Realtime publishers

"Leading the Conversation"

The Shortcut Guide™ To

PC Restoration and Disaster Recovery

sponsored by

Scalable

Mark Scott

Introduction to Realtimepublishers

by Don Jones, Series Editor

For several years, now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Chapter 1: Anatomy of a PC Desktop

Most of you reading this document are sitting in front of your personal computer (PC). For most users, that computer is an integral part of their work environment, often more important than their desk, office, file cabinet, or any other accoutrement found in their workspace. According to Gartner Dataquest, over a billion PCs have been sold, with that number expected to double by 2008 (Source: As cited by BBC News, http://news.bbc.co.uk/2/hi/science/nature/2077986.stm). Most users have, at one time or another, had their PC fail. The cost of recovering from a failure in terms of lost productivity, permanently lost data, frustration, and loss of credibility is difficult to quantify.

The challenge to Information Technology (IT) groups is to keep all those computers running safe and secure. This task can be overwhelming. Most of the information that keeps an organization running is scattered on hundreds or thousands of hard drives. They are located in different offices, regions, and countries. Although it is challenging to copy this information, the backup of these computers can save untold man-hours and hundreds of thousands of dollars in lost productivity and the preservation of irreplaceable data. This guide seeks to develop a framework to help the reader understand the issues. That understanding can help organizations develop a PC backup and restoration system that saves money, preserves employee productivity, reduces frustrations, and helps the entire organization operate more consistently and predictably.

The purpose of this guide is to help IT departments develop a realistic approach to protecting the data on the PC desktops in their organizations. Each desktop—whether a mini tower sitting under a desk, a laptop, or some other form factor hardware—is actually an ecosystem of interrelated hardware, firmware, software, and data. This guide will look at these interrelated layers and examine the challenges of protecting their contents and restoring them quickly so that users can remain as productive as possible.

This guide is organized into four chapters:

- **Anatomy of a PC Desktop** dissects the PC by examining it from different viewpoints to determine what it contains and what should be protected and preserved. This helps determine the requirements for a PC restoration and disaster recovery plan.
- **PC Hardware Life Cycle** considers the maintenance of the hardware platform from repair of failed components through upgrades to platform replacement. It includes re-tasking platforms for other uses and migration of desktops from one platform to another in a effective manner.
- **Software Life Cycle** looks at maintaining operating systems (OSs) and applications. It provides guidelines for maintaining patches and securing software. The chapter looks at moving a personal desktop from one standard to another as people switch roles. It also addresses major upgrades.
- **Planning for Disaster Recovery** provides guidelines for developing a practical, effective system for backing up critical data from individual PCs and creating a system by which those backups can restore individual worker productivity in minimal time.

There is a tendency to think of a PC as an integral unit. But the PC consists of a variety of individual subsystems that work together to provide services to the end users. Like many multi-faceted objects, it is often best to view it from different perspectives. This guide will attempt to envision the PC desktop from four primary perspectives.

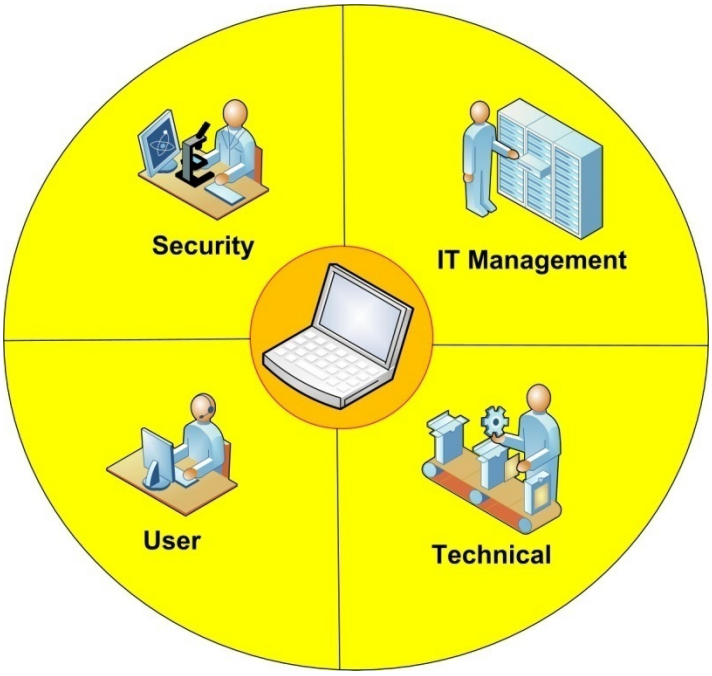

Figure 1.1: The desktop can be viewed from many perspectives. Each perspective shows distinct challenges and options when that desktop requires restoration.

Users see the desktop as a microcosm of their world. It is often a mixture of work requirements and personal life. They depend on this environment to get their jobs done. They store data, credentials, and pathways to the information they need to operate effectively.

Technicians see the desktop as an eclectic collection of parts that must work together to provide the familiar services that the end user expects. Having an accurate view of the individual parts that make up a desktop and access its critical installation components and configuration data can facilitate the maintenance of the desktop.

Those responsible for security and compliance care that critical data is saved and protected. They also care that the desktop environment is protected from unwanted viruses, spyware, and other incursions.

IT management faces the challenge of managing hundreds or thousands of desktops scattered throughout the country or the world. They set policy for the Help desk and technicians, answer to Legal for licensing, provide for the requirements of security, and ultimately are responsible to keep the desktop serving the user.

User Perspective

If you talk to an average user, they think of their PC desktop as a physical entity. A laptop or desktop system unit they use every day. But if you talk to them more, they really consider the desktop to be the programs, data, connection options, and other elements that they often cannot even define. The desktop to them is really an environment in which they do their work.

If you look at the desktop environment like an office, it starts to become clearer what makes the desktop important to the user:

- The desktop contains the files that users create as part of their jobs
- The desktop contains configurations to get to the services of the network
- The desktop contains the tools that lets users do their jobs
- The desktop contains personal customizations that keep them productive

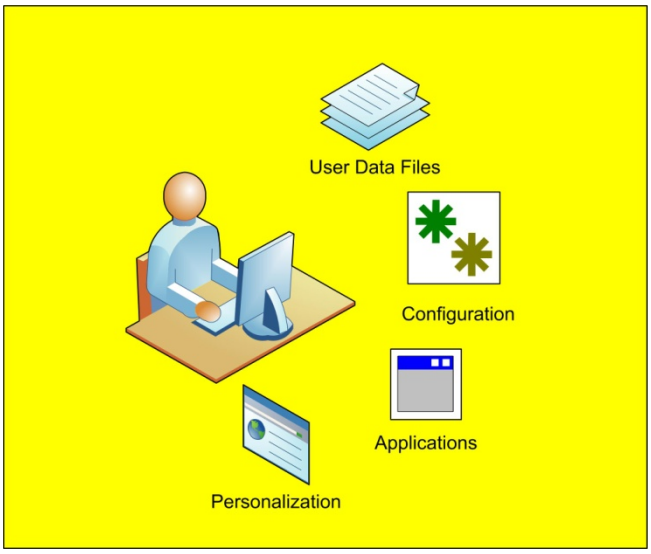

Figure 1.2: Users tend to see the desktop as a unified entity. They are often unaware of the different areas they configure and customize as they make the desktop their own.

Organizing Data Files

People organize information differently. Some people are quite particular about the way their files are organized with every scrap of paper in a properly labeled document, tucked neatly away in a drawer. Others want to keep an eye on things, so they buy bins and organizers, but leave the data where they can see it. Some just place papers in stack. Still others do not take care of their data, and perform endless searches for that scrap they distinctly remember seeing at some point in time.

Data Sprawl

Storing information on a computer hard drive is really no different. Some people quickly learn to organize the data on their drive into a complex array of folders. They carefully name their files and always know where they saved them. Many people will allow each application to determine where the data gets stored. They often rely on the "Recently Used" functionality of a program and struggle if they want to find an older file. A number of users will store the files they are working on right on their desktop, just the way they would a physical file. They can see it and it makes it easy to access via a simple click.

Microsoft has recognized the challenge of managing data sprawl. The company created a Documents and Settings folder where all user documents can be placed. They have been adding to the folder structure with each subsequent releases of the operating system (OS), providing greater granularity to the standard folders for storing information. They enhanced that in Windows Vista, reorganizing the folder structure to include specific folders for Contacts, Cookies, the Desktop, Documents, Downloads, Favorites, Links, Music, Pictures, and so on. The goal is to help standardize where people and programs look for data.

Applications must also establish a default location for storing data. Many applications create their own data directories, either adding special folders to the user directories available in Windows or storing data in subfolders of the directory in which the program is installed.

The problem has become so ubiquitous that Microsoft, Google, and others provide software that maintains an index of all the files on your computer, including their names, content, and meta-data properties, just to help users find their files. Computer performance is impacted as these indexing programs search through the drive trying to find bits of data.

Preserving User Information

IT faces the task of finding a consist method of backing up the data in a manner that makes sense. For PC backup, there are three common approaches.

Imaging technology

With this method, imaging technology is used to make a complete copy of the user's hard drive. The copy should be exact, so restoration of the user's data (and for that matter, everything on the PC) is relatively straightforward. It is often considered the simplest method for restoration. Windows comes with a built-in utility that provides this type of functionality. There are some issues with the method that should be considered, however.

This method copies all files indiscriminately. If there are 100 desktops that each have the same basic OS and application install, and that installation takes 5GB of space, then backing up a complete image of each hard drive means copying 495GB of redundant data. That consumes storage and bandwidth on the network. Since image copies grab the entire disk, not just the incremental changes to the hard drive, they are often too resource intensive to be practical.

In addition, this method assumes a restoration to the same hardware platform. The data includes everything (OS, device drivers, and user data), so switching to a different computer can create difficulties in repairing and resetting the OS and device drivers to run on the new machine. Also, if any critical files are locked during the backup, they will be missing when restored. This can result in a non-functioning application or OS.

Finally, the movement of data from one OS to another (such as moving from Windows XP to Windows Vista) may require the relocation of user data. With an image restore, it can be impossible to isolate and relocate that data.

Centralized User Data File Storage

This method requires users, by policy, to store all critical data on a centralized repository that is maintained by IT. File servers are ubiquitous and easy to set up and maintain. More sophisticated document management systems—such as Microsoft SharePoint, FileNet, Documentum, and others—attempt to make central storage of documents an extension of the application. They add value by versioning and organizing files to make them easier to share. The data is available from any computer, and can be shared with a group of users to facilitate collaboration.

The company can declare that any data stored locally is considered at risk. If the data is not centrally stored, it will be lost if the desktop is lost. This approach is centrally managed and thus relatively easy and cost effective to implement. It does, however, have key deficiencies to consider.

This approach requires the user to be connected to the network to gain access to the central storage location. As mobile workforce and PCs become more prevalent, this becomes an increasingly less-attractive option. In addition, there is no way to automate or enforce the policy without strict compliance from users. Applications may have options and add-ins that make central storage easy, but almost all of them require some user capitulation and most can be bypassed.

There is often a lot of data that users do not want placed on public shares, from confidential information to work-in-progress to unclassified research. Although this is not good data to store centrally, it does help the user remain productive.

User Data File Backups

User data file backups identify the user data files and store them separate from the OS and program files. The Easy Transfer utility found in Microsoft Vista is a form of this type of backup. By collecting the data separately, there is no need to copy redundant OS and application files. The data can be redirected to the appropriate location on a target computer. It can easily be moved from one computer to another. Using this method requires some careful consideration. The backup must be able to locate user files. Files stored in locations other than those expected can be missed. And the backup system must have the ability to distinguish between user data files and program files.

Organizing Configuration Data

The desktop is the primary gateway by which the user connects to their workplace electronically. It inevitably collects a wide variety of personal bits of data to help the user find and leverage the resources within their corporate network:

- Database connections, cached credentials, and special software for connecting to servers on the intranet
- Hyperlinks and cookies that help users work with sites on the Internet
- Contact lists, personal mail folders, and account credentials for accessing colleagues electronically
- Certificates, virtual private networks (VPNs), and security configurations
- Connections to printers, faxes, scanners, and other shared network resources

Identifying Hidden Data

The issue with most of this data is that the user depends upon it but is seldom aware of the dependency. For instance, a user can create dozens of Open Database Connectivity Data Source Names (ODBC DSNs) that allow Excel to connect to databases operating within the enterprise. Saving the spreadsheets without the DSNs will mean this data cannot be refreshed. The burden of recreating the DSNs my be quite time consuming, especially if the spreadsheet owner did not define them in the first place and has no idea which server to which they connect or the credentials presented to that server.

As Internet and intranet technology has become more popular, mission-critical applications are increasingly deployed through Web pages. A user builds a collection of these Web sites in their favorites (or worse yet, their browser history). They create an account and check “Remember Me” so that their credentials are stored in a cookie on their browsers. It is not good security or operational policy to maintain connections or security credentials this way, but the reality is, many users are completely dependent on their browser and cookie state. If they lose that state, they will spend a great deal of unproductive time replacing that lost data.

Email, instant messages, and peer sharing programs are becoming foundational to collaboration within organizations. This type of personal information can be easy to protect. Email can be stored on central mail servers, along with contact lists. Most instant massaging programs store “buddy” lists on the server as well. Peer sharing programs, such as Groove and to an extent, Lotus Notes, can store shared collaborative data. The issue with all these services is that parts can, and often are, stored on the desktop hard drive. Personal post office box files and personal address books are kept locally. Often, policy and the need to keep server mailboxes small necessitate these options. Personal collaboration files shared by peers contain local data until the files are replicated to a peer.

To allow users to connect remotely, it becomes more common to deploy specialized connectivity software. This software is often secured with digital keys. Although users are typically unaware of the keys, they need to be saved and secured. Without them, the user will not be able to connect to the network.

There are many shared resources—such as printers, scanners, fax machines and the like—permeating the workplace. All these devices are necessary to do our jobs, they all require network paths. Most require drivers and some require specialized software. And until the user can re-connect to them, he or she cannot effectively do his or her job.

Preserving Hidden Data

Although the users are often ignorant of their hidden data, they truly miss it when it is gone. The process to collect this data is straightforward, but as with the user data, the method of collection and storage will help determine how it can be used. Imaging the hard drive will preserve the data. The process can be fast and simple to understand, but only practical for restoring a single backup at a time on a precise copy of the original hardware. The drawback is the limited means by which it can be restored. More sophisticated methods of backup can segregate this data and allow selective restorations of some of the data. This is quite effective when migrating between hardware and/or software platforms, or when troubleshooting selective subsystems.

The art of restoring part of the system is to know what the system contained. There needs to be an effective means of inventorying what the user has and accurately backing up the information in a manner that allows selected parts of that information to be restored.

Organizing the Toolset

A desktop contains the tools that allow users to work productively. As with most toolsets, users become accustomed to what they have. They customize their tools and add new tools for specialized work. To keep them productive, those tools need to be kept available.

Planning for Toolset Restoration

It is not unusual for organizations to design a specific toolset of applications and OS components for their employees. By defining and distributing a standard desktop configuration, engineering and support costs can be better controlled.

The issue is that people are not as standard as the desktops that the policy defines. Inevitably, some user or users need a tool that does not come in the standard configuration. Sometimes users follow the defined process for getting custom software installed on their systems. Sometimes they take matters into their own hands. Putting aside the policy and security considerations (some of these will be addressed later in the chapter), it is likely that if a user has installed a tool, the user will need it in the event of a disaster recovery or platform migration.

Users also find add-ins and turn on features. They load them, or turn them on, and then forget that they are there. Sometime it is a simple thing, like turning on specific file associations. Sometimes it is loading a tool from the Internet. The users often come to think of this as the way the program works and forget they did something special to make it so.

Executing Toolset Restoration

The question then becomes one of support. In the event of a desktop restoration, how do the toolsets get distributed? There are a couple of approaches to distributing applications.

One approach is to distribute the responsibility to the individual users. The organization will provide and restore a base set of applications. If the user deviates from that set, he or she must take responsibility to get the enhanced tools installed as a secondary step. This is easy to administrate because application deployment is seldom tracked. Many organizations fall into this approach by default.

Whether or not the user or the desktop support technicians perform these installs, the extra effort takes time and reduces the productivity of the employee. Users are also ignorant of the version or licensing of a particular piece of software they are using. All too often, they do not even know the name of the application. This can make restoration much more difficult and time consuming.

A more controlled approach is to maintain inventories of the software installed on individual user PCs. A list of what exactly composed the desktop is required by the technician if that technician is to accurately restore the desktop. Although the list can be kept manually, most organizations benefit from a solution that automatically inventories the contents of the desktop and stores it. Regardless of how the list is captured, the user can expect IT has the information they need to get their desktop fitted with the tools that they need.

Organizing the Personal Space

The desktop is analogous to a cubicle. People start with the same space but within days they take on a distinct feeling. They change the way the icons are arranged on the desktop. They change the background picture. They modify the system tray at the bottom of the screen. They turn on or off the Quick Launch toolbar and add program shortcuts. All this personalization makes that particular desktop their desktop.

In the strictest sense, IT is not responsible for these modifications. If they are not preserved, they can be recreated eventually. Many of these steps are simple placements of files and shortcuts on the desktop, and are at least partially preserved with a thorough backup. Nonetheless, the ability to restore the backup to its state after the user gets it just so goes a long way to imbuing users with a sense of security and confidence in IT. There is definite cost benefit to the organization if the user does not need to spend hours or days re-applyng their personal settings manually after his or her desktop is restored.

Technician Perspective

Technicians tend to have a much more "three-dimensional" view of the desktop. They are keenly aware of the components that interact to create the desktop environment. Although the user tends to see the environment as a whole, technicians see it as a collection of parts, subsystems and interactions:

- Hardware components and the firmware that allows them to operate
- Drivers that allows the hardware to work with the OS
- The OS, its service pack and hotfixes
- The applications, with their service packs and hotfixes
- The personal configuration and data mentioned in the previous section

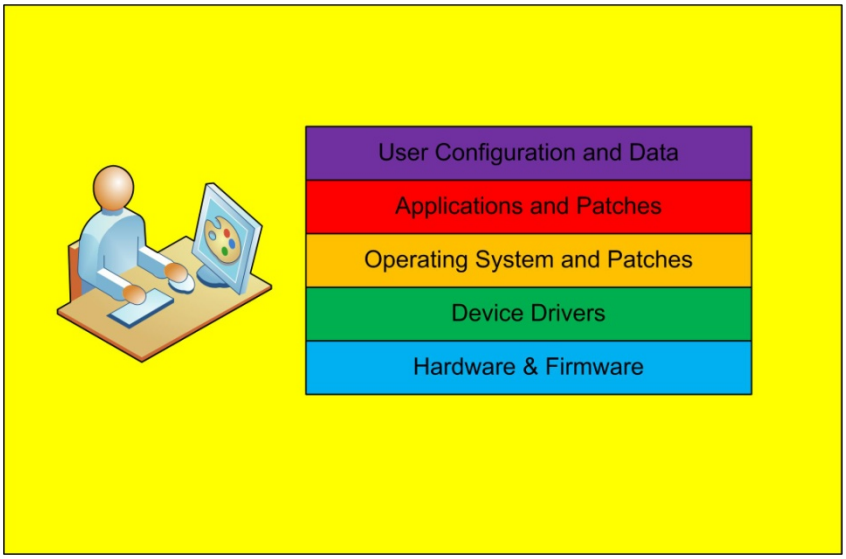

Figure 1.3: The PC Support Technician tends to view the desktop as a set of layers that must work together to produce the end result.

Hardware and Firmware

The overwhelming success of the PC market was to allow computers made with a wide variety of hardware to work with the same OS. It allowed a wide variety of manufactures to innovate, adding features and reducing costs, without changing the core experience of the end user from one system to another. Although it has been good for the market, it is a nightmare for technical support.

The Challenge of Knowing What You Have

Manufacturers are constantly replacing components within their computers. They may be controlling costs, compensating for shortages in available parts, or a host of other reasons. It means the technician really does not know what to expect when they start to work on an individual computer.

A group of the same model of desktops may contain differing components. If there are three different but equivalent modems used in that model, a delivery may contain different units containing all three. Different manufacturers and suppliers will provide differing levels of uniformity, but variation is inevitable.

The other issue is the notoriously short life cycle on individual hardware platform models. With the furious pace of innovation, a model may be available for only a few short months. The next time an order is placed, the equivalent unit has a different motherboard (and supporting chipset), different video and networking subsystem, sound cards, and the lot. It seems even worse with laptops and portable computers.

Beyond that, most components have a set of internal programs they use, called firmware, to make the component behave well within the system. Components change quickly and OS changes often place differing demands on these components, so the firmware frequently needs to be changed.

Changing firmware is tricky, and sometimes it is dangerous. Without valid firmware in place, the component, be it a motherboard, video card, optical drive, and so on, will not work. Firmware changes address specific issues and most manufacturers recommend that firmware be updated only to compensate for specific problems. Conversely, as drivers and OSs change, changes to the firmware may be mandatory.

Managing the Hardware Tangle

To manage the wide gamut of variations in the hardware, enterprise technicians need tools to help them organize the inventory of the units they keep functional. They need to keep current on the hardware deployed. This becomes more significant if the desktop is backed up through imaging. The image stores a specific set of drivers and configurations for the hardware platform from which it was copied. Applying the image to a different platform, or one that has changes in the components, can cause the restored desktop to work poorly, or even fail, once applied. Having a clear picture of the platform so that it can be accurately restored can save a great deal of time and headache come restoration time.

If the backup is componentized, with individual components such as drivers and configurations reinstalled rather than copied, there is more flexibility in the restoration. It makes restoration more reliable, particularly when components must be replaced and elements of the desktop changed to meet new platform requirements.

Device Drivers

Device drivers represent the glue that allows hundreds hardware manufacturers to produce distinct devices and still have them all work with the OS. By varying the device driver, a video card can cross between OSs, working in a Microsoft Windows, Linux, even Mac OS computer, without changing the hardware to compensate. This miraculous layer of software that fuels much of the diversity and cost containment in the PC industry represents the greatest challenge to the technical support staff.

The Dilemma of Drivers

Device drivers are designed to work with very specific hardware components on a specific OS. There are several items one must reconcile before installing a device driver:

- The specific version of the hardware component (many components will have diverse versions that support different drivers—network cards are notorious for this)
- The firmware installed to support the device
- The OS installed
- The service pack installed on the OS

It is not obvious what driver software should be used with a given hardware device. Although there have been substantial improvements, it is still quite possible for the OS to be unable to determine the correct driver to install. Even if the hardware can be identified, it must be made available. Without the device driver, the device will not work within the desktop.

There are still more issues to overcome. A chipset manufacturer will often develop a driver to support their chipset. The manufacturer who uses the chipset to create a component may use the chipset driver as is or may modify it to provide enhancements or link it to additional hardware improvements. At that point, there may be two software drivers that could work with the device.

Drivers are also difficult to test and maintain. When a new OS is released, the hardware manufacturers not only need to write software for the OS upgrade on their current devices, they must consider upgrading the software for older hardware. And even if they do not, the older driver may work with the new OS.

Dealing with the Driver Dilemma

There are several steps that an organization can take to help prevent the dilemma of drivers from interfering with the PC restoration process:

1. Know that drivers are required for a specific platform. As desktops are deployed, keep an inventory of the individual devices and drivers deployed to that desktop. This provides the information that technicians use to expedite the restoration process.
2. Certify the device drivers that work within an organization's environment. Device drivers can update frequently, and not all the changes make improvements. Test the device drivers in advance and know what version works stably with the desktop to be restored. Also, recording the previous version will help speed roll back if a new device driver introduces problems once deployed.
3. Cross reference individual components with their respective drivers. If components need to be replaced or moved between desktop platforms, the driver information should follow the device.
4. Provide a centralized repository for device drivers. Keep the drivers organized so that technicians can find them quickly, and preferably access them through the network (if anyone has seen technicians struggling to find CDs with device drivers, that person understands this issue).
5. Keep a knowledge base of the drivers installed on desktops, issues encountered while using those drivers and any workarounds or solutions developed using the driver. Keep this data available for the technicians.

Backup methodology also plays a role in dealing with the dilemma. Image backups keep the currently installed device driver with the desktop. Restoration of the image guarantees that the same driver that they started with is in place. If the hardware is being replaced, then once the image is restored, the device drivers will need to be adjusted accordingly. This process used to frequently result in the dreaded "blue screen of death," but advances in OSs make them much more tolerant of these types of shifts. Nevertheless, having no network access because the network adapter changed can slow the process of bringing the desktop up to speed.

If the approach to restoration is re-installation, then knowing the proper drivers to install on the target platform becomes much more crucial. Automating the process will go a long way toward accelerating the restoration and minimizing common human errors.

OS and Patches

The OS is the central control system that orchestrates the interaction between the applications, data, hardware, and network systems. Although individual components may fail, if the OS cannot function, nothing works.

OS Challenges

The first step is to know what OS the user is running. This would include the current set of service packs and hotfixes deployed. A large number of organizations set an OS standard and then proceed to help everyone comply. This process of moving to a new version of the OS and/or deploying a service pack could be as simple as programming an automatic deployment or as complex as having technicians visit each and every desktop in the organization for a couple of hours.

The reality is that there are typically several versions of the OS running at every given moment. Some people are reluctant to change and will do everything they can to delay the inevitable. Others want to jump the gun and find ways to upgrade ahead of schedule. With service packs available through Internet download, it can be difficult to stop them.

Sometimes, it is a matter of purchasing. PCs and laptops typically come with OSs pre-installed. The OS is already there and running, and the organization purchased a license for the OS with the hardware, so it is a difficult decision to remove a newer OS and install an older version.

Users with remote locations may be difficult to get to and upgrade. Mobile employees can be difficult to slow down long enough to upgrade. And they can be connected infrequently and may miss standard upgrades. Users with older hardware may require hardware upgrades (and subsequent desktop restorations) before they can move to the new OS. All this says that most organizations have a diversity of OS and service pack levels with which to contend.

Restoring the OS

An OS restoration is wholly dependent on the hardware platform. The OS is the bridge between the user and the hardware, so it must span that gap. As previously mentioned, the bridge between the OS and the hardware is the device driver.

If the hardware platform remains identical, there is nothing faster than an image restoration. If, however, the desktop must be restored on a new hardware platform, the drivers that are appropriate for that platform must be made available. And if the problem is contained within the image (errors in the registry, virus infection, or other anomalies), a restoration will be of no avail.

The technician needs to know what OS and patches to install to restore the operation to which the user is accustomed. That means an inventory of the system, must be kept on hand to effect the restoration.

Applications and Patches

The reason people have their computers, beyond consuming time surfing the Web, is the applications. Companies commonly define a standard set of applications for their users. They license these applications and provide people who can help support them. It should be a simple matter to reinstall that list of applications on a computer when a restoration is requires.

Application and Patch Creep

The truth, however, is that it is very difficult to keep everyone using the same set of applications. There are a wide range of reasons for this:

- Many people do not like to upgrade and fight to keep older versions of applications
- Some people cannot wait to upgrade and move to the next version before everyone else—through legitimate or illegitimate means
- Some companies link their licensing to hardware platform purchases; thus, the people with newer computers have newer software and those with older computer have older versions
- Some users install add-ons that can be downloaded free from the Internet; they can easily fall under the IT radar
- Some users have legitimate need for specialized software; as it is not widely distributed, it can be difficult to keep track of the source disks and licensing keys
- Patches for applications may not be automatically or consistently distributed, particularly to remote location and mobile computer users
- Users may install unauthorized or unlicensed software on their individual desktops

For all these reasons and others, technicians often find it difficult to know what was on the desktop to perform the reinstallation.

Restoring the Application Stack

The simplest way to keep track of the applications installed on a user's desktop is to automate collecting an inventory of installed software. There are many product solutions that will periodically inventory the computers in the network and maintain a database of who has what (this is also useful for maintaining compliance, but more on that in the next section).

The technicians need a simple means of organizing the installation packages. This can be as simple as file shares or cabinets filled with CDs and DVDs. Most products that provide automated inventory of applications will also provide for automated software distribution. The more automated and hands off the process, the quicker the restoration can be accomplished.

The technicians need policy. How do the technicians respond to users who have unauthorized software installed on their computers? These illegitimate applications may be at the heart of desktop performance issues or even computer failures. Or they may be completely innocuous. There must be a clear understanding of how to approach this situation.

A hard drive image restoration greatly simplifies this process. Everything that was on hard drive is contained in the image, so it all returns once the image is restored. But this method has a variety of disadvantages as well. Reinstallation of the application stack and reconstruction of the registry can go a long way toward improving desktop performance. It also makes it easier to move to a new OS or hardware platform.

Personal Configuration and Data

The first thing users hope for after a restoration is to see their familiar desktop displayed on the monitor. They want to open My Documents and find their documents. They want their contacts to appear in their mail program. They want things to be as they were before the restoration.

Capturing the Configurations and Data

Data files are easy to restore. They are plainly visible on the hard drive. As long as you have a copy and know where they came from, you can put them back. This problem is simple on the scale of a single desktop, but quite unmanageable on a large, enterprise-wide scale. Configuration information, however, presents a different problem.

Configuration information can lurk anywhere in the system. Some of it is stored in the registry. Some of it is stored in configuration files. Some of the configuration files are stored in the same directories as the program files. Other are stored in personal data directories for the individual user. Some configuration information is kept in files that are always open. Post office files, database files, and other program files may contain important information that improper backup software may not be able to copy.

If the restoration extends to upgrading an OS, things can become even more interesting. Microsoft reorganized the directory structure for user data in its recent upgrade to Windows Vista. To ease the transition, they created a utility to move personalization data and configuration information to its new location. Of course, to do so, the old desktop needs to be running so that the utility can find and store the information. In a disaster recovery, that is of little help. The overhead of scripting the solution and version compatibilities must also be considered. A solid desktop restoration solution should ease this migration through proven, repeatable processes that can adapt to changes easily.

Restoration of the Data

Restoration of the image requires that user data files as well as the system state be restored. The system state includes registry data and other internal information that is not typically copied in a backup. The technician also needs to ensure that the backup had the proper agents running on the desktop to back up hard-to-copy files such as databases.

As long as the target system is nearly identical to the original, an images restore can make the restoration quick and simple. But if the desktop needs to be restored to a new hardware platform, such as a laptop or a desktop PC with a new SATA hard drive subsystem, the image restore will become much more challenging. Conversely, a re-installation approach must be carefully planned and managed. Configuration information must carefully be restored, and there is a significant risk that some configuration information will be lost. For the technician, the best teacher is experience. If a technician has practiced the restoration, they will be cognizant of the issues and can prepare to deal with them.

Security and Compliance

The challenge for the organization to help users remain secure and more compliant is steadily growing. Increasingly, software companies are enforcing licensing policies and agreements. More and more malware, viruses, spyware and other malicious software finds its way into the Internet. It affects the performance of the desktop and threatens the security of the data it contains. Corporate and government regulations require that data remain secure and access be monitored and audited.

The perspective of the organization concerning security and compliance seems quite straightforward at first glance. The desktop must be a secure, compliant place where the employees can perform their work. But as the workforce has become increasing mobile and people want desktop services extended outside the office, the challenges grow. The techniques that protect data and secure extranets can interfere with backup and restoration. There are several areas the security team must consider:

- The data stored locally on the computers must be secure
- The desktop must be able to operate in a secure, safe manner within the network
- The desktops must comply with legal and corporate regulations

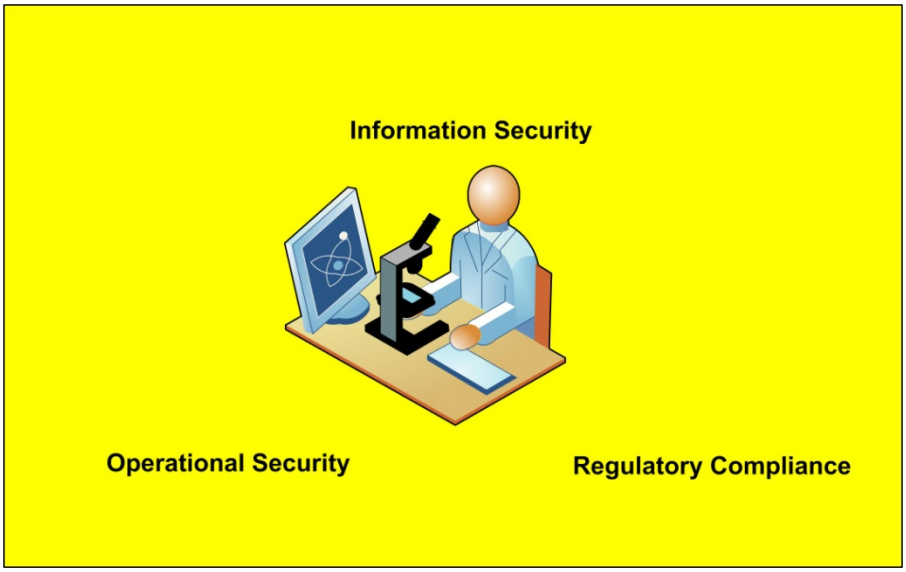

Figure 1.4: There is a growing need to protect the data contained on desktops and the operational efficiency of the desktop and to ensure that it reamins legal and compliant.

Information Security

As more users employ laptops and mobile devices, more information leaves the security of brick and mortar walls. 4GB of critical corporate data can be slipped onto a device the size of a postage stamp. Data is freely and easily moved.

Securing Critical Data

The proliferation of identity theft and the devastating effect that these security breaches cause is triggering more companies to utilize encryption to secure their data. Encryption can extend to files, folders, even entire hard drives. The Microsoft Windows OS can provide these services, and there are a variety of other products that can be implemented.

Restoring Secured Data

The restoration of secured data requires encryption and decryption keys. These keys are random numbers used to scramble the data. When the original encryption is established, the keys are generated. They can be backed up onto an external, portable medium (CD, USB key, floppy, and so on). The keys are also stored on the computer hard drive. This allows simple (often transparent) decryption of the scrambled data.

The keys can be backed up by most commercial software. From a restoration standpoint, the most critical issue is to be aware that encryption is being deployed. Whether or not encryption is employed, the backups themselves must be secured. If the backup file can be copied and restored without authorization, the data therein contained is at risk.

An opportunity offered by a restoration is to ensure that data is properly secured. Data that should not be stored locally on the desktop can be identified and moved to secure storage. Data that should be local can be tested to ensure that it is indeed encrypted.

Operational Security

It is critical that networks remain secure. There are several considerations when securing the network:

- Who can connect and get an IP address?
- What software should be installed and functional before a computer can connect?
- What is required to connect from outside the local campus?

The answers to these questions directly affect the backup and restoration process.

Locking Down the Network

Different organizations provide different levels of internal network security, depending on their individual policies and tolerance of risk. Most organizations will allow anyone who can plug into a port to gain access to the local network. This approach is simple to administer and does not require any special configuration. Organizations that are more security conscience will require the media access control (MAC) address of the network adapter to be registered in order to obtain an IP address. Some networks scan for required software before a computer is allowed access to the network. The scan may check for required software patches and antivirus and/or anti-spyware software to be installed and operational.

As network access extends to allow users an entry to corporate network resources remotely, there is a need for virtual private networking (VPN) software. This may be the client that is integrated into the Windows OS, but frequently relies on other software from vendors such as Novel, Cisco, and others. This software builds an encrypted bridge through the Internet and allows people outside the campus to connect securely. To secure these networks, vendors implement various levels of Network Access Control (NAC). Unless a computer can validate its security health (virus protection running, firewalls enables, and so on), the computer not be granted access to the network.

Restoring a Secure Desktop

The challenges of restoring the desktop are shaped by the internal security of the network. If network access is granted to designated network adapters, restoring the desktop on a different hardware platform requires coordination to allow the new hardware access. If the desktop is rebuilt through re-installation, the system must be brought into compliance before it can be reconnected to the network. The requisite software must be clearly defined to the technicians performing the restoration. The network must tolerate a computer connected to the network that is not compliant during the restoration process, or the computer must be isolated during restoration.

Viruses and malware can cause crashes, so it is often wise to examine the desktop for software infection. If an image restoration is performed, this process should take place in isolation, disconnected from the network. If a re-installation is performed, controlling the software that is placed on the restored desktop will typically resolve the problem. VPNs must be reconfigured. This task often involves the use of security keys, so either the old keys must be properly restored or new keys generated.

During restoration, computers may be non-compliant. They must be tested for connectivity to ensure they will function outside the local area network (LAN). Success restoration will require a clearly defined set of policies and procedures.

Regulatory Compliance

Companies regulate what runs on computers for a variety of reasons. For many industries, there are legal requirements covering the use and auditing of data. This often means using specific programs that adequately audit the use of such information. There are real costs that accompany the support of software, so company policy commonly dictates the software installed to help control those costs. Companies are responsible for the software installed on their computers and must properly license that software.

How Computers Become Noncompliant

People use their computer to get work done. They are looking for ways to make things easier for themselves. If someone can find a way to get to data more quickly or with greater access, they will try. It is important to meet the needs of users, but they do not always appreciate the other dynamics involved, such as maintaining complete audit trails.

Some people do not like change, and find ways of holding onto old software after it has been officially obsolete. Others like to jump the gun and get the latest version of a package before it has been released by corporate IT. Still others will find alternative packages that do the same thing. Some of them are freeware or shareware. Others may be Internet applications that pass data through the public cloud. Any of them can incur support costs and cost time.

Software piracy is rampant. Users often have software at home that they know and would like to use at work. It is often a simple matter to run a quick install and get an unlicensed version of an application on a computer. It often goes unnoticed and seems harmless enough.

Restoration and Regulatory Compliance

Restoration of a desktop is an ideal opportunity to check the compliance of a desktop with corporate policy. If the restoration is performed by image restoration, the computer can be checked after the restoration is complete. Unauthorized, unlicensed, and unsupported software can be removed.

If a re-installation approach is adopted, the issues become simpler. Only authorized, licensed software is re-installed. The process of the restoration ensures that the resulting desktop is compliant. The restoration may also result in computers that perform better because the registry will be cleaner and any unbidden software installs will be eliminated.

IT Management

The IT group has the task of considering all the various perspectives on the desk and creating a system that ensures that the desktop is protected and users can be kept productive while containing costs. They must work in four key areas to meet these goals:

- Policies
- Processes
- Personnel
- Products

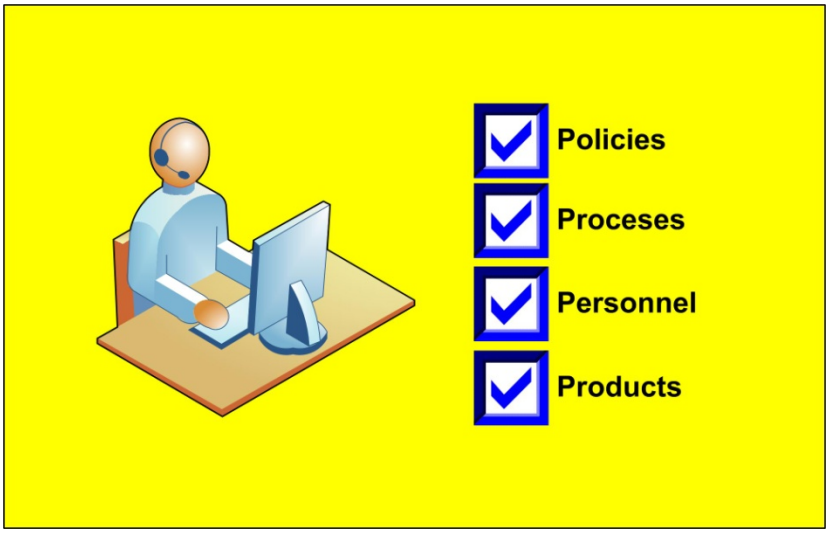

Figure 1.5: IT must develop policies and procedures, train and hire personnel, and choose the product suite that will ensure that the desktops in their organization will be protected.

Policies

The policy for desktop restoration needs to be clearly spelled out for the users and the technicians who must implement the policy. It should clearly state the requirements for each and set a level of expectation for what will be restored. The policy should be written and kept up-to-date as the needs and demands of the business change. Clearly stated policies will help users understand what to expect as well as how and why they should participate in the process. Policy will direct the technicians in what they need to do, what they should not do, and help them work with the users in a productive manner.

User Policies

User should be given an expectation of what they will get if their desktop is restored. If any information is at risk, they need to know. Items to include in this expectation contain:

- File backups (with some indication of when the last backup was likely to have occurred)
- Types of configurations that will be restored and those that will not
- Software that the user can expect to find on the computer
- Any changes to service, such as VPN connectivity or other security-related matters
- Any upgrades or other changes the user may expect to receive
- Actions that will be taken for detection of unauthorized data and software found on the desktop

Users should also be aware of their responsibilities in the process. If data is to be backed up, the computer must be operating and connected to the network while the backup procedure is performed. This can range from letting computers run during a scheduled time during the day (say over lunch) or leaving a computer on overnight. This can become more difficult for remote users who may connect to the network at irregular intervals. These users are often at higher risk, so they must take their responsibility to back up their system seriously.

Users should also be given some level of expectation of the process with which they interact to get their desktop restored. This forms a service level agreement (SLA) between IT and the user.

Technician Policies

The technicians need to know the scope of the service that they provide to the users. Since they will deal directly with the users they service, it helps to know what they are authorized to offer and how to explain what they cannot provide. The policy can help mitigate issues and prevent hard feelings. If a technician discovers compromising or potentially illegal material on the drive, they need to know the proper steps that they are expected to take.

First, users will only receive data that is backed up. Many people believe (or at least hope), there are technicians that can always find data, even when hard drives have been destroyed, erased, or physically misplaced. They believe that backups happen magically, even though they, themselves, left their computer off or cancelled the regularly scheduled backup in progress. The policy can clarify this point.

Some users are going to have unauthorized material on their computers. It could be inappropriate files or links to questionable Web sites. It may be unauthorized or unlicensed software. There are a variety of things that may not be restored. The technician needs to know what to keep and what to remove. He or she must also know their responsibility in reporting what they find, and whether or not to dispose of unauthorized material from the hard drive.

The technician needs to know the SLA. It is quite useful to refer to the policy when users want to know what is happening with their restoration and when it will be done. The policy is not meant to be a shield between the user and the technician but rather a vehicle that helps to explain the process in a consistent, predictable manner.

Since the technician is interacting with potentially secure data and network connections, he or she must also understand the security policy as it relates to the handling of data backups, security keys, and communications software. The manner in which they handle sensitive materials will underlie the security of the entire backup and restoration process.

Processes

The process used to backup and restore desktop data will greatly determine the success of the system. Backing up data is tedious. The only way to truly confirm the backup is to restore the data. A technician or user can go years performing backups and never once perform a restoration. When they finally do get a failure, they only then learn that the backups did not capture critical data or cannot actually be used to restore the desktop.

Backup Processes

Restoration is only as good as the last backup. A backup schedule that can be adhered to by the users is critical. Most systems can be set to perform backups during the night. That sounds simple enough, but the systems must be available to perform the backup. For standard desktop PCs, this can be as simple as getting users to leave on their computers when they leave for the day. For mobile users, the challenge is far greater.

The success of the backup process can only be maintained through monitoring. IT must review the status of the desktop backups on a regular basis. Missing an occasional backup is typically not crucial (but, of course, Murphy's Law indicates the backup will work perfectly until the backup just prior to failure). If multiple backups are missed, an alerting system will help determine why the backups are failing and correct the situation to restore the security of that desktop.

Restoration Processes

The only way to know for certain that a restoration will be effective is to perform it and test the results. The restoration process must be documented and tested, and standards for a successful restoration must be established. As long as everyone involved in the process knows what constitutes a successful restoration, the process can be measured and proactively updated to provide the best results.

Restorations should be performed on a regular basis. As new hardware is rolled into the organization, new applications are installed, OSs are upgraded, new data security policies are implemented, and new types of credentials are added to the desktop, the ability of the system to capture and restore these changes must be validated. The process, through use, must be validated to work as designed.

The process must also handle the exception policies. If image restores are used, and security policy indicates that a restored desktop must comply with corporate policy, the process should examine the restored desktop for unauthorized content and provide the means for extricating it. If either an image restoration or a re-installation approach is taken, restored data files should be checked for appropriate security measures and filtered for illegitimate content. There should be a final certification process to indicate that the restored desktop is properly restored and ready for use.

Personnel

The technicians used to monitor the processes and perform the backups require both technical and interpersonal skills (a tough combination to find in technicians). People who have lost their desktop may be irritable and even unreasonable. The desktop is often an extension of their work, so it can be very disconcerting to have that extension fail. The technical staff needs to be able to deal with coworkers who may be acting in stress while their desktop and its precious contents are unavailable. Also, if the desktop cannot be fully restored, due to aged backups or unauthorized content on the drive, technicians must understand how to deal with the user who will not get back what he or she lost.

Good systems can help technicians do their work, but a skilled technician is invaluable when things do no work as planned. There are often challenges involved in getting a desktop to reconstitute on a computer, let alone manifest on a completely new piece of hardware. For drive images, there are the challenges of readjusting drivers and configurations when the hardware changes. For re-installation, the challenge comes in getting the customization information re-located in the proper place.

IT needs to keep technicians well trained and familiar with changes in policies, processes, and products used to maintain the security of the desktop. From changes to OSs and applications to securing different information to upgrades to backup agents, technicians need to be kept aware and prove their ability to fulfill the SLAs between IT and the users they serve.

Products

There are a wide variety of products available on the market to help protect desktop computers. Before choosing a product, it is important to understand the expectations of the restoration policy and process. This will help develop the criteria by which the products can be compared. Consider the following questions:

- Will restoration be used to migrate desktops from one hardware platform to another?
- Will restoration be used to bring desktops into security compliance?
- Will restoration be used to assist in OS or application upgrades?
- What are the requirements for performing backups?
- What are the hardware requirements for storing backups?
- What are the hardware and network requirements for the restoration process?

Once these criteria are established, they can be used to help determine the features and services that should be offered in the backup and restoration product selected. In addition to performing a simple comparison of price and features, there are a number of intangibles that should also be considered.

Finding people who use the product are very helpful in determining the overall quality of the product. Learning how the product works under real field conditions can be most telling.

The value of the product can be difficult to quantify. The cost must be considered in terms of total cost of ownership (TCO). In addition to the cost of the product itself, the cost of the product's impact on servers, storage, network bandwidth, management time, and a variety of other factors beyond the cost of licensing must be determined. In addition, the time spent backing up and restoring data must also be considered. It is important to bear in mind all these factors when choosing a product.

Most vendors will help break down all the associated costs for running their individual systems (albeit, perhaps, cast to emphasize their individual strengths). By using the information provided by several vendors and creating a common chart, comparing all costs and all features, it is possible to develop an effective matrix for comparison. It is also helpful to contact people who have the product in place and validate the claims of the vendor.

There is a great deal to consider when developing a comprehensive program for securing the desktops of an organization. This chapter defined the PC desktop ecosystem of hardware, firmware, OS, applications, data files, and configurations. The subsequent chapters of this guide will provide additional details about what to consider when building such a program. Chapter 2 will build on the foundation laid here to explore in detail what role hardware plays in providing a user's desktop.