

Confessions of a **Help Desk** Informant

5 Hard Truths

(and why nobody wants to talk about them)

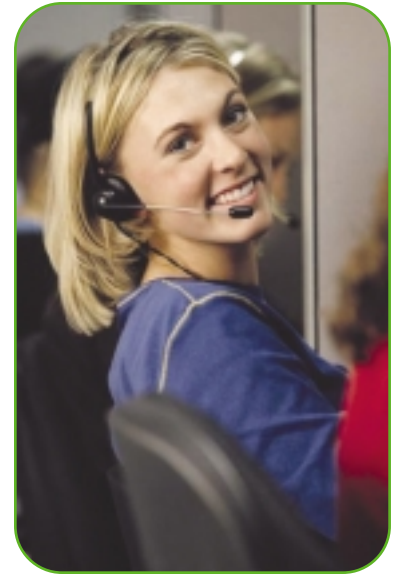


Confessions of a Help Desk Informant

The IT Help Desk serves a critical need in today's corporate environment. Business computing technology grows more complex and widespread every day, and a company's success depends on the support the Help Desk provides.

Despite its importance, the Help Desk is under fire in most companies. As workers become more dependent on their computers, the Help Desk's responsibility grows. As technology advances, providing support becomes more difficult. And under intense cost-cutting pressures, the Help Desk is asked to provide more services with fewer resources.

This booklet examines five hard truths facing the Help Desk organization—and a new generation of support technology that is improving the performance and productivity of the Help Desk and the people they serve.



Five hard truths about the HelpDesk

The issues facing the Help Desk pose some hard truths for most companies. The company's expectations often exceed IT's ability to deliver, and since these issues are difficult to address in the normal course of business, they're often downplayed or ignored. But they must be resolved if the IT organization is to provide the solid, cost-effective support the company needs. Let's take a closer look at five of these hard truths—the expectations within the company, the reality within IT, and an example for illustration.

Despite its importance, the Help Desk
is under fire in most companies.

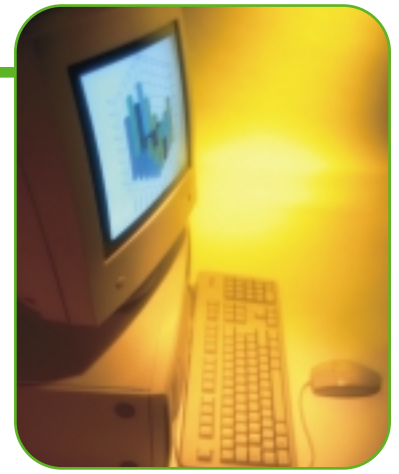
Truth 1

Current metrics do not enable IT to align its efforts with the business.

The company expects that the IT organization uses powerful technology and tools to track the user problems it handles, to identify ongoing IT problems in any area of the company, and to generate reports showing how well IT is addressing all these problems. This enables IT to focus its efforts on the problems with the biggest impact on the business.

In reality, IT deals with many user problems “outside the system,” so a significant portion of IT’s problem-resolution activity goes partially or entirely untracked. Also, many hidden costs of user problems aren’t recorded, such as user downtime and time spent by IT, users and co-workers to recover and recreate lost data.

In addition, the reports produced by current tools generally focus on Help Desk-related metrics (like abandoned rate and time in queue) rather than metrics related to the company’s business. Since IT doesn’t have sufficient resources to handle all problems immediately, it must prioritize—and since its metrics don’t enable them to identify problems with the biggest impact on revenue generators and other key business drivers, IT gives top



priority to problems that affect large numbers of users, are reported by VIPs, or simply seem critical.

Claudia, the CEO’s admin, found that her computer was acting up—running slow, freezing up, losing files. She asked Jack in the next office, who seemed knowledgeable about such things, for advice. Always eager to help, Jack spent an hour confidently adjusting several obscure system settings while Claudia watched helpfully over his shoulder, but to no avail.

Not one to bother with the Help Desk, Claudia called Chad, a friend in IT, directly. Chad abandoned the laptop he was working on for Sarah in Sales and rushed to the aid of the CEO’s admin. After readjusting several obscure system settings, Chad determined that Claudia’s hard drive was faulty. He spent the rest of the day replacing the drive and rebuilding the system. Over the next several days, Chad spent many more hours restoring Claudia’s familiar work environment, and some of her co-workers spent time searching for copies of missing files he might have sent them.

In the end, Claudia, Chad and others spent more than thirty hours trying to fix her system. None of that time was recorded anywhere. And Sarah in Sales was very upset that IT didn’t have her laptop repaired in time for her big client presentation.

IT’s metrics don’t identify problems with the biggest impact on key business drivers.

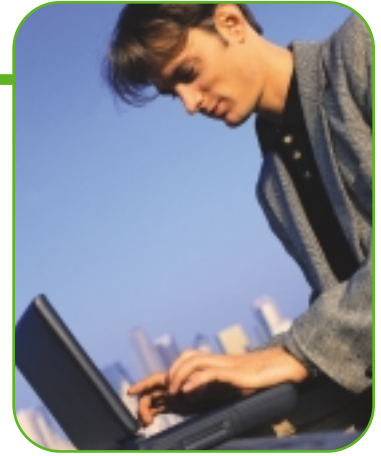
Truth 2

The company's mobile workforce poses a major IT risk to the company.

The company believes that the proliferation of mobile computing devices has enhanced the effectiveness of the mobile workforce and integrated their operations with the rest of the company. In the company's expectations, IT supports these mobile devices in much the same way as desktop PCs, resolving problems as they arise. The company's "hot spares" get users back in operation very quickly when laptops fail.

The reality is very different. Despite various types of remote connections (WAN, Internet, dial-up, etc.), mobile workers' computers are isolated from the rest of the company much of the time, and particularly from IT support. As a result, their hardware, operating systems and user data are generally underprotected. IT relies on them to manually back up their data to the corporate server or portable media, but this is typically done rarely if at all, and even the most conscientious worker can't protect the system's "personality" — network and printer settings, application and desktop settings, favorites, shortcuts, bookmarks, templates and so on.

Recovery is a problem as well. On the road, recovering from a problem bigger than a lost file is often impossible. And even when they get back to the office, users often resolve major problems by simply giving up their familiar machine for a replacement from IT and recover their data as best they can from portable media. These users typically spend a great deal of time recovering lost files and restoring the system's personality—and make many calls to the Help Desk in the process.



And even simple problems can persist for months, impacting users who are afraid to try to fix the problem or who don't know (or are embarrassed) to ask for help.

Leslie arrived in London on Sunday, with a big client demo to give in the morning. Out for a tea-time stroll along the Thames, she took some nice pictures with her new digital camera. That evening, back in her hotel room, she installed the camera software on her laptop to download her photos. But when she checked her demo application, it wouldn't run. She uninstalled the camera software, but the application was still dead.

Back at the home office, the Help Desk was closed for the weekend. Leslie managed to reach her boss at home, and she promised to find a technician to help. The technician called at midnight. He spent the next two hours researching the knowledge base on the camera vendor's site and talking Leslie through some possible solutions. Unfortunately, with the short time and great distance, none of them was practical. The technician assured her that he would continue searching for a solution and bade her good-night.

It was late, but Leslie wasn't through. If she couldn't actually run the demo application, she could create a presentation to simulate it. She worked till dawn building slides to illustrate product functions. Exhausted but determined, she did her best in front of the client. Their reaction was polite: "Thanks ever so much, but we really need to see a demo before we decide. Can you come back next week?" Of course she could; what's one more transatlantic trip? That would give her time to get the demo working again. Too bad it would push the sale past the end of the quarter.

Truth 3

IT's backup system cannot completely restore a user's system.

In the company's expectations, its backup system protects corporate data and users' systems effectively. When problems happen, individual files or entire systems can be restored from backups with relatively little loss of data or time.

In reality, at many companies, the backup system relies heavily on individual users, requiring them either to back up important files manually to the network or portable media, or to store files in specific locations on their PCs for automated backup. Either way—even for users who do this faithfully—much of each user's system remains unprotected.

Recovery is problematic as well. Recovering individual files is often difficult, especially from tape, or when the exact filename or date is unknown. Recovering a lost system can be much worse—the system is typically not recovered, but is instead rebuilt from scratch by cloning a system image, reinstalling applications, recovering user data from backup, and manually restoring the machine's personality.

The impact of this incomplete protection on employee productivity can be enormous. IT personnel and users may spend several working days restoring a machine—multiplied many times when a virus, theft or natural disaster affects many machines.

Factoring in the accompanying loss of business opportunities, the shortcomings of the backup system can pose a significant threat to the company.

The coffee machine was a popular spot that Tuesday morning—no point in sitting at an empty desk. Besides, the police were checking for prints, so best to stay out of the way. The thieves had found a service door propped open and had gotten away with ten machines. The company's computer vendor delivered replacement machines on Thursday (at premium cost), and by the end of the day Friday, the IT staff had reloaded the standard OS and applications and restored everyone's data from backup. John, the IT manager, beamed with pride at the quick recovery.

Well, not quite. Monday morning, the IT staff was back, setting up e-mail and Internet access on the new machines, connecting them to network drives and printers, and reinstalling specialized applications. But after lunch everyone was hard at work again—personalizing their office applications, redefining their bookmarks and favorites, setting up their desktops, recreating their document templates, and on and on.

That afternoon Stephen discovered that he was missing his deliverables for the big McWhirter account—due the next day. Turned out he hadn't been storing them in his My Documents folder, so they were never backed up. Ditto for Barbara, his teammate on the account; distrustful of network backups, she carefully copied her files to a Zip disk, which she kept safe and sound in the drive attached to her machine. When the company missed the delivery and lost the account, John the IT manager was quick to point out how Stephen and Barbara had failed to do their part in the backup process. Unfortunately for John, the CEO didn't see it that way.

The shortcomings of the backup system can pose a significant threat to the company.

Truth 4

Migrations and upgrades are a big headache, for both users and IT.

The company expects that IT minimizes the disruption of migrations and upgrades by thoroughly reviewing and testing new hardware, operating systems and application versions beforehand. IT performs migrations and upgrades in an orderly, nondisruptive way. User data and other information are generally transferred smoothly. Users are back to work quickly, and the Help Desk is available to resolve any problems that may arise.

The reality is that migrations and upgrades typically have a major impact on both IT and users—in fact, many companies are reluctant to upgrade, despite the benefits, precisely because of the disruption it causes. This is not to say that IT doesn't make a good effort to keep disruption to a minimum by testing new products and rolling them out in phases to reduce risk. However, incompatibilities and other problems associated with new products are hard to anticipate fully, and many risks are inherent in the process.

In particular, data is often lost because of the difficulty of transferring it to and from temporary storage before and after the migration, and of coordinating this transfer with the migration process and users' normal work activity. In addition, for a migration to new hardware or operating system, the personality of the user's machine is typically lost, requiring each user to spend hours restoring it manually. And the Help Desk lacks the resources to help large numbers of users resolve these and other problems immediately.



Ed was managing the migration of 1,000 employees from Windows 95 to Windows 2000. Having been through this before, he laid in wholesale quantities of instant noodles and invigorating soda for his team. He divided the employees into groups of 100, planning to move one group a week to make sure that each move was complete before the next one began. He told the first group to "clean up their files" in preparation for the move. A few accidentally deleted valuable data in their zeal; others made up for this by doing nothing at all.

When the rollout began, his team worked with the employees one by one to copy their data files to the server, dutifully advising each one to be sure to remember where everything was stored or data could be lost. During the preceding weeks, the team had prepared for the migration by creating images of Windows 2000 and many combinations of applications for various hardware platforms; now they cloned the images to the employees' machines. They also went from one machine to the next, reconfiguring e-mail and Internet access, reconnecting them to network drives and printers, and copying user data back from the server.

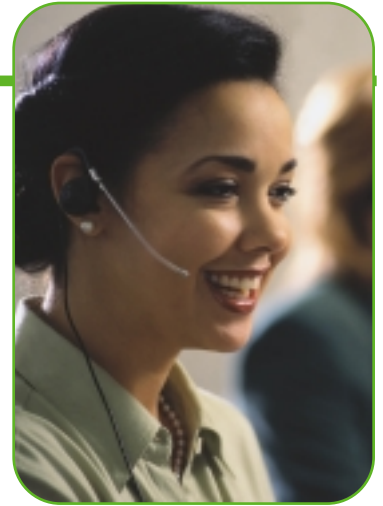
The next morning, the Help Desk was ready for action, fortified with coffee and donuts. Unfortunately, they weren't expecting 100 simultaneous service calls. They worked long and hard to help users resolve incompatibilities between applications, restore missing files, and reconfigure systems to work the way they did before. After a week the calls had died down, and IT started getting ready for the next group of employees. One down, nine to go.

Truth 5

IT can't fully protect users from viruses.

In the company's expectations, IT provides thorough protection from viruses through anti-virus software on both the server and users' machines. The company's firewall keeps out many dangerous files. IT implements strict policies to have users regularly update virus definitions and to keep users from downloading infected files from e-mail or the Internet.

In reality, these anti-virus measures leave several vulnerabilities. Anti-virus software only guards against known viruses; it provides no protection against the many new viruses that appear continually, and it doesn't reverse the loss of data and other effects of infection. Firewalls are based on experience and anticipation, so they don't cover all threats. IT's anti-virus policies don't cover all cases, and users don't always follow them. With these vulnerabilities, the risk of data loss is considerable; for example, despite companies' anti-virus measures, the Love Bug virus permanently destroyed countless files.



They say one "ohnosecond" is the length of time between hitting Enter and realizing your mistake. For Deanna, it was one heartbeat. Opening the personal e-mail attachment had released the new IH8MS virus, which sent a copy of itself to everyone in her Contacts list and then destroyed her Outlook mailbox and Explorer favorites.

With a knot in her stomach, she started calling her contacts to warn them. By the time she thought to report the virus to IT, they'd already heard about it from many other infected employees. It had spread like wildfire, striking half the machines in the company before IT pulled the plug on e-mail.

Recovery took days. Personal folders and favorites weren't included in the company's backup procedure, so employees spent many hours recreating them manually—especially the sales team, who relied heavily on their contacts lists. The impact on the company in terms of lost productivity and lost business was considerable. Deanna had always wanted to make a name for herself in the company, but this wasn't quite what she had in mind.

Anti-virus software only guards against known viruses;
it provides no protection against new viruses
and it doesn't reverse the effects of infection.

New Solutions for Costly Problems

The problems described above cost companies a tremendous amount in terms of resources, time, lost productivity and morale. Yet many companies are making little progress in addressing them. One reason is that IT often has no better alternatives—they do the best they can with the methods and tools that the industry has to offer, or that the company can afford. Also, raising these issues within the company can heighten awareness and frustration, increasing the impact of these problems without helping to solve them.

Recent advances in Help Desk technology are changing all that. A new generation of Help Desk systems with powerful new capabilities is providing a cost-effective way for IT organizations to solve these problems and improve the perception of its effectiveness within the company. Let's take a look at recent innovations in four key support areas: problem resolution and user self-service, remote assistance, disaster recovery, and system upgrades.

Problem Resolution and User Self-Service

Help Desk systems now provide enhanced problem resolution capabilities that can be highly effective in minimizing user downtime and extending Help Desk resources. These capabilities are based on the ability to efficiently preserve a perfect snapshot of each user's system. Thanks to advanced data compression technology, these snapshots can be captured and stored on the corporate server quickly and automatically over any network or remote connection—protecting every networked and remote user while consuming very little network bandwidth or storage.

With these snapshots, the Help Desk can restore current or prior versions of lost files or folders for a user by simply copying them from the server to the user's machine. The Help Desk can help a user quickly recover from more serious problems by rolling the system back to a pre-problem condition, enabling the user to return to work without waiting for a technician to troubleshoot the problem.

Help Desk systems also provide user self-service features—based on the same system snapshots—that benefit both users and the Help Desk. These systems enable users to recover on their own from everyday problems such as lost files or application errors, getting them back to work again faster without involving the Help Desk. And when used as part of a Help Desk problem tracking solution, these self-service features can automatically generate and resolve job tickets, enabling IT to track problems that were corrected by users without Help Desk involvement.

Remember Leslie in the example above, stuck in London with her failed demo? With this self-service problem resolution capability, she could have dialed into the home-office server and rolled the system back to its working condition in minutes, even over an international phone connection. That would have spared her the entire ordeal, and she would have made her sales goal for the quarter.

Remote Assistance

The Help Desk is asked to support more users than ever, with tighter resources. With lots of users in many network and remote locations, remote control can be the key to effective support. An effective remote control system lets Help Desk personnel take complete control of a client workstation over a network or dial-up connection to fix problems, install software, change configurations and more—all directly from the Help Desk without a single deskside visit. Intended specifically for the Help Desk application, these remote control systems can be integrated seamlessly into the Help Desk console to provide complete, secure control over users' machines in

the familiar console environment. These systems can greatly enhance user productivity and Help Desk effectiveness by reducing the time and effort needed to respond to and resolve problems.

With new Help Desk capabilities, the devastation caused by the virus in Deanna's e-mail could have been avoided. For those users needing additional assistance, the Help Desk could first perform an assisted rollback on the user's PC. This would recover both personal folders and web favorites. Next the Help Desk could show users how to modify their anti-virus profiles to watch for the IH8MS virus in the future. All this could be done by IT without making a deskside visit.

Disaster Recovery

Using system snapshot capability, Help Desk systems can now completely restore a user's system from a total system failure, a lost or damaged machine, or any other disaster—returning the user to full productivity as quickly as possible. These systems can even restore a user's familiar configuration from "bare metal" on a new machine—not through a lengthy scripted reinstallation of the operating system, applications and other files, but by quickly installing a minimal operating system that in turn restores the entire system from a snapshot taken earlier. This restoration can be done over a network or high-speed remote connection, or from recovery CDs created for this purpose.

With this disaster recovery capability, the Help Desk could have restored Claudia's complete system on her

new hard drive, getting her back to work immediately without distracting her co-workers. What's more, that quick solution would encourage her to call the Help Desk instead of the tech next time, enabling IT to track her problem

properly and avoiding the disruption of support work for key revenue generators.

As for the midnight computer theft, John the IT manager could have restored the ten employees' systems—complete in every detail—on their new machines from the latest snapshot in just a few hours, saving many hours of wasted effort and keeping the delivery for the big account on schedule despite the theft.



System Upgrades

A new generation of migration tools is putting an end to the costly, time-consuming process of manual migration. Using the system snapshot capability described above, these tools can move a user's complete system—including applications, data and personality—seamlessly to a new hardware platform or operating system. These tools also automate the migration process, providing a user-friendly interface to enable IT personnel to specify the parameters of the migration, and then performing the migration automatically on any number of machines. In this way, these automated tools eliminate much of the effort of installing specialized applications,

transferring files to and from temporary storage, and manually restoring network and personal settings. At the same time, by performing the migration accurately and reliably, these tools greatly reduce the need for post-migration troubleshooting.

If Ed and his team had used this type of migration tool to migrate his 1,000 employees to Windows 2000, they could have moved each group in much less time, greatly reducing the total time and cost of the rollout. And the employees all would have found their systems exactly as they left them, getting them back to full productivity immediately—and making it just another day for the Help Desk.

Summary

There has been a wide gap between what companies expect from their IT organization and what IT is able to deliver. Thanks to a new generation of PC support technology, IT can close this gap, improving performance and productivity throughout the company and enhancing the image of the IT organization.

More about Previo...



About Previo

This look at some of the issues facing Help Desk organizations today is brought to you by Previo, a leading provider of innovative products and services for the enterprise Help Desk.

Previo has a rich history of technology innovation going back to 1983. Previo's patented data compression technology, the heart of its famous Stacker® disk-doubler software, is the foundation for a variety of innovative products for protecting corporate data and workforce productivity.

Today, the rapid spread of computer technology throughout the business world is creating tremendous challenges for IT organizations. Previo is helping them meet these challenges with eSupport Essentials™, a full-featured enterprise Help Desk system with powerful capabilities for problem resolution, remote control, disaster recovery, and system upgrades.

Our customers include progressive companies like AC Nielson Company, Agilent, Alcon Laboratories, AT&T Labs, Baxter World Trade, Central Michigan University, County of Westchester–New York, Florida Power & Light, Grinnell Mutual Group, Hart Hanks, Lamb Weston, Lockheed Martin Technology Services, Motorola, MTS Systems Corporation, Nortel, Pepsi-Cola Company, Prudential, Teredyne, Thompson Consumer Electronics, Timken, Toshiba, Trane, and US Internetworking.

**For more information, call Previo at 877.977.3846 (U.S. toll-free)
or 44 (0) 1344.397593 (U.K.), or visit www.previo.com.**