Realtime
publishers
"Leading the Conversation"

The Shortcut Guide™ *To*

PC Restoration and Disaster Recovery

sponsored by

Scalable

Mark Scott

Copyright Statement

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at http://nexus.realtimepublishers.com.]

Chapter 4: Managing the Disaster Recovery Process

When many people think of desktop recovery, it is in association with disaster recovery. The previous chapter explored how to lay the groundwork to use a robust, well-designed desktop recovery system to provide much more than disaster recovery. These systems can be integral in improving security, performance, regulatory and corporate compliance, and other aspects of hardware and software life cycle management.

There is little question, however, that the desktop extends and enhances the ability of each employee to perform his or her individual tasks. The desktop preserves the work product of the employees, with files that can represent hundreds of hours of labor. That work space is housed in a set of hardware that can fail. It can be lost. It can be corrupted or erased. The customizations and configurations that make the desktop so productive for an individual is slightly more complex than bytes stored in the right place on the hard drive. All this investment is worthy of protection.

This chapter will address the role that desktop restoration solutions play in disaster recovery. As with other chapters, it will look at the policies, processes, personnel, and products that help combine to ensure that, should a desktop become inoperable, it can be quickly restored. By protecting the work product and productivity of an organization’s staff, the desktop restoration solution is the core of keeping the organization up and running:

- Plan for disaster—This section will delve into the topics that an organization must consider when planning a disaster recovery system. By foreseeing the conditions that may be encountered and determining their potential disruption and cost, an organization can determine the level of risk they can endure and how much they can invest to manage that risk.
- Administrate the solution—Many organizations who fail to recover from disaster fail to do so because they do not plan how to execute the restoration. This section will address establishing policies and procedures that ensure the system designed can fulfill its role.
- Implement the solution—This section examines the steps typical in building out a desktop restoration solution. By examining a typical solution, it will illustrate the process of establishing the solution within an organization.
- Leverage the solution—This section considers the process of maintaining a desktop restoration solution. It seeks to show how the process of regular maintenance of user desktops can be combined with disaster recovery to provide a solution that benefits the organization every day.

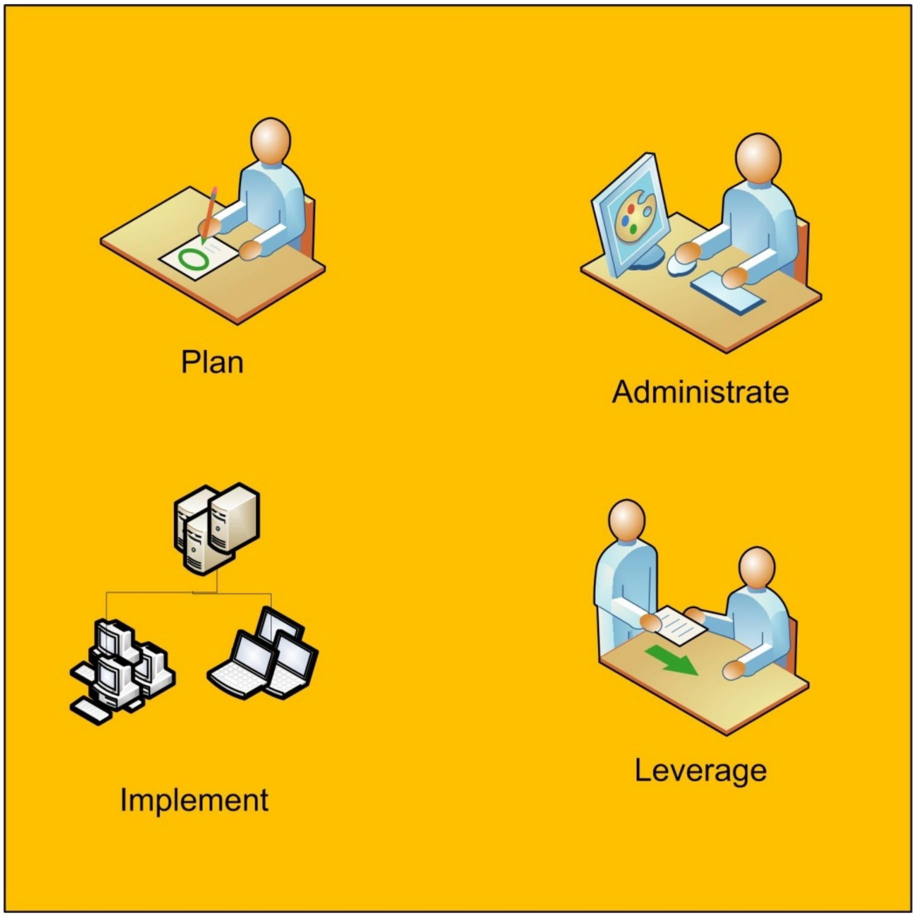


Figure 4.1: Using the desktop restoration solution to protect the organization.

Planning for Disaster

For the purposes of this chapter, disaster recovery encompasses unplanned events that make a desktop unavailable for a user. To properly plan for such events, the types of unplanned events that may be encountered must be identified. For each level of problem, there must be a mitigation strategy that will return the desktop to service. There must then be planned activities to ensure that the data is secured and that it can be restored in a timely manner. Finally, the plan must include feedback so that the processes can be refined and the system continually improved.

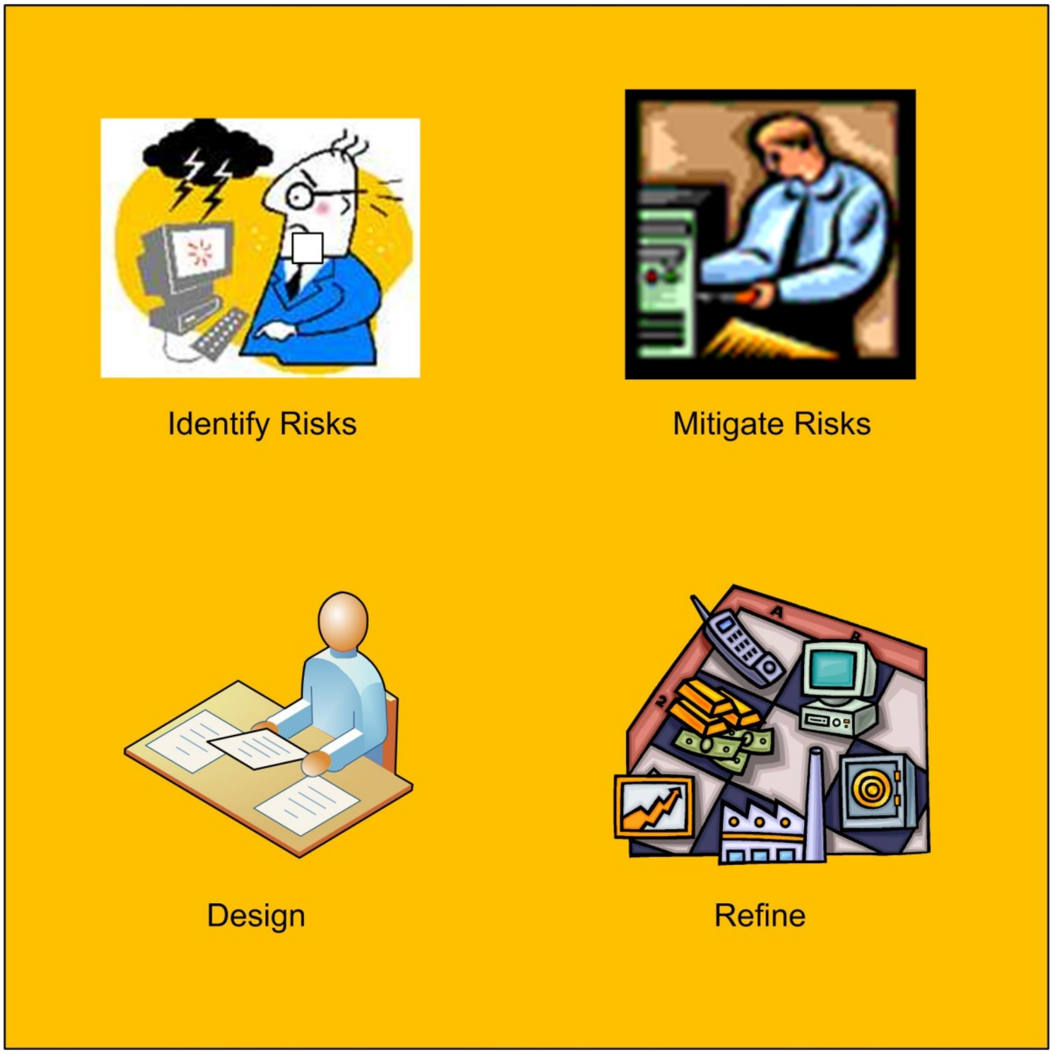


Figure 4.2: By planning for disaster, risks can be minimized.

Identifying the Risks

There are a variety of threats that place the desktop at risk. Their occurrence is unlikely but must be addressed or the productivity and work product hosted by the desktop can be lost. The desktop consists of parts. Each desktop is also part of the organization. By considering the components and their individual exposure, one can classify the risks to the desktop and better plan to protect them. Consider Figure 4.3 for how the various desktop components contribute to the desktop.

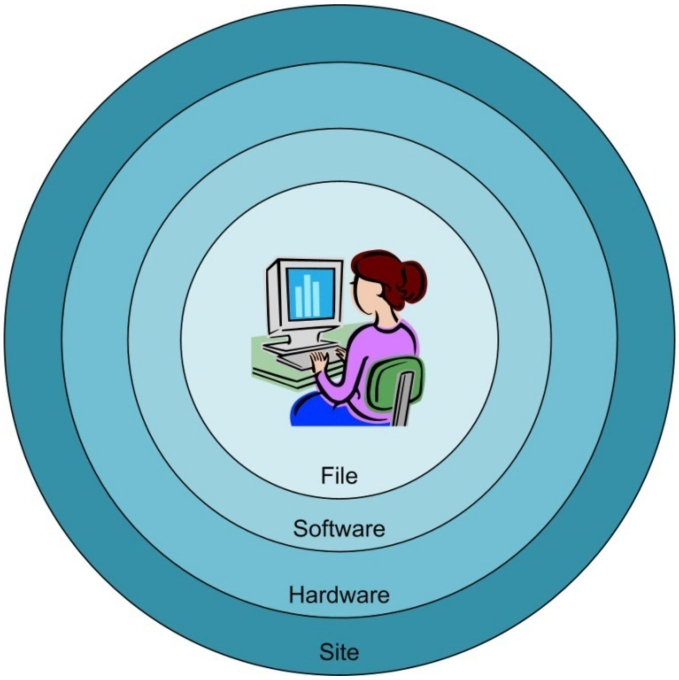


Figure 4.3: By thinking of the area of risks, mitigations can be designed.

File-Level Risks

Files represent the fruits of the labor of an organization's associates. There are several ways that files can be put at risk and that the desktop restoration solution can be used to help.

For the examination of this risk, the assumption is that the desktop is operating normally. The file is in some manner damaged or lost. Perhaps it was saved incorrectly. It may have even been saved in a location that the author cannot identify. Perhaps it was inadvertently deleted. Sometimes files are altered when they should not be. Perhaps the file was opened in a newer version of an application and saved in a format that is incompatible with the previous version. Perhaps changes were made that were unauthorized or inappropriate. An application may have been decommissioned, then a need to access the data discovered at a later date. The risk is that the loss of the file is the loss of the labor invested to create it. A virus or worm may have corrupted or deleted the files.

✎ Some of these risks are mitigated by document management systems, such as Windows SharePoint Services, FileNet, or Documentum. However, most users keep a number of files on their personal hard drives that never get stored in the document repository. Local desktop backup protects these files from loss without depending on the user to store them properly.

Software-Level Risks

There are a number of software risks for a desktop:

- OS can experience difficulties. This can be due to lost or damaged executables or errors or conflicts when applications or service patches are installed.
- Applications can be damaged in many of the same ways. Software patches can occasionally corrupt them and sometimes binary files are deleted or damaged.
- OS patches can sometimes adversely affect applications.
- Profiles can become damaged. Damage of a profile can do anything from making desktop shortcuts disappear from the desktop to making application files fail to operate correctly.
- Security files can be corrupted. This can be encryption keys and certificates or cached credentials. Any of these losses can hinder the productivity of the desktop user.

📖 For more information about software risks, see Chapter 3.

Hardware-Level Risks

The hardware components in a personal computer or laptop can become defective. Sometimes their replacement is practical and the system can be left intact to continue to host the desktop. Sometimes not, such as in the case of a defective hard drive. Sometimes the more practical approach is hardware platform replacement.

Other times the hardware itself may be lost. With the increasing popularity of laptop and notebook computers, the desktop is on the road where it is at risk of being lost, stolen, or damaged.

The interface of the hardware to the rest of the desktop is driver software. Sometimes these drivers are deleted or damaged. Sometimes applying the wrong driver to a piece of hardware makes the desktop environment unstable.

📖 For more information about hardware risks, see Chapter 2.

Site-Level Risks

On occasion, natural or man-made disasters can destroy the physical location where the personal computer hardware that hosts the desktops is located. When this happens, all the work stored on a large number of desktops is endangered. Even if the site is intact but the machines cannot be accessed, the work that could be performed on those desktops is lost.

Mitigating Desktop Disaster Risks

As there are a variety of risks, there are a variety of mitigation strategies to reduce those risks. The desktop recovery solution should be designed to address the particular challenge of each level of the risk and respond quickly and effectively.

Mitigating File-Level Risks

The risk of losing files is easily mitigated by keeping copies of the files in a secure location. The type of desktop recovery solution will directly determine how quickly and easily this protection can be effected.

A system that categorizes user data files and makes them quick to locate and restore makes restoration of lost files a minor issue. By simplifying the process of locating and restoring the file, the time lost while the file is unavailable is minimized. A system that minimizes the time spent by the technical staff to restore the file also reduces the cost of protecting the user’s work. When designing the system and choosing the appropriate tools, consideration should be given to how long such a restoration will typically take and the cost of the time expended while the file is unavailable.

Mitigating Software-Level Risks

The most common solution for software issues is re-installation. The application must be removed (not always an easy or straightforward process). Then the current software patches must be re-applied. In some cases, an older version o the software must be installed and then a full version upgrade applied. Once re-installed, the software must go through re-configuration and personalization.

Although this process can be managed manually by a service technician, it can be time consuming—costing the organization not only the time expended by the technician but the lost productivity of the employee who is denied use of his or her desktop. If the application is re-installed, any customizations made to the application for the sake of the user may be lost. More productivity will be lost as the application is reconfigured to serve the needs of the user.

A desktop restoration solution can be devised that automates the re-installation of any application. Systems that use configured installs can minimize time spent by the technical staff. The consistency of a proven automated system can make things operate much more smoothly. A system that automatically stores the customizations made by the user—configuration files, credentials, preferences, and so on—and that can re-apply them on demand will further refine the process, saving time and reducing the frustration of the user whose desktop has been damaged.

If a malicious piece of software has damaged the system (or some other event has made the OS unstable), the system may need to be restored from scratch. Again, a desktop restoration solution that can cleanly re-install the authorized and validated components that should be on the system is invaluable. Such a restoration eliminates unauthorized software that should not be installed in the desktop (and may have caused the original instability). A clean re-installation can also have the added benefit of improving performance.

Mitigating Hardware-Level Risks

If hardware is damaged, it can be repaired or replaced. The desktop restoration solution can be designed to help in a variety of ways. A desktop restoration solution can be used to distribute the appropriate hardware drivers to personal computers when changes are made to the installed hardware. They can also distribute drivers if the existing driver is damaged.

If the hard drive is lost, or if it is determined that the hardware platform should be replaced, the desktop restoration solution can help migrate the existing desktop to the new hardware without loss of personalization information. A configured desktop restoration solution can re-install the OS and applications, making adjustments to the new platform during the installation. This can make the process of moving between two dissimilar systems more reliable and faster.

One option is to migrate the desktop to a different, proven personal computer to get a working system back into the hands of a user as quickly as possible. Once they have the new system, the old system can be taken in for more detailed diagnosis and repair without imperiling the productivity of the user. Once the system is reconditioned, it can be used for the next user who has a system in need of repair.

Mitigating Site-Level Risks

All desktop restoration solutions ultimately store the data on the user's desktop in an alternative file storage location, typically attached to a server. If that server is stored in a different physical location than the personal computers it protects, it can be used to restore the desktops at a different location.

If all the desktops are lost, they can be restored once new hardware is located. If they are merely inaccessible, critical desktops can be restored to minimize the impact of lost productivity.

Designing a Solution

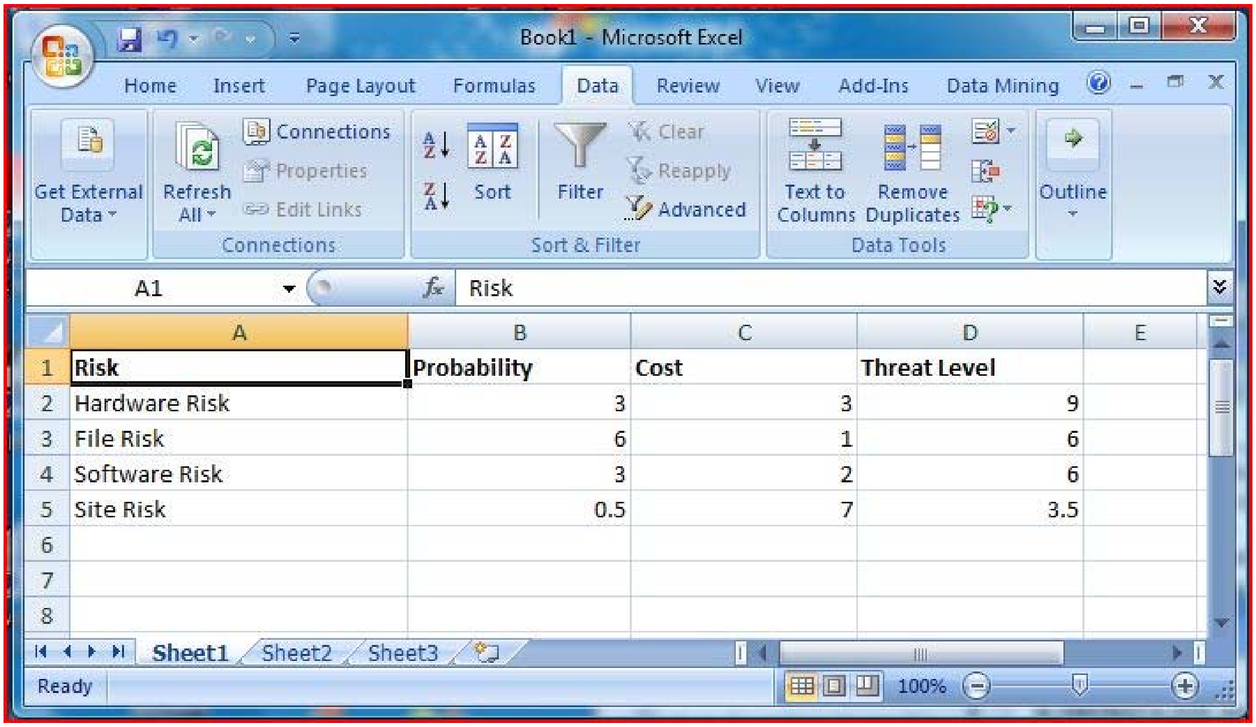
The design of a desktop restoration solution involves considering the risks and their mitigations as stated earlier. There are multiple solutions to each of the discussed risks. Differing mitigation strategies have differing associated costs. An effective desktop restoration solution must balance the cost of the system with an estimated return on investment (ROI).

Although the value of the desktop restoration solution beyond disaster recovery has been explored in the previous chapters, there is a point at which the solution should be reviewed as an insurance policy. The cost of the system must be balanced against the economic loss should a disaster occur.

Evaluating the Risks

Different organizations will have different levels of risk associated with their desktops. For instance, if an organization has a firmly established discipline of using a document repository to store the work product of its workers, file-levels risks may not be as important. If an organization issues primarily laptops as the personal computers used to host desktops, that organization's hardware risks may be elevated.

The first step in the design of the solution, then, is to determine the requirements. By denoting the risks particular to a specific organization, as assigning a relative number to the risk, they can be prioritized. One approach is to list the risks, assign them a likelihood factor of 1 (very unlikely) to 10 (virtually assured). Then assign a similar factor for cost of 1 (very little cost to recover) to 10 (very expensive to recover). Multiply the two factors to determine the overall threat value of the risk. Then sort the list in descending order. The following spreadsheet shows how this might be accomplished.



Formula bar: A1 | Risk

	A	B	C	D	E
1	Risk	Probability	Cost	Threat Level	
2	Hardware Risk	3	3	9	
3	File Risk	6	1	6	
4	Software Risk	3	2	6	
5	Site Risk	0.5	7	3.5	
6					
7					
8					

Figure 4.4: Threat modeling helps design the requirements for the desktop restoration solution.

This example is relatively coarse and simplistic. A more detailed breakdown of specific risks should be undertaken to provide more specific requirements. Once the requirements have been listed and prioritized, the solution can begin to take shape.

Choosing Mitigation Strategies

With a list of risks and their relative priorities in hand, the available solutions can be evaluated. Each solution should be evaluated based on its ability to meet the risks at hand. One may be better at handling file backup, another at support for desktop migration. With an understanding of the likelihood and cost of each risk, it becomes easier to qualify which solutions best handle each scenario.

The problem becomes more difficult when considering the cost of the solution, however. One restoration solution may cost only $20 per system on average, where another may cost $35. If the second can help in more areas of risk and reduce the time in which the systems it protects can be restored, it may well be worth the extra $15. The total cost to keep the desktop safe and workers productive will impact the bottom line of the entire organization.

The next step is to consider the value of other services that the restoration solution can offer. If the restoration system can provide value in other areas of the organization beyond disaster recovery, this added value should be considered. If the restoration solution can be used to help troubleshoot desktop problems, help identify hardware or software for obsolescence, and help maintain corporate compliance on the desktop, these additional services should also be considered when making the choice of the proper solution.

It is often difficult to quantify the value of the desktop solution. Most reputable vendors will have invested in case studies and development of objective evidence that shows the value of their solution. Third parties may provide studies that validate the claims of the vendor. Trade publications often provide evaluations and customer testimony as to the value of a solution. Often, current users of the system can be contacted to discover whether the system preformed as advertised. All these inputs help determine which solution is best for a specific organization.

A checklist of the solutions available should include the following considerations:

- The ability of the solution to mitigate the risks to the organization
- The total cost of ownership (TCO) of the system, weighted by the risks involved
- The added benefits offered by the system
- The quality of the solution, as validated by third parties and solutions users

Refining the Solution

The best solutions often come from a clear understanding of the entire solution—the policies, processes, personnel, and products that will be implemented to create and operate the solution. Before committing to a solution, a clear understanding of the entire scope of the solution should be drafted. Preliminary plans for policies that need to be implemented; processes that will need to be monitored; personnel that needs to be hired, trained, and retained; and the ongoing costs of the products should be carefully examined.

This step of mapping out all the elements of the solution serves as a double check before the solution is purchased. By thinking out the other portions of the solution beyond the purchase of the tools, management can better grasp the total scope of the solution they plan to craft. The key, prior to purchase, should be no surprises.

Implementing the Solution

Once the system is selected, it must be implemented. Although each individual system will have its own variations, there are some common factors that accompany all solutions. The processes used by the solution will impact the IT operational infrastructure. There are things that will happen on a daily basis that must be arranged so that they do not hinder existing activities. The solution should provide the full range of services as designed. Consider the steps necessary to put the desktop restoration solution in place and make it functional within the organization:

- Building a solution infrastructure
- Implementing the desktop backup processes
- Planning the desktop restoration processes
- Taking full advantage of the solution

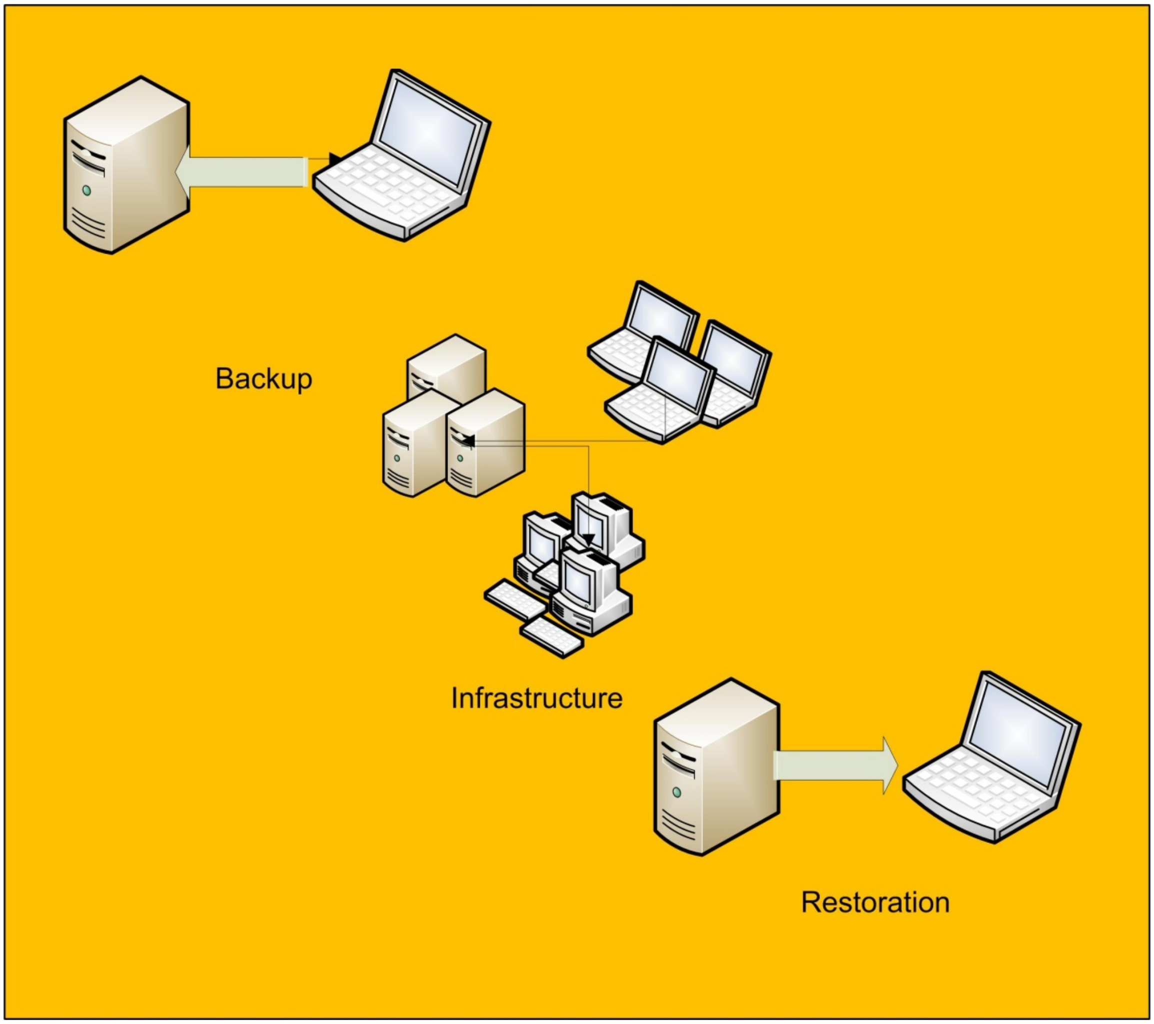


Figure 4.5: A well-executed implementation helps reap the full benefits from the desktop restoration solution.

Desktop Restoration Infrastructure

The desktop restoration solution will require an infrastructure on which it can operate. Each solution may use different methods, but there are common resources that will be implemented.

Servers

The solution will be required to store the data collected from the desktops. That typically requires a server and storage. There are several solution-specific considerations with the servers.

Some solutions require dedicated servers on which to run. Using a dedicated server may increase the TCO—not only the expense of purchasing the hardware for this use but also in terms of operating and maintaining additional servers. The use of the servers must be considered in the solution. For many organizations, the servers will see their heaviest use during non-peak hours when users are not actively using their desktops and the desktops are backing up their data. This is often a time when application servers are less busy because the users are not actively using them. A multi-purpose server that serves the applications during the day and desktop backup at night may be cost effective.

The location of the server is also relevant. If the servers are located at the same site as the desktop they back up, there is less protection for a site-level threat. Servers housed in a different site than the assets they protect can help mitigate additional risks.

Storage

Another consideration is disk storage. Backup of many individual desktops can take a considerable amount of space. The nature of the restoration solution will somewhat dictate this need. Some solutions make a complete copy of the hard drive. The amount of space and network bandwidth to execute such a solution can be prohibitive.

The desktop restoration's ability to optimize storage is a key factor in its ability to contain the TCO. The files should be stored as efficiently as possible. The other consideration is the ability to retrieve only the files required to execute a particular restoration activity, such as the re-installation of an application and re-application of its configuration.

Network

The backup and restoration of data from the individual desktops to the server will require network bandwidth. The use of this bandwidth must be carefully planned to avoid interruption of normal activities within the organization.

Most of the bandwidth used by the solution will be used for backup. It is best to perform backup when the process does not compete with the user for resources and when fewer files are open. For organizations that maintain typical business hours, this means backups will occur during non-working hours (typically at night). This also tends to be a time when less bandwidth is required, so it is good use of resources. Organizations that run 24-hour operations must carefully plan the use of the network to ensure that the backup of one set of desktops does not hinder another set of desktops from performing their tasks. If the backup of data is to a remote site, the affect on the wide area network (WAN) connections must also be considered.

Different backup systems will require different levels of data transfer. A system that requires only the backup of new files or files that change will use less bandwidth than systems that require wholesale backup of the data on the drive.

For organizations that have many diverse locations, consideration should be given to the placement of servers. If multiple servers can be placed at key locations throughout the organization, it may minimize WAN traffic, and thus reduce congestion and cost.

Packages

If the solution is a configured, installation-based solution, the individual components that comprise the desktop installation must be packaged. This requirement provides the restoration solution with the capability of installing distinct applications. In addition to allowing systems to be restored, it allows the distribution of new or updated software, and provides for future clean installs of the authorized software that composes the desktop.

If the restoration system is based on copying drive images, this step of the implementation is unnecessary. Image backups can only replace a copy of the hard disk data; they cannot flexibly install only the required portions of the desktop on demand.

The process of building the packages will vary depending on the tool chosen. It can be as simple as installing the application on a clean reference machine. The tool can monitor the changes made by the installation and automate the process of building a package that can install the application on any target machine. The packages can be used not only to perform clean restorations of the applications but also to build entirely new desktops as required. By performing a single installation, and recording the results, the tool any be able to reproduce that installation on any targeted system.

Agents

Most desktop restoration solutions will require the installation of an agent on the target desktop. The agents, once installed, will handle the scheduling of the backups of the individual desktops. The agents may also serve other purposes.

The agents will inventory the resources of the desktop. By keeping accurate track of the hardware and software within the desktop, they have the potential of maintaining an accurate inventory of both. This can serve to track assets and validate regulatory compliance. The information can be used to help troubleshoot systems and keep up-to-date on the system changes without maintaining excessive paperwork. And the agents can help ensure that the software licenses are accounted for and placed where they belong.

For most tools, deployment of the agent will be automated. Some tools will require that a list of machines be built in a database. Others will be able to query Active Directory (AD—or other directory listings of active computers on the network) for a list of the machines on the network. Almost all tools will have a provision for installing the agent manually on a machine.

An organization will need to determine the most efficient means of distributing agents for the initial installation. Once installed, the agents will be used to help inventory the system and manage the process of scheduled backups for the targeted desktops.

Desktop Backup

The protection of a given desktop is only as good as the last backup. Backup requires the cooperation of the users in concert with the careful scheduling of resource utilization to ensure that data is protected with as little disruption as possible.

User Policy

Scheduling is a two-faceted issue. First, the users must be cognizant of the scheduling policy. Although the collection of data can easily be scheduled to happen automatically, if the computer is turned off, the scheduled event will not occur. If the data collection attempt happens when the user is in the middle of work, the user may well cancel the event to prevent any deterioration in the performance of the desktop. There will always be some users who resist, and there must be a clear policy in place to help them succeed in protecting their data and workspace.

The issue becomes more complex with mobile computing hardware. Laptops and notebooks may not be connected to the network on a regularly scheduled basis. This may make scheduling the backup difficult. If users seldom connect, during the times of connection, they may object to devoting resources from their desktop to performing backups. They may not desire to stay connected long enough to complete the backup. If the users are remote and accessing the corporate network through a virtual private network (VPN) or lower-bandwidth connection, backups may take a considerable amount of time.

Consideration should be given to the restoration to determine how it can be used to minimize the time required for a backup, especially if the backup must be performed while users are performing other tasks. There is also a point at which, by policy, users should be required to allow backup of their equipment to occur.

Resource Utilization

The other element to scheduling is the use of shared resources. The servers that perform the backup, if they are not dedicated to this purpose, should cooperate with the other workload managed by the server.

Most servers will use a storage area network (SAN) to store the data. Most SAN arrays are shared among servers and must meet the needs of multiple workloads. Backups should be planned to work cooperatively with the SAN and place load on the SAN during times when the impact on other services will be minimized. Again, restoration solutions that minimize the amount of data stored and retrieved each night will help ease the competition for resources.

The other major resource to consider is the network. If the backups clog the network and prevent users from being productive, the backup will add expense to the organization. This can be more critical if the backups are moved across limited, higher-cost WAN links. Solutions that can run automatically during non-peak times, and solutions that minimize the amount of data transferred, will help ease many of these issues.

Archive Policy

As backups accrue, so does the space they consume. Even using configured desktop backup solutions, the size of user data will continue to grow. A policy must be established to determine how long copies of data will be kept, and how many version of the files will be retained.

As users re-organize and "keep up" their desktops, they move and delete files. To most desktop restorations solutions, deleted files can be marked in the system but are not deleted from the backup copy.

> 💣 An image-based backup system will not preserve deleted files, as these files are no longer part of the hard drive. Thus, if a file is accidentally deleted and the backup image replaced, the file is lost.

IT must work with the tool to determine how to handle deleted files. The files can be deleted from the archive to save space or they can be retained for a period of time. They can also be archived to long-term storage. This policy must be established so that the process of dealing with deleted files can be configured within the system.

Restoring the Desktop

The process of restoration is somewhat dependent on the type of desktop restoration system implemented. If the system is dependent on the restoration of a complete drive image, there is little flexibility to be had. In the event of a disaster, the entire drive must be restored.

If, however, a configured desktop restoration solution has been implemented, several restoration scenarios open up. These expanded restoration options allow a more flexible approach to restoring the desktop, especially if the entire system or hard drive is not lost.

File Restoration

If all that is lost is a single file or folder, certain desktop restoration solutions allow the restoration of just the missing files. This is expedient and helps protect users from inadvertently deleting valuable work artifacts. It can also protect from files becoming accidentally damaged or altered.

Application Re-Installation

If the only issue with a desktop is an errant application, the application can be re-installed by a configured desktop restoration solution. The re-install will replace the application binaries and restore the configuration and customizations associated with the application.

Application patches can be applied in a similar manner. If an application patch or upgrade goes awry, the new software can be uninstalled and the previous version reinstalled using the previous installation package. This helps protect the desktop from losing the application. And sometimes a clean re-installation of the older version of the application paves the way for a clean patch installation or upgrade.

Hardware Changes

If the restoration of the desktop requires the modification of hardware, there are drivers and support applications that will need to follow the change. A configured desktop restoration solution can make that software readily available to the technical staff. It makes the changes go swiftly and minimizes human error.

Administrate the Solution

Most organizations carefully consider the cost of purchasing a desktop restoration solution. They count the price of the software, servers, storage, and other bits of hardware they will need. Many organizations will capitalize such expenses, and thus want to minimize them so that they appear to have less impact on the bottom line of the organization.

But the real value and cost of the solution lies in how it is used day-to-day. Many backup solutions are purchased and then left to languish because there is no staff to maintain the system or ensure that it is operational and doing its job. Some lower-cost solutions cut corners on initial cost by moving burden to the individual users to be disciplined to perform their own backups and monitor their success or failure. Still other organizations surrender the value of the solution by not being able to effectively perform restorations as required, even if the backups exist.

A well-designed solution should be simple to monitor, easy to use for restorations, and flexible when changes occur within the organization. If the solution cannot be operated and maintained easily, it will soon lose its value to the organization.

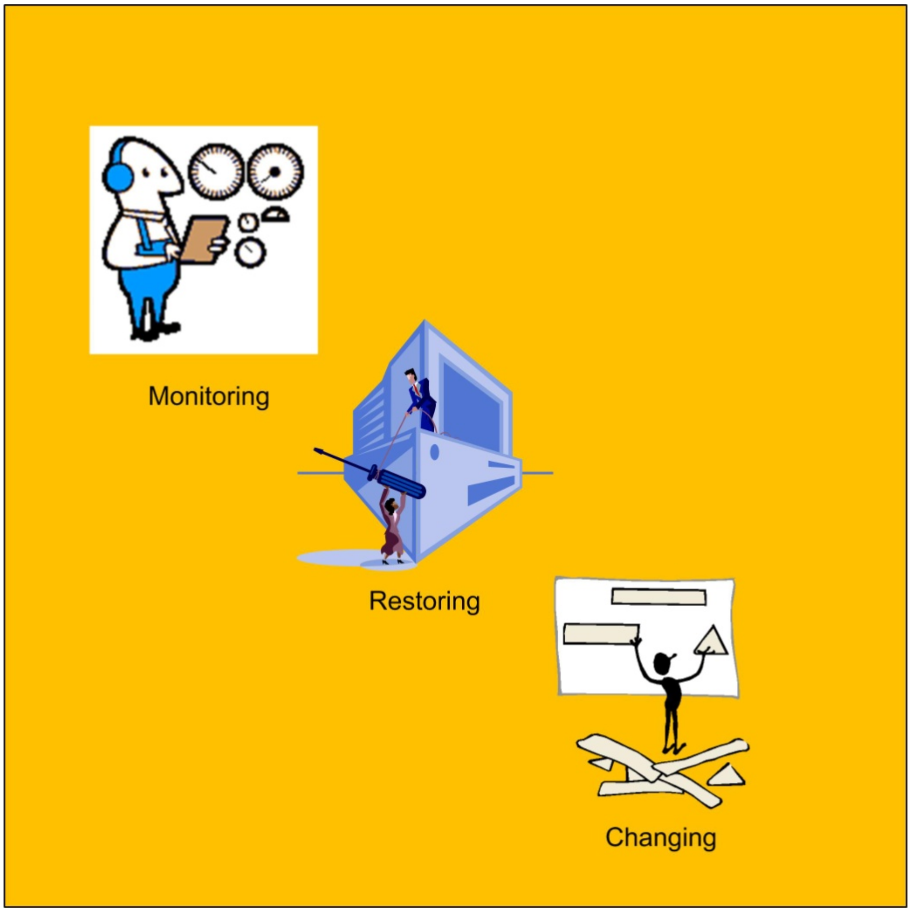


Figure 4.6: The true cost and value from a solution are measured in its ongoing use.

Monitoring

Monitoring backups is a tedious task. It is easily overlooked. It really is not important until a disaster occurs and then it is discovered that the lost desktop has not has a recent backup. Monitoring also involves keeping track of the infrastructures components—in particular, the storage systems used to safeguard the desktop data.

Desktop Backup Monitoring

Monitoring must be overseen by someone who is empowered to take action to ensure that backups can be successfully captured. Those who monitor the solution should be able to discern the cause of the failures, whether it is technological, such as a bad backup agent or network connectivity issue, or whether it is a matter of user non-compliance.

A missed backup here or there is likely not an issue. (Of course, Murphy prefers to throw his wrench into systems that have not been backed up.) A policy that clearly defines the organization’s tolerance for missed backups and steps used to correct missed backups will help smooth operations.

The quality of the desktop restoration tool also plays into this. The ability to remotely administer the agents located on the desktops and adjust schedules easily to match changes in conditions within an organization can help ensure that the data is backed up. Several steps can help reduce these hurdles:

- Minimize the impact that the backup process has on users
- Help users overcome difficulties they experience in complying with the backup policy
- Ensure that no technology issues prevent the backup from occurring (firewalls, network bandwidth issues, and so on)

The true cost of the solution, in this case, is impacted by the ease or difficulty in assuring the backups are secured. Policy must be created to ensure that the backups are collected. Most tools will make sure that a process exists to automate the process. People must be tasked to enforce the policy and oversee the process. And the product selected to perform the backups must be robust enough to meet the needs of the organization.

> Some organizations provide their users the ability to backup manually but do not enforce the backup policy. This has little cost until a restoration is requires and no backup exists (Murphy likes to choose the unprepared as his victim). The cost of this sort of restoration solution can only be measured in the lost work and productivity incurred from such a breach.

Infrastructure Monitoring

In addition to assuring that the individual desktops are backed up, the infrastructure components should also be monitored. This includes monitoring the servers, shared resources, and time to perform the entire backup

Servers

The servers must be kept operational for the backups to run. Although most restoration solution components are quite stable, they should not be ignored. The most common issue is a lack of drive space to store the backups.

Drive space should be monitored on a regular basis and changes to the space considered. As will all things involving archives, the amount of space required and the space consumed will grow consistently. The growth of space will depend on the restoration solution employed. Systems that minimize redundant storage of data (such as OS and application binary files) will require less storage.

The other step that will affect the total space used is the archive policy. The length of time that deleted files are kept online will determine how much space will be required for backup storage. If files are moved to offline storage, systems to track where the archived files are stored will depend on the tools and processes used by the solution.

Shared Resources

Some desktop restoration solutions can share servers with other applications. This is advantageous for reducing hardware and software licensing costs and making efficient use of IT resources. When this is the case, it is important to schedule backups during times when the other application services are in a period of limited demand. This will minimize the impact of the backup on the organization's application infrastructure.

The key resource to consider is the network. By their nature, backups are best performed during times of reduced user activity (after business hours). When users are not actively using their desktops, there is typically more local bandwidth available and thus less business impact.

The desktop restoration solution itself impacts this as well. Solutions that back up only the minimal daily changes made to the desktop will transmit less data and thus impact the shared resources in a reduced manner.

✎ For organizations that run 24 × 7, backups may be required while users are actively using their desktops. For such circumstances, solutions that minimize the time and resources spent copying changed data may be the only practical answer.

Time

The total time required to perform the backups may also come into play. For most organizations, there is a window of time during which the backups should be performed to minimize impact. If the time required to perform the backup exceeds that window, it will begin to impact other business activities.

Many desktop restoration solutions can be distributed so that the backups can be performed in parallel. Particularly solutions that can use shared servers are attractive because more servers can be used to collect the backup data simultaneously. This shortens the total window.

✎ Distributing servers at key points within an organization's network infrastructure can also help contain network bottlenecks. Locating servers on key subnets can reduce network congestion and help control the utilization of WAN links.

Organizational Changes

Organizations change over time. They move from one facility to another. They open new facilities. They acquire companies and need to expand and integrate their operations. These changes can have a direct impact on the operation of the desktop restoration solution. A well-conceived solution will make expansion and reconfiguration to meet these changes smooth and efficient.

There are several considerations that must be made to meet the requirements for changes in the organization. First, the software requirements are seldom constant. This will necessitate testing and configuring the system to accommodate different software. For a configured restoration solution, the ease at which packages for new software can be implemented plays a key role.

Changes in site and network configuration should be assessed. If a new site is added to the organization, what is the impact of the changes to the solution? The cost of taking restoration management of a large number of desktops should be considered one of the costs if the organization is growing, opening, or acquiring new facilities or rapidly expanding staff needs.

The solution should be dynamic and allow the addition of servers and collection points to facilitate the growth of sites. The overall capacity of the solution should be considered. The overall administration of the solution can come to play in this. How easily is the solution administered as it grows? Can multiple, independent locations be managed from a single location? The cost of personnel to oversee the solution and the level of automation it employs will strongly affect the value delivered by the system.

Another consideration is the overhead of bringing a large number of new desktops into corporate compliance when an acquisition occurs. This can span obsolescing software packages, removing unauthorized or unlicensed software, and rapidly deploying new applications without destroying the personality encapsulated on the existing desktop.

✎ A solution that can inventory desktops and re-install corporate-compliant desktops can be a great boon to an organization that makes an acquisition.

Leverage the Solution

The key use of a desktop restoration solution is to protect the work artifacts and productivity of the users of those desktops. Although the solution should always protect those objectives, there are many other benefits that these solutions may offer. To receive the full benefits of the solution, the organization should consider these benefits and determine what value they may provide.

The first step is to use the solution in the manner in which it is designed. When personnel change who do not know how to leverage the solution or who have their own means of accomplishing tasks, they may begin to shift away from using the solution. Perhaps as the solution is first rolled out, portions are not used (such as desktop re-platforming). When the time comes to use the solution in that manner, it may not be used because the technical staff is unfamiliar with the process. Diligence is required to demonstrate the value of the solution and use it to its fullest potential.

Although each solution will vary in the benefits that it offers, there are some additional features that can add a great deal of value. These, and other benefits, should be considered as the solution is designed, implemented, and used each day.

Figure 4.7: Leveraging all the value of the solution reduces its overall cost.

Inventory

Most organizations work to comply with software licensing laws. But it can be difficult to manage software assets. Systems are required to track licenses. There can be significant cost savings by re-allocating licenses removed from one desktop and then applied to another.

A desktop restoration solution that manages the software on the desktop can detect unlicensed and unauthorized software installed on that desktop. It can be used to keep an accurate inventory of the licenses currently installed. It can also provide detection of unauthorized software installed on the desktop.

Distribution

A configured desktop restoration solution can be used as a tool to distribute OS patches and upgrades, application upgrades, and distribution of new applications. It may work in conjunction with the inventory system to track where those licensed are installed.

The desktop restoration solution can be used to build new desktops by distributing the software used on them. This allows for flexible distribution of software when it is purchased or rapid re-configuration when companies are acquired and new desktops are added to the environment.

It can be used to migrate desktops from one hardware platform to another (for more information about this, see Chapter 2). It allows the desktop to exist as a flexible collection of digital entities that can be materialized on any required platform with network access.

Compliance

A solution that tracks inventory and can distribute software can be used to ensure that desktops remain within corporate and regulatory compliance. The inventory can make sure that the software on the desktop is the software that is supposed to be there.

A configured desktop restoration solution can also be used to return a system to compliance. It can be used to re-install the desktop software, including only those elements that are in compliance. This simplifies the process of keeping the desktops safe and the organization legal.

Summary

In the information age, much of the work performed by employees is stored on their personal computer desktops. The product of their work is often files that rest on the hard drive. Their ability to interact with other systems within the organization is a set of software applications, network access, credentials, and other elements of that desktop. If the desktop fails to serve the employee or the work files are lost, it has a direct impact on the employee’s productivity and the bottom line of the organization.

A desktop restoration solution that can capture and protect the work environment of the user can mitigate the risk of lost time and work for their workforce. A flexible, well-designed solution can go beyond the bounds of simple file protection and add value to the hardware and software life cycle management in the organization.

The solution is a confluence of policy, processes, personnel, and products. When these are brought together through careful planning, implementation, administration, and ongoing improvement, they can protect the assets and productivity of the organization’s workforce.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.