

## Desktop Management: Saving Your Small Business Resources!

By [LP Morton](#)

### Introduction

Personal computers have delivered on the promise of productivity for knowledge workers. As a consequence, desktop and laptop computers have proliferated to almost every knowledge worker in a company. Advances in network bandwidth and the availability of wireless connectivity options have radically increased the number of home and remote workers. However, the increased use of personal computers and remote access has added significant workload and coordination to the already busy IT schedule.

For many companies, desktop management is not a core competency and there are other IT tasks that are considered mission critical or more strategic. Yet for many knowledge workers, the desktop is mission critical. Schedules, correspondence, contact lists, presentations and work in progress all live in the desktop for most office workers. Take away the desktop and work stops until the desktop is back up and running.

Most small and medium businesses do not have the IT staff and tools to treat desktop management issues with the attention they deserve. IT shops in small and medium sized companies are generally over-taxed and doing the best they can to keep the IT infrastructure running smoothly. Budgets are much smaller than those of their large enterprise counterparts, staffing is limited, and toolsets are few and far between. Too often manual processes and “just enough to get by” scripting is the answer to desktop management in the small and medium sized company. Individual users can be left to handle minor issues for themselves, and pseudo power users often get themselves into trouble and require IT staff assistance to resolve problems they have created through their self-help efforts. It is no longer a viable answer for small and medium sized business to treat desktop management casually.

### Importance of PC Management

The task of PC management has become too large and too important to be handled on an ad-hoc basis with limited tools. The number of personal computers is significant. There are many versions of operating systems and many different software applications. This is also complicated by the number of employees working from remote offices. The scale has become rather large, even in a small to medium sized business. Now add in the constant stream of Microsoft patch updates (security, operating system and application software updates), periodic operating system upgrades, user initiated software installations and configuration changes, antivirus updates, and IT configuration changes. The rate and volume of change is significant, if not overwhelming. Not to mention the problem of Microsoft phasing out their support of old office applications and operating systems. Windows 95 is no longer supported and 98 is now no longer going to be supported.

The risks of doing a poor job of desktop management are now quite high given the security risks to every PC every day. Left unprotected, PCs are subject to Trojans, Keyloggers, Root Kits, Spyware and Viruses. One of the best ways to be protected is to apply all patches to operating systems and applications in a timely fashion. However, coordinating, staging and testing these patches is time consuming and something that should not be left to end users or ad hoc processes by the IT team. Every desktop needs Anti-virus software that is constantly updated, and users cannot be trusted to keep their virus data files current. Mobile users should also be protected with personal Firewall software, but again, users cannot be depended upon to install and keep such software current. Leaving this to chance can put the entire network and subsequently the entire company at risk. The employee desktop today contains significant corporate data, both data taken from corporate repositories for use on the desktop as well as work-in-process data not yet stored on a secured and backed-up repository. Employees handle important and sensitive data that needs to be protected. This can include price lists, customer lists, customer data, human resources data, strategic plans, product plans and corporate financial information. Security breaches, viruses, and spy-ware can lead to stolen, lost or corrupted data. Regular backups can mitigate the risk of lost or corrupted data, however most users are not disciplined enough to perform regular backups. Mobile and remote users complicate the backup problem and render home-grown backup scripting ineffective.

Dealing with the disruption and potential data loss of security breaches can represent significant productivity loss. Work-in-process data on the desktop can represent weeks of effort and may be difficult or impossible to recreate. The loss of such data can affect project time-lines, which in turn can cause customer satisfaction issues and/or contractual penalties. Desktop data loss can also affect revenue if a desktop problem interrupts critical timeframes for customer proposals.

Another factor driving the need for good desktop management is the increasing regulatory compliance issues that are affecting businesses of all sizes. Consumer and patient privacy laws such as HIPAA (Health Insurance Portability and Accountability Act) and the wave of trend setting privacy laws out of California affect businesses of all sizes. Sarbanes-Oxley compliance includes rigorous asset management, change management and other controls for IT. This should be of concern for more than just the public companies covered by the law. Many small and medium sized businesses are working toward an eventual acquisition as an exit strategy, and most such acquisitions are by companies that are subject to Sarbanes-Oxley. It is much easier and faster to work through the due diligence phase of the acquisition if the company being acquired has implemented the types of controls required by Sarbanes-Oxley. Good desktop management can assist a company in certain aspects of regulatory compliance.

#### Effective PC Management

Effective PC Management begins with knowing what you have to manage. Complete and accurate asset and license management is key. Knowing how many machines of what type, their location, memory, hard drive, processor speed, etc., is a big step forward for many small and medium sized businesses. Tools available today have automatic

discovery capabilities and excellent management reporting which can assist IT staff in establishing and maintaining good processes for asset management. With an accurate picture of the installed hardware base, it becomes much easier to assess operating system and business suite software upgrades.

Keeping track of software licenses and where they are installed is another important function. Accurate information of which machines have which software installed is a major starting point to effectively manage PCs across the company. This information can minimize the number and duration of on-site visits by IT support personnel. It can also ensure that software licenses are appropriately managed; paying for only those copies of a particular software that are needed and reducing the risk of fines in a software license audit.

Another good practice is to keep software installs to the minimum required for each employee to do their job. This will shorten install time, reduce updates and patches required, and use fewer resources leaving more capacity for each user's needs. Some systems administrators will attempt to make things easier by standardizing the desktop to one image for everyone. PC management is one place where "one size does not fit all." Overcomplicating the software image for every user by installing all applications everywhere will increase work in the long run and make everyone unhappy. A better practice is to define unique user types by department or job function, and to define a standard image for each user type. This can limit the time to upgrade applications and allow for better service for each user.

With an accurate inventory of all hardware and only the software needed on each desktop, the next step toward effective PC management is to automate software distribution. Automated software distribution minimizes the number of onsite visits IT staff must make. This lowers the cost of support and allows for more frequent updates. This can be applied to virus data files, operating system patches as well as updates and new versions of application software. Changes should be staged in a separate environment for testing and then rolled out based on individual or group user profiles.

Automated software distribution is the first step in remote management. Full remote management includes the ability to remotely control the desktop and make all required configuration changes through a networked connection. This is a critical function as the number of remote and mobile workers has increased. IT staff must be able to perform administrative functions from their office as if they were sitting in front of the PC of remote and mobile workers.

When considering how to implement desktop management best practices, companies need to acquire management tools to automate the management tasks. Companies can license tools and build an in-house management infrastructure, access management tools through a hosted Software as a Service (SaaS) model, or outsource the entire desktop management process. Each of these alternatives is explored in more detail below.

Alternatives for Acquiring Good Tools:  
Build, Software as a Service, Outsource

A company with as few as 2-20 employees can struggle with manual desktop management processes. The more

desktops to be managed and the more mobile and remote workers to support, the more difficult it becomes to deliver good service with manual processes. The severity of issues that can arise from poor PC management requires that the problem be taken seriously and therefore automation should be given significant consideration.

There are now many options available to automate some or all of the PC management functions, and some of these options are cost effective even for small and medium sized companies. However, tool selection should be made carefully to ensure that the necessary functions are addressed by the tool, to keep training time to a minimum and to avoid selecting a tool that requires more effort to administer than it saves. As with any decision, all of the alternatives should be considered before making the decision. PC management is no different, and it can be accomplished through several approaches: management tools deployed in-house to internally manage PCs (the “build” approach), using a Software as a Service hosted management tool with internal staff, and outsourcing the management of PCs to a third party.

#### Building an Internal PC Management Infrastructure

This traditional approach to management involves identifying tools to purchase, purchasing those tools, deploying the tools, training IT staff on how to effectively use the newly deployed management tools, and staffing sufficiently to manage the PC infrastructure on an ongoing basis. One of the advantages of this approach is that the IT organization retains full control of the management infrastructure and functions because the solution is an internally deployed solution. However, the control also brings with it the responsibility to manage the management system/software itself.

The build approach typically requires a larger initial budget outlay for purchase/licensing costs, with on-going maintenance fees, and any investment in additional hardware that is required to run the management infrastructure. In addition to these initial licensing costs, it is also important for IT organizations to realize that there is an associated cost of management. The IT staff is naturally responsible for managing the IT infrastructure, but in addition, they are also responsible for managing the IT management infrastructure itself. For example, in the case of internally deployed management software tools, these costs reveal themselves in deployment costs of the management tools, maintenance of the management tools (upgrades, patching), support personnel for ongoing operational support, management tool consulting services, training, software licensing costs (both initial purchase and recurring maintenance costs), hardware costs for additional hardware that is required to run the management software, and the cost of integrating tools in-house.

The cost of management depends on several factors; the ease-of-use and ease-of-deployment of the management solution, the stability of the management code, the frequency of new releases, and the maturity of the IT organization. Most of these factors translate to IT staff time that is required to manage the management infrastructure. In

addition to these direct costs, maintaining a help desk to assist users with PC issues is another additive cost of management. For geographically dispersed companies, the help desk may be required to operate 24x7, which adds significantly to the cost of ownership.

#### Software as a Service

Another way for IT organizations to employ PC management functionality is through management software delivered as a service. This option shifts the responsibility for the management software deployment and maintenance to the service provider. Software as a Service (SaaS) results in eliminating the following costs for enterprises: deploying the tool, maintaining the tools, consulting services to deploy the tool, software licensing, internal tool integration, hardware to run the management software, and troubleshooting when the tool is not working properly. Instead of these costs of ownership, the cost of the hosted software is in the form of fixed monthly subscription fees.

PC management SaaS can bring additional advantages beyond the features of the tool. Virus protection and automated update of virus data files is a feature often available. Some services include significant coordination of new patches; simplifying the staging, testing and deployment of patches. The service may include automated backup and offsite storage features providing excellent data protection with little additional effort or hardware costs. Hosted software solutions also provide news and information on new practices and trends which can assist the small to medium enterprise IT staff.

Some IT departments may be concerned over the loss of control by using a management infrastructure provided as a hosted service. The quality of the service provided must be excellent and the reputation of the service provider is critical. However, only the infrastructure itself is under third party control in this alternative. Company IT staff remain in control of the actual end user interface and the actual processes and actions taken on individual desktops.

The SaaS model provides access to a full suite product without the upfront license and setup costs. It allows the IT staff to maintain control of the desktop management process without the effort required to setup and maintain the management environment. It does require training and good internal processes. It also requires a way to track service requests and problems. To provide effective support, a help desk is useful, and for some companies a 24x7 help desk is necessary.

#### Outsourced PC Management

The point of acquiring good PC management tools is to provide effective PC management. There are a number of full service outsource options available to small and medium sized businesses for desktop management. This alternative solves the effective PC management problem by turning the work over to a service provider. The service provider is responsible for tool selection, deployment and operation. The service provider also brings trained staff and proven procedures.

Like the SaaS model, the outsourced model eliminates the costs of licensing the management tool, deploying the tool, consulting services to deploy the tool, integration

costs, maintenance costs and hardware costs. Additionally, the outsourced model eliminates the costs of internal staff for PC management and the costs of an internal help desk function for PC management. Outsourced PC management is typically charged on a per desktop per month fee. It is more expensive than a SaaS model as the service includes the staff and the help desk functions.

Outsourced PC management brings good tools and good processes to the problem of PC management, protecting the assets of the company while providing professional performance enhancements to maintain top performance expectations from the PC. Some businesses have experienced higher individual user costs for desktop management as individual users can spend more time attempting to solve their own problems rather than look to the third party provider for help.

The quality of the service delivered by the service provider must be excellent, and the services must be flexible enough to fit in with the way the company works. A collaborative working relationship must be established. This can require a different kind of management oversight than exists in some small and medium sized businesses. An outsourced service may bring improved service by providing a 24x7 help desk, a tremendous resource saving feature for a small business productivity need.

#### Morton & Morton's Perspective

Desktop Management is a critical business practice that, when done well, can keep employees productive and keep external threats to the company network in check. The traditional approach to managing PCs has been to deploy the management software in-house or use manual methods. Most companies now realize that manual efforts are no longer viable given the number of desktops, the frequency of changes and the risks to employee productivity and data. However, outsourcing the process to a competent third party company is by far the best method to reduce the cost of the company's resources and protect the intellectual assets of the company at all times.

We will provide you the best protection of your assets and reduce your small business resource requirements to manage the desktops and keep the performance level up the expected user level for the best productivity and do it at a cost that you can afford.

L. P. Morton, Ph.D.  
Morton & Morton Inc. ([www.morton-morton.com](http://www.morton-morton.com))  
820 Northwood rd.  
Fort Worth, Tx 76107  
817-625-5980  
[drmorton@swbell.net](mailto:drmorton@swbell.net)

Larry P. Morton, Ph.D. President Morton-Morton Inc. <http://www.morton-morton.com>

Article Source: [http://EzineArticles.com/?expert=LP\\_Morton](http://EzineArticles.com/?expert=LP_Morton)