records the time attendance for your employees? Some companies use a barcode, magnetic strip, or Radio Frequency Identification (RFID) chip on their employee badges to indicate when each person arrived at or departed from work (punched in/punched out). This information is recorded in a database for payroll purposes. Such a workstation must be in a place where it cannot be sabotaged or stolen (because it contains significant private information about employees).

However, most workstations are not kept in locked rooms. They are out where

abandoned the office, it takes but a moment to snap shut a laptop, slip it into a briefcase, and go out the door! Desktop units are also fair game, but they are a bit bulky and more likely to disappear overnight or on a weekend. Handheld units, such as tablets or cell phones, barely make a bulge in the pocket of (stylishly) baggy trousers.

One way to hang on to your equipment is to strap it down to your desk. This is typically a steel cable through a loop in the back of your workstation. You can also buy a similar device for your laptop. To remove it, you must have the key to the lock. True, this can be defeated with brute force, but it drastically reduces the number of units stolen. However, it will not stop the deliberate attempt to damage the unit, so do not keep anything critical out in the open when it can be hit, burned, shocked, or crushed.

Workstations used in warehouses and on the factory floor should be housed in locked cabinets. Factories are a harsh environment for electronic components. A monitor and keyboard are all that a user requires. Ensure that the cabinets are well ventilated to avoid overheating the components. Locking the cabinet protects the unit against theft and sabotage. It also prevents someone from loading unauthorized software onto it.

Another important physical security issue for personal computers involves safeguarding the workstations' vital records. It is important that all PC software licenses are gathered after purchase and filed for future reference. Some companies create a software "image" of the operating system and all standard programs. This image is then copied into each workstation they own. The serial numbers on the software then all read the same. By holding these licenses in a secure location (often the same off-site storage used for your backup media), you can readily prove how many copies of a program you own.

The other vital workstation records are the backup media. These devices (CD-ROMs, tapes, external hard drives, etc.) all contain confidential company data. They must be correctly labeled and safeguarded as such.

BACKING UP YOUR WORKSTATION PROGRAMS AND DATA

The key to a rapid recovery from a theft, damaged workstation disk, or sabotage is restoration from your last good backup copy. Mainframe computers typically make a full copy of everything they have stored on disk once a week. Every day, they make an incremental copy of whatever has changed that day. In this way, they capture all the data and software necessary for them to function. The storage media (usually magnetic tape) is carefully transported and stored. Over time, some tapes are kept for historical copies and others are rotated back into use.

Workstations are another matter. Data files are often scattered about the hard disk mixed in among programs, obsolete data, and pictures of Aunt Meg, and following a naming convention that defies most logic. Although a complete (image) backup of each workstation is desired, it is expensive and most users will not faithfully do it. In addition, there is the cost of the backup hardware, handling the backups, and all the media necessary to copy these disks.

SELECTING A WORKSTATION DATA BACKUP STRATEGY

Hard disk capacities in workstations have grown rapidly over the years, and the smallest available disk sizes are more than most users can fill. Still, your backup tool must be capable of copying everything on the disk onto the media selected.

Before beginning your data backup strategy, *require* users to store all mission-critical files on a computer room file server. Make this a firm rule and, whenever you find such a file, stay after it until it is migrated properly. These files should not be left to chance, and the computer room staff will ensure they are included on the normal backup tapes. This category should include databases, spreadsheets, legal documents, and anything that is truly mission critical, which includes all documents that must be retained for legal or regulatory reasons. For a few individuals, this may mean that all their files will reside on the server. So be it! The user's workstation can still access the data as if the files were present on their workstation's disk.

That said, your first consideration is, "What do I want to back up?" Workstations hold a lot of programs that may not even be used but could require a considerable amount of space to repeatedly back up. For example, a workstation's operating system may require several gigabytes just to back up the software. Applications software can easily triple this number. Most of these programs rarely change. If a workstation were stolen or otherwise rendered unusable, you should be able to install your standard software image on a new workstation and load any additional authorized programs from your support staff copies. Then the data can be loaded and you are finished. Therefore, for most workstations, it is not necessary to make backup copies of the programs—just the data.

Special-purpose workstations may have specific configuration settings in the software or operating system that are necessary for it to work properly. For these workstations, you may want to make image backup copies (the entire disk).

This is important because the larger the amount of data to back up, the longer it will take. If you are copying unnecessary materials, it will make your backup strategy more expensive, to no purpose.

Once you have trimmed the job down to copying only data, consider which data you want to save. If you are keeping copies of old files and correspondence on your workstation for historical purposes, consider moving them to a CD and deleting it from the workstation. Again, why copy something over and over when once will do? The archive CD should have the proper level of security on it. Either store it off-site with your other vital records or in a locked vital records storage unit onsite. Mark every CD legibly as to the originator, date created, and contents. Do not stuff it in your desk if it contains any sensitive information.

Another valuable space saver is to delete files you no longer need. Some people never clean out their attic and others never delete files from their PCs. If it isn't needed—delete it! If in doubt, copy to a CD and then delete it.

Data, under which are folders by topic and by product, such as Excel. To back up all the data, copy them to a CD-ROM for storage with a drag and drop. Click on the Data directory, drag it over to the CD-RW drive, and drop it. The operating system copies it for you and then waits for you to tell it to burn the CD. You can type away while the copy is made.

CDs are so inexpensive, on average less than 20 cents each, that they are practical for data backup as long as the older, unneeded copies are properly destroyed. For most end-user workstations, this is the easiest way to make their own copies. Be sure they understand and comply with your standards for marking backups (for easy identification when it is needed for a restore). In addition, simplify the collection and filing of backups. From time to time, check off who is handing in backups to identify the people who are forgetting their good data processing practices.

Another option is to use a cloud storage vendor to store your backups. Many devices and applications can be configured so that the data is stored at a third-party cloud provider and is readily accessible from a replacement device if needed.

With that said, here are the factors to consider when selecting a backup strategy for your users.

■ **Storage Volume Requirements.** The backup media used should be capable of handling the anticipated volume.

■ **The Length of Time to Make the Backup Copy.** Huge amounts of data take huge amounts of time to copy. However, a typical end-user workstation should not require more than a single CD to back up its data, if storage-intensive files such as audio, movies, and pictures are stored separately from the data.

■ **Interoperability.** The backup media should ideally be compatible with the operating systems and applications in use today and in the future. For example, in 2003, most major PC assemblers announced their intention to drop the 3.5-inch floppy disk from their new PCs. Many new PCs no longer come with CD or DVD readers.

■ **Backup Software.** Ensure that users know the process for making backup data copies and that their tools are easy to use. This will improve the chances that backups are regularly made.

BACKUP TECHNOLOGIES

Many different technologies are available for end-user backups. Whatever is used, be sure to mark the backup with the date and the user's name. The most popular include:

■ **Tape Drives.** These are readily available for desktop computers. Most tape backup software can be set up to run automatically. Tapes provide the greatest amount of storage space. Depending on the technology, a single cartridge can hold several hundred gigabytes. However, to fill such a large tape may require a considerable amount of time. Furthermore, the higher the capacity, the greater the cost per cartridge. Multiply this by the number of workstations that need to be backed up and this can be an expensive proposition. Tape is best suited for server backups.

■ **Removable Media.** Products such as Zip cartridges from Iomega are used similarly to floppy disks. They are faster and easier to use than tape drives. The cartridges are comparable in cost to tape media, but they have a lower capacity.

■ **Compact Disk Read Only Memory (CD-ROM or CD).** Rewritable (CD-RW) drives are standard on new PCs and have replaced the old floppy disks as the medium on which to load software and data. CDs are low in cost and have a capacity of approximately 700 megabytes (MB) of data per disk. Most CDs (known as CD-Rs) can only be written to once, but CD-RWs allow you to write to and edit the material on the disk. Given the low cost of CDs, they are the most cost-effective way to back up end-user PCs. If all your data are consolidated under one master directory, you may be able to fit them all onto one disk.

■ **DVD-Rs (DVD Writers).** These are a step up from CDs in that a DVD holds approximately 4.2 gigabytes (GB) per disk. The disk is the same compact size as a CD. These devices are gradually dropping in price. Most PCs now have one drive that formats and reads both CDs and DVDs.

■ **Cloud Backup.** This is usually a commercial service that uses the public Internet to back up data from the end-user workstation to a remote server connected to the Internet. Software is loaded onto the workstation that is used to schedule the backups, select the files to be backed up, and communicate to the backup server. Data files are normally encrypted to ensure security during transmission. A major advantage of this method is that the user does not have to deal with backup media, and the backups can be run unattended. One disadvantage to this approach is time, as the speed of your Internet connection affects how fast data can be transferred to the backup system.

However, this is a very useful tool for "road warriors," as it allows them to back up their data while traveling. Remember, only back up the critical files that have changed. Almost all hotels have installed broadband services for travelers, so this option is becoming more attractive.

■ **Network Storage.** If the workstation is connected to a network, that unit can back up its data via the network to a server. The network file servers are then backed up daily so your files eventually end up on tape. There are two basic ways to use the network:

1. *Backup Initiated by the Server.* The server can be configured to read the data from the workstations and store the data either to the server hard disk or to a backup medium.
2. *Store Data to the Server.* A networked disk can be configured for use by the end users who configure their application software to write to the virtual drive rather than to a local drive. The networked drive is then backed up as part of the normal server backup process.

Desktop.com is a computer resource for business. The Best Business Magazine

directory. Multiply it times the number of users. This approach, while elegant, may not be practical.

The second obstacle is bandwidth. All these workstations can clog the network with massive data transfers. Finally, the server disks can only run so fast.

WORKSTATION VIRTUALIZATION

Another option for making recovery of workstations easier is to use virtualization technology to run an image of the workstation on a protected server. If the workstation is lost in a disaster, the workstation image can be restarted on a new workstation and the end user does not miss a beat. This also makes the workstations easier to maintain as new software is installed and old applications are removed. A virtualized workstation can provide a managed, stable desktop environment that can be accessed using a standard PC or a less expensive thin client device. The virtualized desktop software (such as VMware Workstation or Microsoft Virtual PC) provides a virtualized full client environment using a server-based hypervisor. This allows the user to have full administrative control over the desktop environment and applications. Some of the advantages of desktop virtualization include:

- ▶ It's easy to deploy desktops to new users.
- ▶ Desktop machines can be less expensive PCs or thin client devices.
- ▶ It's possible to use your desktop environment from any PC with network or Internet access.
- ▶ There's access to typical desktop features such as multiple monitors and USB devices.
- ▶ Disaster recovery at the desktop is simplified as a new device can be quickly installed to use the virtualized image on the server. Backups can be managed at the server level.

Virtualization of desktop workstations also creates the opportunity to have desktops provided via the Internet, much like many vendors are doing with applications using the "software as a service" (SaaS) model. For desktops one term being used is "desktop as a service" (DaaS), while others use the term Virtual Desktop Infrastructure (VDI) as a service.

Some issues to be aware of when considering desktop virtualization:

- ▶ Your per-seat cost may be initially higher due to the cost of the servers, virtualization software, and Windows licenses.
- ▶ The OEM version of Windows that comes with most new PCs cannot be used in a virtual environment; new licenses must be purchased.
- ▶ There will likely be user resistance to giving up their full client PCs.

END-USER BACKUP ISSUES

It is important that the data recovery plan emphasize the availability of the data, protect the data's confidentiality, and ensure the data's integrity. Some processes to follow to make restoration of workstations easier include:

- Train end users on the importance of backing up data on a regular basis. If the process is simple and easy to follow, they will usually cooperate.
- Document vendor and configuration information for all specialty workstations.
- Establish a mail slot-type drop-off for backup media in the data center, where they can be dropped off securely. Provide labels that may prompt end users to fill in essential information. When tapes are recycled (old backups no longer needed), provide them to users at a pick-up point. From time to time, test these backups to ensure they can be read. Sometimes data backups look like they worked but they did not.

HARD DISK RECOVERY

Sometimes you are just sure that whatever was on your hard disk is lost forever. This could be a workstation that was melted in a fire or submerged for days in a flood. It could have suffered a head crash. Don't be too depressed. There are companies that specialize in recovering data from severely damaged disks. They can also recover data from deleted files (the ones that the usual file recovery software cannot rebuild).

These companies use specially trained engineers to disassemble the hard disk unit in their clean rooms and extract the data. The services can be expensive, but the savings to your company can be considerable.

MOBILE DEVICES

Mobile devices are the wave of the future. The ideal is a unit that can accompany you throughout your workday and that is unobtrusive, light, and always ready for use. Today we have laptops, notebooks, netbooks, e-readers, tablets, and web-enabled smartphones. Once these devices depart the cozy confines of the office, they introduce a new range of issues to be addressed.

MOBILE SECURITY

Unlike desktop workstations, laptops and tablets advertise how light and easy they are to carry. This portability also makes them easy to steal. Once a mobile PC is taken out of the office, it loses whatever protection your facility's security force provides. Several steps should be taken to protect this equipment:

1. Keep it out of sight if possible.
2. Do not carry it in a carrying case that is obviously for laptops or other mobile devices. Use a standard briefcase or pack it in your luggage.
3. When it is not in use in your hotel room, store it out of sight.
4. When attending seminars or business meetings outside the office, never leave it

5. While it is in your car, keep it out of sight. Then if you go to a restaurant for lunch, it isn't visible sitting in your car.
6. When passing through airport security, ensure no one is ahead of you before laying it on the scanner's conveyor. This way it should arrive at the other side the same time that you do.

Essentially the same holds true for a smartphone. While you carry it on you and keep it in easy reach, you also want to keep it out of reach of thieves. If a thief cannot see it, they cannot target it. Airports are a favorite place to steal laptops and phones, and there are many ways to waylay the unsuspecting. Targeting a company's executives in an airport is a very effective tool for industrial espionage. You think it was just a thief, but your competition may now know many hidden details of your operation.

Some managers take their laptop or notebook computers home or use personal tablets or smartphones to catch up on work. The problem is that if they have an accident on the road, someone must know to promptly remove the device from the vehicle as soon as possible (with the permission of the police). A notebook or smartphone is an easy theft item that could be removed from a wreck and not be missed for several days. More than the PC itself, it is the data you are safeguarding.

MOBILE DATA BACKUP

Mobile devices present their own particular backup issues and are even more of a problem because they are less likely to be connected to the corporate network. Users are also a problem, as most think that a disaster such as a lost or damaged device will not happen to them. These devices are much more fragile and more easily stolen than desktop PCs.

Always make a full backup or virtual image of your laptop before a business trip. This will lessen the impact on your job, because the replacement unit can be restored from the backup. If necessary, a new unit can be loaded and sent out to you.

If your laptop has critical data files (such as legal briefs of contracts), they can be burned to a CD and stored in a different piece of luggage. Again, if the laptop is lost, the CD can be loaded onto a new unit. Guard the CD carefully—your coat pocket will do!

The average IT-enabled person uses at least three portable devices and spends more than one hour a day trying to keep these devices synchronized.

PROTECTING END-USER VITAL RECORDS

Ensure that your department's vital records program includes the handling of your data backups. Workstations tend to be somewhat secure, but if competitors can lay their hands on your data backups, in most cases, you would never know. Furthermore, to break into your workstation they must hack past the password, but no such obstacle confronts someone who wants to read the backup tape. Therefore, always treat backup media as critical data and store it properly.

Another vital record is the paper copies of your workstation software licenses. These are essential to prove the number of licenses you have purchased in the event of a software audit. If your equipment was lost in a fire, the licenses can be used to demonstrate ownership and the software copied onto your new equipment (always consult your company's attorneys if such a situation arises).

Along with the licenses, the original software media must be secured as a vital record. This reduces the likelihood that people will install unlicensed software on multiple workstations. On the one hand, they may believe they are helping fellow employees by providing programs for their use. On the other hand, they may be ready to resign and are setting you up to be turned in for using pirated software! Don't take chances. After installing programs, promptly gather the media and store it with the vital records. Then if you are accused, you can show you have taken prudent steps to control and stop it.

Vital records can turn up in several unwanted places. Before recycling tapes from storage, be sure to erase them because they may not end up with the same user every time. Backups on CDs cannot be recycled and should be rendered unreadable, usually by crushing them or putting them through a paper shredder.

Another set of vital records to protect is found in your surplus workstations. When a PC is ready for donation to charity, remove the fixed disk and destroy it. Some people crush it; others make holes in it with a heavy drill. There is a lot of sophisticated technology in the world that can recover data from your disk, no matter how thoroughly you reformat it. The charity receiving the PC will need to find someone to loan it old hard disks. *Never* send one out in your surplus PC.

ADDITIONAL RESOURCES

www.tigerdirect.com (<http://www.tigerdirect.com>)—Devices for securing workstations to a desk, backup hardware, and media.

www.bsa.org (<http://www.bsa.org>)—Business Software Alliance (BSA) educates consumers on software management and copyright protection, cybersecurity, trade, e-commerce, and other Internet-related issues.

CONCLUSION

When supporting workstations, it's not a matter of if it will break, but when. Periodic upgrading of both hardware and software is necessary to ensure that support will be possible if a critical PC fails.

Although the proliferation of personal computers has produced many benefits, it has made life more difficult for those charged with protecting vital corporate

