

Introduction

Whether you support 10 or 10,000 users, creating and following a set of best practices will help your support organization deliver the quality service your end users deserve and demand. We've compiled 13 of Support Republic's best articles into this document to help you craft your own set of best practices. These articles are grouped into four categories: management, security, end user/IT support communication, and hardware and software issues. Within each category you'll find articles that cover topics every support organization should consider, including metrics, best practices for PDA support, end communication issues, best practices for laptop support, and much more.

Table of Contents

Introduction	1
Table of Contents	2
Management	3
Learn what every help desk manager should know about benchmarking	3
Prioritize your support calls with a call level chart	6
Choose the right training style for your help desk	8
Security	11
Emphasize security issues through help desk best practices	11
Best practices for mobile workforce information backup	13
Teach users these five laptop security musts	15
End User/IT Support Communication	17
Ten ways to improve user utilization of your help desk	17
Help your users and your help desk by mastering the five phases of a support call	18
Know how to stop the abuse: Dealing with abusive callers	20
Hardware and Software Issues	22
Remember best practices for opening a machine	22
Three rules for supporting laptops	24
Naming conventions ease the burden on support	26
Personal digital assistant support best practices	30

Management

Learn what every help desk manager should know about benchmarking

Jul 24, 2000 | [Bill Detwiler](#) | [E-Mail](#)

Is your help desk up to par? Are your clients getting the quick, accurate, first-class service they deserve? Could your help desk be outsourced? If you're not sure about how to answer these questions, read the Gartner Research Note, "What Is the Value of Benchmarking the Help Desk?" by T. Kirk on the value of help desk benchmarking.

In today's competitive, cost-conscious IT world, help desks that fall short will soon be outsourced. Help desks must constantly measure their performance and use this data to improve their procedures. The following Gartner article examines metrics, the benefits of benchmarking, and how to use the data collected. This information is essential to every help desk manager.

Many support organizations are struggling with the question, "How am I doing?" We examine the benefits of formal benchmarking in measuring support effectiveness.

Client feedback suggests the most-frequent benefits of benchmarking the help desk are higher service levels and concrete data for justifying increased funding and evaluating external services provider costs. By measuring their performance against other organizations, support managers can feed that information into organizational changes, sourcing requirements, service-level development, continuous process improvements, and technology integration to achieve quality service and lower costs. In this *Research Note*, we review the benefits of benchmarking technical support activities in all sizes of organizations and offer specific examples.

Definition

Benchmarking is a comparative evaluation of those metrics that provide an understanding of the relative differences and similarities between the support environments being benchmarked. These results can be achieved only through the use of consensus methodologies and robust metrics that enable consistent data collection and true peer group comparisons. The goal of help desk benchmarking analysis is to provide meaningful, implementable recommendations that are determined by analyzing an enterprise's IT support results against "best class" organizations.

Sample benchmarking metrics

Call handling:

- Agent handling: 84 percent (agent-handled calls/total inbound calls)
- Automated: 7 percent (calls completed without an agent (e.g., VRU/total inbound calls)
- Abandoned: 9 percent (abandoned calls/total inbound calls)

Call contact completion:

- First contact: 62 percent (calls resolved involving one person—a Tier 1 analyst)
- Second contact: 24 percent (calls resolved either involving two people on help desk side or two phone calls to or from the help desk/total inbound calls)
- More than two contacts: 14 percent (calls requiring more than two phone calls or more than two help desk persons/total inbound calls)

Average call queue time: 30 seconds (average speed of answer)

(Note: Measures such as call statistics, complexity, and costs are important. However, they cannot be reviewed without the help of end user and employee perspectives such as customer satisfaction, agent education, and stress levels. Source: Real Decisions, a Gartner Group company)

Examples of benchmarking benefits

- **Link customer satisfaction and service levels.** When queue times are greater than a peer group average of 30 seconds, the benchmark can indicate a requirement for better staff scheduling, use of automated support or expectation-setting with SLAs.
- **Implement continuous improvement initiatives.** A help desk benchmark helps organizations develop effective voice response unit and ACD phone practices and reporting, maintain a skills inventory, off-load self-help with intranet-based offerings, develop good problem and change processes, and identify career paths.
- **Develop help desk best practices.** A help desk benchmark provides guidelines for implementing technologies and practices aimed at improving the number of calls coming into the help desk that are resolved at the first point of contact. Knowledge bases and remote-control screen sharing make it easier for help desk analysts to understand the problem, provide insight for resolution, and educate the end user.
- **Communicate with top management.** Benchmarking can indicate the need for technology transfer to handle a new migration, as well as provide recommendations for looking outside the IS organization for capable service providers.
- **Lower the total cost of ownership.** Benchmarking that uses head count metrics can determine whether an organization is understaffed by analyzing employee abandonment rates, morale, stress levels, and job satisfaction. Since employees are the help desk's most valuable and expensive resources, it is important to avoid costly attrition problems. Solutions include implementing clear opportunities for career progression, developing a formal training program, and implementing employee recognition programs and rewards.

Link customer satisfaction and service levels

By understanding how other enterprises run their IT technical support function, an enterprise can focus on specific initiatives to improve the perception and operations of the help desk to achieve SLAs. It is difficult to manage requirements if performance is not measured. The most obvious criterion for help desk benchmarking is customer satisfaction. Customer satisfaction scores indicate end user perception of the help desk's value; a poor support function will undermine all other IS activities.

Implement continuous improvement initiatives

Benchmarking is critical for quality initiatives within the support organization. It is especially helpful for continuous improvement efforts, which require a baseline measurement program to be effective. Help desk benchmarking can help organizations avoid the evolutionary process of trial-and-error improvement. By analyzing the internal operations for support, organizations can identify strengths and weaknesses in organizational structure, process definition and technology application, and pinpoint areas for improvement.

Develop help desk "best practices"

The accelerating rate of change in the IT industry makes it increasingly more difficult to determine how to improve productivity and quality while reducing costs. Clearly defined targets of best-in-class metrics, and the rationale for such performance, enable support managers to measure progress towards specific goals and enable the participants to selectively adopt "best practices." By focusing on areas with the most potential for improvement, enterprises can become the IT support provider of choice among their customers.

Evaluate outsourcing alternatives

The cost performance methodology used in help desk benchmark studies closely resembles the process undertaken by outsourcers in creating a proposal and providing ongoing performance feedback. The analysis of comparative information gives insight into the question of when and how much to outsource technical-support functions. A help desk benchmark helps determine whether the help desk has the necessary skills portfolio and bandwidth to address incoming technical-support demand.

Communicate with top management

Analysis that lends itself to improved IT management practices can be used to validate or justify capital expenditures, head count, and other operational requirements. A help desk benchmark will provide employee and end-user feedback to assist enterprises to better understand various concerns and prioritize support goals and objectives. An analysis of training for help desk personnel can indicate an improved ability to provide a higher level of service by testing for proficiency, developing skills inventory, integrating training efforts, and developing and marketing informal (mentoring program, knowledge bases) and formal training (CBT, instructor-led, distance learning).

Lower total cost of ownership

Value is gained from knowing the performance metrics of top performers in a help desk benchmarking database. An examination of cost performance, productivity, and quality metrics focuses on areas that should be addressed and highlights areas that represent competitive advantages. For an enterprise, a help desk benchmark can determine that call completion at first point of contact is low compared to other support organizations. The overhead of transferring calls to more-experienced specialists has a negative impact on cost efficiency and customer satisfaction.

Bottom line

The risk of not benchmarking the help desk is outsourcing. Organizations that actively implement best-of-breed benchmarking practices will reduce the threat of outsourcing, achieve improved customer satisfaction, identify service gaps, improve employee retention, and result in an overall reduced total cost of help desk ownership.

Copyright: 2000-2001 by Gartner Group, Inc. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness, or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Prioritize your support calls with a call level chart

Nov 19, 2002 | Donald Ayers-Marsh | [E-Mail](#)

Whether your IT organization supports 100 or 100,000 end users, effectively prioritizing support calls is a critical process for providing high-quality, efficient service. Such a system enables a help desk tech to quickly and accurately rank and route calls by their importance and the expertise required to resolve them. When creating a prioritization system for your organization, take care to create a practical scheme that can be periodically reassessed and reworked.

One method of call prioritization that I have found to be particularly effective is a call level system. To create call levels, support calls are divided into different levels based on a combined measure of the expertise and amount of time required to resolve an issue. Each level corresponds to a staff member or members whose duty it is to address that level of call. Typically, intake staff solves the simpler issues and assigns the more complex issues to an appropriate level, often referred to as Level 1, Level 2, Level 3, etc.

To help you create such a call level system for your organization, I have created a call level chart that you can [download](http://www.techrepublic.com/download_item.jhtml?id=r00320021118dla01.htm) (http://www.techrepublic.com/download_item.jhtml?id=r00320021118dla01.htm) and then customize to fit your organization's needs. Here are some benefits of using a call level system, tips for creating a system for your company, and a sample of our call level chart download (see **Table A**).

Table A

Call level	Criteria	Procedure	Resolution target
Level 1	<ul style="list-style-type: none"> • Basic usage or problems with operating system, commercial or in-house software, or connectivity • Network account issues (e.g., passwords) as assigned • Self-help solutions available via intranet, documentation, and so forth • Referrals to other units (e.g., data security, HR) • Projects or responsibilities assigned to a specific staff member • Other problems that can be resolved within the target time limit 	<ul style="list-style-type: none"> • Intake staff performs diagnostic procedures, documents relevant information and any attempt resolutions, and then: <ol style="list-style-type: none"> 1. Closes the call if resolved. 2. Refers the caller to the appropriate person or unit, or... • Promotes it to Level 2. 	10 minutes

Why use a call level system?

A call level system tends to achieve a greater number of solved problems per staff hour expended. Level 1 staff members can either resolve or assign a large number of issues per day, providing the quick first response that is critical for users to feel that their concerns are being addressed, and reducing frustration and multiple calls. Level 2 and Level 3 staff can focus on their areas of expertise while Level 1 staff avoids spending time working on problems they're unlikely to solve.

When the Level 1 person cannot provide a final solution to a problem, the next most qualified person to help is assigned to it. If calls have been logged on to a voice mail or e-mail system, the assignment may take place before the user is even contacted. By directing callers to the best resource quickly, this tiered system minimizes the repeated handoffs and delays that leave users feeling that nobody cares or wondering about support staff competence.

Answering numerous phone calls and switching tracks frequently can be lethal to tasks requiring focus and creativity, providing only the illusion of getting more work done. With a call level system, upper-level staff who may have management or project responsibilities gain the blocks of time that are often necessary for both resolving issues assigned to them and for fulfilling their other work responsibilities.

If issues are tracked to allow support staff to review the resolution of a call, Level 1 staff can review issues they have promoted to increase their own knowledge base. Due to the large number of calls they receive, Level 1 staff can also be instrumental in detecting patterns of problems and in suggesting resolutions for frequent issues.

Issues to consider when creating your call level system

When creating your call level system, consider the following points:

Call priority

Call priority should be integrated into any call level scheme. Level 1 staff would assign an initial priority when promoting calls they cannot resolve and would immediately contact Level 2 staff for any critical issues.

Help desk analysts can work multiple levels

With a smaller staff, some individuals may work at more than one level but at different times. Thus, one may spend a certain amount of time resolving Level 1 calls and then switch to Level 2 mode to concentrate on the calls promoted to that level, or your staff might try rotating schedules for taking Level 1 calls.

Remember: Call level doesn't always correspond to skill level

When implementing a call level system, remember that the different call levels require different types of skills. A Level 1 staff person might be quite skilled but prefer the faster pace at that level. A Level 2 person may not know everything but could be a good diagnostician and researcher. Staff at each level should be respected for the resources they each bring to a support team.

Download TechRepublic's call level chart

You can download our call level chart by following [this link](#) or by following this URL: http://www.techrepublic.com/download_item.jhtml?id=r00320021118dla01.htm. TechRepublic has many useful documents, templates, and applications available for download, so be sure to check out our other offerings.

TechRepublic's call level chart is available as a Microsoft Word document and an Adobe PDF file. To increase download speed, we've zipped the files. You will need an unzip utility, such as [WinZip](#), [PKZIP](#), or [WinAce](#), to expand the zipped file. You will also need Microsoft Word or the Adobe Acrobat Reader. You can download the free [Adobe Acrobat Reader here](#).

Choose the right training style for your help desk

Nov 6, 2002 | [Jeff Dray](#) | [E-Mail](#)

Because end users often view the help desk as the font of all IT knowledge, it's important to keep your team members up to speed on the latest IT developments and refresh their knowledge of older subjects to ensure they're delivering consistent support. These objectives can be achieved only through continued education and training. But with a wide variety of training methods available, choosing the one that is best for your help desk can be tricky.

To help you make the right decision, I have divided the various help desk methods of training into four categories: formal instructor-led training, e-learning, on-the-job training, and group presentation. Each category has distinct advantages and disadvantages, as shown in **Table A**, that you should familiarize yourself with. Having this knowledge will help you make more informed training decisions for your help desk.

Formal instructor-led training

Formal instructor-led training is the most structured of all the training methods. This method ensures that techniques are taught in a uniform manner, in an environment free from distractions—and, if you've chosen a reputable training organization—by an instructor who is an expert in the course material. It is probably the best training method for presenting a new or complex subject. Formal instructor-led training also provides your help desk techs a break from their daily routine, which can help prevent burnout.

Unfortunately, these many benefits don't come cheap. Instructor-led training is the most expensive of all the training methods. It's not uncommon for a course to cost over \$1,000 per person. You must cover not only the cost of a professional instructor but also the cost of having your staff away from work. In the UK, companies can be quite cost-conscious, and such an outlay is often the first to go when they are looking to save money.

E-learning

Flexibility is probably the biggest advantage to e-learning programs because they can be accessed from most any computer and completed as time allows. E-learning programs also tend to be significantly cheaper than formal instructor-led training, but unfortunately, e-learning's biggest advantage can be its biggest disadvantage.

E-learning's high flexibility means that organizations often want employees to fit e-learning courses into the gaps of their normal workday or take the courses at home. In my experience, neither of these approaches works very well. In the former, busy techs are likely to be interrupted while taking the e-learning courses, and such interruptions make effective learning nearly impossible. In the latter, employees can construe a mandated e-learning program at home as just another instance of work creeping into their own private time. This can lead to resentment, which again makes effective learning nearly impossible.

E-learning can be a valuable training tool when used correctly. Schedule time during the workday for techs to concentrate totally on their courses. Minimize interruptions and keep the training limited to their normal work hours.

Table A

Training method	Time required	Group /individual	Flexibility	Cost	Advantages	Disadvantages
Formal instructor-led training	Usually whole day(s)	Both	Low	High	<ul style="list-style-type: none"> Information presented in a uniform manner Information taught by expert Minimal opportunity for interruptions 	<ul style="list-style-type: none"> Expensive Techs are required to be away from the job
E-learning	Usually several hours (often spread over several days)	Individual	High	Moderate	<ul style="list-style-type: none"> Less expensive than formal training Information taught by expert Highly flexible schedule 	<ul style="list-style-type: none"> Subject to frequent interruptions High flexibility can lead to misuse
On-the-job training	Flexible	Individual	High	Low	<ul style="list-style-type: none"> Free Focuses on real-world issues 	<ul style="list-style-type: none"> Potential to perpetuate bad habits Instructor not always an expert
Group presentation	Short sessions when time permits (usually an hour or so)	Group	Moderate	Low	<ul style="list-style-type: none"> Almost free Fairly flexible depending on help desk and presenter availability Can focus on real-world problems in your organization 	<ul style="list-style-type: none"> Presenter may or may not be an expert Can be difficult to schedule IT professionals aren't always the best instructors

On-the-job training

Let's face it: Most help desk training is received on the job. Unless your organization has a hefty training budget, your training program for new techs probably consists of placing them with a senior tech for a few weeks to teach them the ropes. There are two big advantages to on-the-job training. First, it's free and, second, the new techs get to experience real-world problems. Unfortunately, if not done properly, on-the-job training can lead to the perpetuation of bad habits. Your organization should take great care that the information delivered through on-the-job training is accurate and consistent.

Group presentation

Although sponsoring group presentations is a low-cost training approach, it combines many of the other training methods' advantages. First, it's cheap because the presenter is usually a member of your help desk team, or perhaps someone from outside the help desk but within the company. Second, it's fairly flexible; you need only schedule a time when all or most of the help desk techs can meet for an hour or so to hear the presentation. Third, everyone who attends the presentation receives the same information. Fourth, real-world issues from your organization can be used to illustrate new concepts or problem-solving methods.

Yet the group presentation technique isn't without a few disadvantages. First, you must ensure the presenter thoroughly understands the subject matter he or she will be presenting. It does you no good to have your team members learn erroneous information. Second, although more flexible than the formal instructor-led training, group presentations can be difficult to schedule because they depend heavily on the availability of your teams and the presenter. Third, not all IT professionals are great trainers. If you don't choose someone who is a good instructor, you're just wasting everyone's time.

A great way to conduct group presentations is through brown-bag lunch sessions. This lets you minimize the time your team members are away from their jobs but isn't as intrusive as scheduling a meeting after or before normal work hours. Either have your team members bring their lunch to the meeting room or, better yet, spend some money from your department's training budget and buy them lunch.

Go for a blended approach

In the end, the training method you choose will depend heavily on your help desk techs' needs and available resources. And no one of these methods is any more or less valid than the others. I would promote a system of blending these methods to make a coherent program of recognized training methods that can be used as and when deemed appropriate.

Security

Emphasize security issues through help desk best practices

Jul 25, 2002 | [Mike Walton](#) | [E-Mail](#)

As the representatives of all things IT, support techs should be teaching end users proper IT practices in everything they do. The best way to teach good security practices is to establish a set of help desk best practices that focus on physical and password security, and then consistently maintain them to help develop a culture of security in your organization.

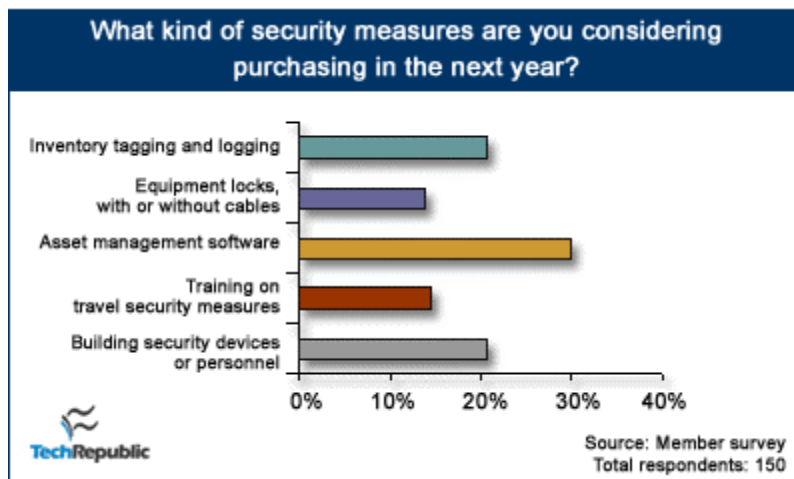
Physical security

The importance of adequate physical security was recently reaffirmed to me by an incident that happened at a friend's company. The company is located in a quiet, suburban office park in a nicer part of town. They have key-code locks on all exterior entrances and key locks on the main interior entrance. You would think this would provide adequate security, but one Saturday night, an individual (or more likely a group of individuals) entered the office and stole about 25 laptops.

This is not an uncommon occurrence. In a [May 2001 survey of TechRepublic members](#) (<http://www.techrepublic.com/article.jhtml?id=r00320010525wtn01.htm>), the largest number of those who took the survey and had lost computer equipment said the equipment was lost on corporate property.

In the same survey, about 20 percent of the respondents said building security was high on their wish list for 2002 along with asset management and inventory tagging (**Figure A**).

Figure A



Equipment locks aren't popular, but they could save a company money.

Mobile computers, such as the laptops stolen from the company above, are probably the most vulnerable pieces of equipment distributed to end-users. The analyst firm [Gartner](#) estimates the costs associated with a stolen \$3,500 laptop to actually be \$6,300. That figure includes estimates of costs to procure and deploy replacements, dealing with police and insurance claims, data replacement and recovery, and lost productivity.

Security measures such as cable locks and asset tags on all equipment contribute subtly to establishing a culture of security in end users. Support pros can emphasize physical security with end users by ensuring that equipment locks are used and by purposely checking asset tags when they make trips to end users' desks.

Support pros can also encourage end users to guard their laptops by explaining security issues to end users before they take their laptops on the road. Ensure all the proper software is installed and review security tips with traveling users. To help you with this task, check out our download "[Sample FAQ PowerPoint for traveling laptop users.](#)"

(http://www.techrepublic.com/download_item.jhtml?id=r00320020520wtn02.htm)

It's also a good idea to have end users tape business cards to their machines. Check out the article "[Teach users these five laptop security musts](#)"

(<http://www.techrepublic.com/article.jhtml?id=r00320020424wtn01.htm>) for more ideas about laptop security.

Press those positive password policies

As a support tech, you've probably heard plenty of password horror stories—passwords taped to monitors or freely shared among users. TechRepublic columnist [Jeff Dray](#) once worked for a major United Kingdom telecommunications company where he [saw user IDs and passwords](#) (<http://www.techrepublic.com/article.jhtml?id=r00320010125det01.htm>) posted on a dry-erase board in a company office, where they "were clearly visible from the pub across the road."

While that's an extreme example of poor password protection, it isn't uncommon for end users to tell support techs their passwords during a visit. In another [article](#) (<http://www.techrepublic.com/article.jhtml?id=r00319990504jed02.htm>), columnist [Jeff Davis](#) offered three points of advice that ring true for support techs:

- If the user has left you his or her password on a note stuck to the monitor, the password needs to be changed.
- If a user dictates the password aloud for you, the password must be changed before you leave.
- If your service call requires you to change the user's password, make sure the user changes the password again before (or immediately after) you leave. That way, you can always credibly say, "I don't know what that user's password is," and you can never be accused of misusing someone else's access.

Davis also recommends that you make sure that end users know how to change passwords so that they can change them if needed before the network administrator forces a change.

Help desk security best practices

Follow these tips for establishing security best practices:

- Secure mobile equipment with cable locks both in and away from the office.
- Place asset tags in obvious places on equipment to subtly remind end users, visitors, and would-be thieves that all equipment is tagged and tracked.
- Have traveling users tape their business cards to their laptops.
- Instruct users not to post their password in a visible location.
- Inform users not to share their passwords with anyone, even the IT support staff.
- If an end user tells a support pro his or her password, require the user to change it at the end of the support call.
- If the support tech must change an end user's password, require the user to change the password again before the support tech leaves the site.

Best practices for mobile workforce information backup

Apr 4, 2002 | Gartner | [E-Mail](#) | [Archive](#)

By J. Girard

How will enterprises manage critical information distributed across mobile workstations, PDAs, and smart phones?

An enterprise cannot become resilient unless it can effectively operate a backup-and-restore method for all of its user workstations—in the offices, mobile, and remote. Installing a voluntary backup system for user convenience is not good enough; users will not make regular or sufficient backups. They will lull themselves into a false sense of security, until the next disaster leaves them helpless. A resilient organization also cannot afford to rely on “luck.” Even if work disruptions caused by user data loss are not widely discussed, they are happening, because they are statistically unavoidable. Continuous backup and the ability to restore anywhere and anytime is fundamental not only as a convenience to individual users but also to the survival of the business.

In the laptop market, the great majority of tools for backing up and restoring are based on the erroneous assumption that the user will have constant access to a high-speed LAN. One company, [Connected](#), broke away from this mind-set seven years ago and remains the leader and most mature player. Connected’s closest competitors in the remote backup market are [Veritas Software](#) and a new entry for the fourth quarter of 2001, [XcelleNet](#). All three companies provide the capability to continuously and incrementally back up data off a user’s system. Users of Connected’s TLM product can be served whenever connected to the Internet. A VPN is not required, because the backup data is secured with triple Data Encryption Standard (DES) encryption and device authentication. Veritas offers similar capabilities but has more limited encryption (40-56-bit DES options) in its current release; therefore, it is best used over private networks or VPNs. XcelleNet will become an important player in the backup market because its broad range of management products already bridges the gap from laptop to personal digital assistants (PDAs), smart phones, pagers, and other mobile devices. Enterprises that implement one of these products will receive a full return on investment after the first time that a critical user system is lost, stolen, or damaged.

The PDA and smart phone markets represent the largest and fastest-growing threat to business resiliency because of their mounting numbers and varieties. By year-end 2002, the average IT-enabled users will use at least three portable devices (0.7 probability) and will spend more than one hour per day trying to maintain synchronization among their “personal network” of devices (0.7 probability). These users are literally juggling their enterprise’s most critical assets not only on laptops but also on toy-like miniworkstations that are easier to lose or break than laptops. Many hundreds of thousands of laptops, PDAs, and smart phones are lost each year, resulting in device recovery losses in the billions of dollars.

Tool choices for managing and synchronizing smaller mobile devices are confusing due to the sheer number of players and the variations in their features. A partial vendor list includes:

- [Altiris](#)
- [Computer Associates](#)
- [Extended Systems](#)
- [Infowave Software](#)
- [Intel](#)
- [iOra](#)
- [Marimba](#)
- [Microsoft](#)
- [Mobile Automation](#)
- [Mobiliti](#)
- [Novadigm](#)

- [Novell](#)
- [On Technology](#)
- [ManageSoft](#)
- [Pumatech](#)
- [Synchrologic](#)
- [IBM/Tivoli](#)
- XcelleNet

Suite vendors have bundled pieces of mobile solutions into legacy office product lines. Framework vendors develop broad solutions on their own core technologies. Point-solution vendors rely on one or a few high-value features to gain market share. Enterprises will need to weigh their experiences with vendors in all categories to determine which type of investment will provide the most effective backup and restore capabilities for their current and planned mobile devices. When evaluating synchronization/management vendors, enterprises must require examples in the context of their own business processes, of how the products will ensure that backups are automatic, and how synchronization between devices will be assured.

Best practices for resilient mobile devices

These seven steps are distilled from Gartner research and client feedback. These steps will lead enterprises to develop practical, achievable support practices that address the needs of the business by striking a balance between user awareness and supporting technology.

1. Incremental backups of workstations and laptops with full OS are feasible, relatively easy to manage, and reliable. The cost of implementation can be partly justified by also planning to use a tool like Connected TLM for its other major use: to facilitate migrations to Windows/XP.
2. Enterprises should not wait to find the one “ultimate” tool for desktops, laptops, and smaller mobile workstations. Use of a legacy backup system in the office and one to several new and separate products for mobile/remote users is perfectly reasonable.
3. The enterprise philosophy for all small mobile devices must shift from personal synchronization to server synchronization. Employees who use mobile devices primarily offline from networks must be advised to synchronize frequently to their laptops or desktops, which in turn will be backed up.
4. Employees who use small mobile devices online to the Internet or a corporate network must have a server-based synchronization product operating on their device that is capable of continuous, incremental backup.
5. Priority should be given to backup/synchronization products that can restore data to a different platform in the event that an exact hardware replacement is not available.
6. All tools selected must support the concept of an administrator password for encrypted data access in the event that the original user is not available when the data is needed. The enterprise will need to adopt strong internal password-handling practices so that this feature does not become a back door for cybercrime.
7. Automated tools with incremental, background updating processes are the only method likely to succeed. Voluntary backup tools under user control will not provide adequate data protection.

Gartner originally published this report on Dec. 14, 2001.

Copyright: 2000-2001 by Gartner Group, Inc. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness, or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Teach users these five laptop security musts

Apr 26, 2002 | [Mike Walton](#) | [E-Mail](#)

While encryption software might protect your organization's data if a laptop is stolen, preventing the laptop from walking away in the first place is your best line of defense.

IT pro Pat Vickers and Gartner analyst John Girard both recommend that these five tips on how to physically secure laptops be taught to all laptop users:

- Keep your laptop in sight while going through security checkpoints.
- Always have the laptop in carry-on luggage.
- Tape a business card to the laptop.
- Avoid leaving your laptop in hotel baggage-hold rooms.
- Lock the laptop or removable hard drive if equipped in a secure place when it's not in use.

Loose grips lose chips

Vickers described a typical laptop sting in the article "[Eight tips for the new laptop user.](http://www.techrepublic.com/article.jhtml?id=r00319991216jed40.htm)" (<http://www.techrepublic.com/article.jhtml?id=r00319991216jed40.htm>)

The traveling end user approaches a security checkpoint in an airport, carrying a laptop computer in its case. Two thieves manage to get in line right before the laptop user.

When the user gets up to the x-ray machine, he drops his laptop in its case on the conveyor belt. Meanwhile, the forward-most thief is passing through security and waiting at the end of the conveyor belt.

The thief just in front of the end user has all sorts of problems when he goes through the metal detector. He didn't take all the change out of his pockets. Then, he forgets about that gold necklace around his neck, which requires him to go through the detector over and over again.

Meanwhile, the first thief walks away with the user's laptop. Security is concentrating on the second thief who's setting off the alarm and all the other baggage coming through the x-ray machine. No one notices who took the computer bag.

According to Gartner analyst John Girard, the most common places for laptop thefts are airport security checkpoints, ticket counters, hotel restrooms, meeting rooms, and registration lines.

While laptops are best protected from bumps and bruises in their carrying cases, Vickers points out that potential thieves can spot those cases very easily. Laptop users may not realize they were such easy targets.

The best course is to treat the laptop, either in its case or snugly stored in other luggage, as carry-on luggage, even if the end user doesn't plan to do anything with the computer during the flight. And don't take your eyes off of it.

Inadvertent losses

While these two tips, keeping a close watch and treating the computer as carry-on luggage, may help prevent someone with the intent of robbery from getting the laptop, Vickers suggests taping the end user's business card to his or her equipment as a way to avoid accidental loss.

When a group of traveling end users is from the same organization, they will likely have the same or similar laptops. Computers can get mixed up if everyone is working off the same conference table. Someone could inadvertently pick up someone else's computer and leave his or her own behind.

Another scenario might be that a user shows up at the hotel before a room is ready for them. Many hotels will hold the traveler's luggage in a holding room. Girard points out that hotel baggage-hold rooms are to be avoided for storing laptops. Even if someone doesn't go into the room and walk off with the computer, many times, hotel staff will move the traveler's luggage to the room before the end user returns, and guess what gets left behind?

Fused at the hip

Even if the end user is cautious, support staff can't expect that the computer will never leave the end user's sight. Girard suggests that when the laptop is not in use, it should be locked in a secure office or hotel safe. Some laptops have hard drives that can be easily removed when the computer is not in use, and these are small enough to fit in the hotel room's safe.

One way to encourage the locking of the laptop, particularly for users who will be using their laptops throughout the day, is to provide a [device to lock the computer to a desk](http://www.techrepublic.com/article.jhtml?id=r00320010604wtn01.htm) (<http://www.techrepublic.com/article.jhtml?id=r00320010604wtn01.htm>) or other immovable object in their hotel room or conference room.

End users also can use cable locks when they return to the office. If the laptop is left in a pseudo-public office space, the lock will prevent removal from the desktop.

Bringing it home

Like many types of security, protecting laptops is often more a matter of common sense than high-tech gadgetry. The problem is getting the end users to buy into the program.

Support departments can encourage and highlight security issues with users by assisting the users with taping their business cards on their equipment, or, if you can successfully make the case, issuing cable locks to mobile laptop users.

End User/IT Support Communication

Ten ways to improve user utilization of your help desk

Aug 31, 2000 | [Jeff Dray](#) | [E-Mail](#)

Help desks should constantly strive to improve their methods of client interaction. Users must feel comfortable with the help desk and know they will receive prompt, courteous, and effective support. Here are ten practices your help desk can use to strengthen user relations and improve client utilization.

1. **Be proactive.** Don't wait for a problem to occur before you meet the users—get out there and introduce yourself and the team. In touring the building, you may find ways to improve the way users work. You may be able to show them easier ways to work, shortcuts, better software, and so on.
2. **Have a help desk open house.** This get-together is a great way of receiving feedback on your work and learning exactly what the users want. Everything you teach the user is one less problem log later. It also shows the user that you want to improve communication, breaking down that "us and them" atmosphere.
3. **Make contacts in each department of the company.** Forge links with these power users and authorize them to handle routine problems. When necessary, these contacts can report more serious issues and training deficiencies relevant to their department.
4. **Publish a monthly newsletter.** You can offer hints and tips related to the most commonly asked questions, as well as getting your face known around the company.
5. **Set up an intranet page for the help desk.** You could have a short biographical piece on each team member, detailing hobbies, interests, and special areas of expertise, as well as an online form for reporting problems during off hours.
6. **Tag every piece of supported equipment.** While you are designing the tags, why not include the help desk number? You could also include useful information like reminding the caller to make a note of any error messages, to call from a phone that is adjacent to the equipment, to have the equipment running when they call—all those annoying things that often waste time.
7. **Publicize the help desk.** Get some posters up that show the hours of operation, what you can help with, and what the help desk's phone number is. You would be amazed how many people do not know the help desk number and call via the switchboard.
8. **Send every user a laminated help desk tips card.** On one side, list the help desk's phone number, e-mail address, and hours of operation. On the other, print helpful tips, such as noting error messages, calling from the room where the equipment sits, and remembering what they were doing when the error occurred.
9. **Work yourself out of a job.** Make your users the best trained, best supported, and most efficient in the world. In the highly unlikely event that you make the entire help desk redundant, your bonus and promotion package should be out of this world!
10. **Most important of all, enjoy yourself.** Have a joke with your colleagues and, where appropriate, with the callers. Some help desks I have visited are so serious that you wonder whether it can be any fun at all to work there. When the users start to include you on their e-mail distribution lists for jokes, you know you have reached them in a way that means that true communication has been achieved.

Help your users and your help desk by mastering the five phases of a support call

Jan 22, 2001 | [Jeff Dray](#) | [E-Mail](#) | [Archive](#)

A well-developed call cycle can help you get to the bottom of a caller's problem. You can create a call cycle by splitting the basic phases of a help desk call into simple, recognizable sections. Once you've mastered this technique, you can handle a call uniformly and effectively, which will help not only the caller but your colleagues as well.

1. Listen: And take control of the call

Take control of the call by immediately asking for the caller's contact and problem information. While the caller describes the problem, you can open the call log and enter this information.

Enter call information on the fly

When taking a call, be sure to "hot log" the problem, that is, enter the details into your help desk's call tracking system while you are actually talking to the caller. Hot logging reduces the chance for incorrect data entry and allows you to close the call more quickly.

You might find it hard to listen if the caller is not communicating well, whether due to frustration, nerves, or anxiety. If this is the case, you can steer the conversation in the right direction by asking closed questions (ones that can only be answered with a yes or a no).

Occasionally, I digress to other subjects during a support call. For example, I might use the time it takes for a PC to reboot to discuss the weather. This shows the caller that he or she is speaking to a real person rather than a support-providing automaton. If you digress, however, be sure to move the conversation back to the problem at hand once the PC has rebooted or a piece of software has finished installing.

2. Acknowledge the problem: Let the caller know you understand his or her predicament

Recap the caller's problem. This allows the caller to clarify any details you might have missed the first time around. Another trick I use is to summarize the problem but alter a detail so that the caller has the opportunity to correct the information. This technique allows me to check that communication is working in both directions.

3. Provide the solution: Make sure the caller understands what he or she needs to know

Be sure to make the solution easy to understand (e.g., don't overwhelm a novice with an overly technical explanation) and make sure the caller understands what you just said. Outline why the problem occurred and give concise details of the fix. If alternative solutions to the problem exist, ask additional questions to see whether these potential fixes might work better for the caller.

4. Recap the call: Make sure the caller understands and feels comfortable with the resolution

Recap your conversation and invite the caller to ask additional questions. Close the call with an agreed course of action. Make sure the caller knows to call again if he or she needs further assistance but always try to leave things on an upbeat note. Finally, thank the person for calling and end the call. Do not hang up too abruptly, however. Let the caller hang up first. I think doing so seems less pushy.

5. Check your facts: Make life easier for your colleagues

Double-check your call log and make sure that your comments are concise and accurate. Your coworkers may need to revisit the problem later, and they will need to know exactly what transpired because you may not be there to answer any questions.

If you hot logged the call, you can probably close the problem log at the same time the call ends. That way, you'll be ready to take the next call as soon as it comes.

Know how to stop the abuse: Dealing with abusive callers

Jul 26, 2000 | [Jeff Dray](#) | [E-Mail](#)

Abusive callers are, unfortunately, part of the job when working a help desk. The good news is that you do not need to put up with them. If you follow the steps outlined here, you'll be able either to make these callers behave in a civilized fashion, or send them on their unpleasant way.

What is an abusive caller?

Do not confuse abusive callers with angry callers. It is quite possible for a caller to be furious without losing their cool and becoming abusive. You can help angry people and, with the right treatment, turn them into happy ones.

Callers are abusive if they speak to you in a way that makes you feel uncomfortable or if they make comments of a derogatory nature. You define the level of abuse by how it makes you feel personally. However, don't take the caller's abuse to heart, even if the attacks become personal in nature. You are doing your best to help (at least you should be). If your efforts are not good enough for the caller, remember the hundreds of people who were happy with your work. Abusive callers are more than likely upset about a totally unrelated matter, and are abusive to you because they lack the maturity and objectivity to separate this annoyance from the matter in hand.

What constitutes phone abuse?

Phone abuse can be categorized as any derogatory verbal exchange that is aimed at you personally, or that makes you feel uncomfortable. This can be anything from comments aimed at your religion, race, or gender, to rudeness, shouting, or even taking other calls while speaking to you. Nobody should ring you up and then put you on hold. This just demonstrates bad manners and is always the caller's problem, not yours. If somebody calls me, then starts to talk to somebody else, I usually hang up.

Is the customer always right?

Everybody has the right to some respect. Customers are not always right, no matter what their problems may be. If they start to hurl personal abuse at you, then they are definitely not in the right, and you have the right to no longer talk to them.

Support from your company

It's important that you familiarize yourself with your company's policy on abusive callers. If that policy says that you have to sit there and take it, then frankly it's time to find a new and better employer.

What can I do when abuse occurs?

When a caller is ranting and hurling abuse, nobody is getting anything out of the exchange. Stop trying to help the caller and start taking charge of the call. You can tell abusive callers that you are not comfortable with the way they are behaving and ask them to stop. Explain why you do not feel comfortable.

Remember, you aren't a machine and do not deserve to be treated as one. You have feelings, just as the caller does, and the caller should respect them, no matter what the issue is.

Above all, stay calm. Don't rise to the bait or snap back. That's what they want. They want you to lose control and start a shouting match. Nothing would make them happier than for you to fly into a rage so that they can take the moral high ground and make a complaint against you. Sometimes letting them think that the call is being recorded is useful, particularly if the caller is internal. Keeping calm can also defuse the situation, may result in an apology, and is your best chance of getting back on track.

Let the caller know that either the abuse stops or the call does

Should the abuse continue, calmly inform the caller that you will not put up with it and will terminate the call if it continues. This will either calm the caller down (if he really wants your help) or make him worse, in which case you can end the call. Be firm about it. Make it clear that the ball is in their court—if they want support, you are happy to provide it, but the call must proceed in a polite and professional way.

Terminate the call

If the abuse continues after your warning, simply hang up. Don't repeat your threat endlessly and definitely do not argue. You have stated your position clearly.

Example conversation

Help desk worker: "I will hang up if you continue to talk to me in this way."

Caller: "You #@#@ well won't! You'll do as I say, you #@***#@!"
Click!

Inform your manager or supervisor

If you have to end a call, the caller may call in later to complain. This is nothing for you to worry about. As long as your supervisor knows about the incident, he or she will support you. Anybody who has worked on a help desk knows the score. Supervisors should be informed so that they can deal with the complaint when it comes in. I have known a complaint to arrive, and then after a few minutes the supervisor hung up on the caller as well! When this individual got through to the managing director of the company, expecting some kind of freebie for his trouble, he was told that he was no longer welcome to use our service.

Finally some good news

Luckily, abusive callers are the exception and not the rule. In fifteen years and many thousands of phone calls, I have prematurely ended less than five as a result of abuse. I have also never been disciplined for the way I speak to a caller or for hanging up on them if the situation demanded it. Ninety-nine percent of the people I speak with are very pleasant. They just need help. Even though abusive callers are thankfully not a common occurrence, when you are prepared to deal with a bad call experience, it is much easier for you, and not the caller, to be the one in control of the situation.

Hardware and Software Issues

Remember best practices for opening a machine

Aug 24, 2001 | [Mike Walton](#) | [E-Mail](#)

The Hippocratic oath may have been written long, long ago to ensure the proper conduct of physicians, but support professionals should take note of the venerable pledge's admonition to "do no harm."

That's not always an easy task when much of your open-machine surgery is performed at the cluttered desks of hapless end users. These conditions are often complicated by the fact that there's typically carpeting on the floors and frost *inside* the windows.

Still, it doesn't hurt to remember that there are certain accepted best practices for cracking the case and working on computer components, including:

- Preparing for the unexpected by backing up data and recording configurations
- Turning off and unplugging all related equipment
- Using the appropriate tool for the task
- Doing what you can to reduce the risk of electrostatic discharge (ESD)

Preparing the patient

Before you can cure an ill computer or open it up to upgrade its capabilities with new cards or chips, there are a few things that you should do to prepare your patient—and yourself.

If the situation allows, it is best to back up the data on the computer to another storage device or medium. This ought to be part of the standard operating procedures with any organization's computers, but if the IT staff isn't doing it, you can bet the end users haven't done it for themselves.

You might want to record the vital stats for the hard drive or drives on the machine along with all of the BIOS settings. These are details that will come in handy if you have to give it a lobotomy, or it blows up on you.

In the medical profession, doctors will wash their hands and put on sanitized attire before the operation. Support techs need to prepare themselves for operating on a computer's inner workings as well.

Among the things you should do is tie any loose hair back out of your face. Watches, rings, bracelets, and long necklaces should be removed to prevent them from being damaged or conducting an electrical charge.

Uncontrolled electrical charges are something to be wary of while working on a computer. After you have shut down the computer, many people recommend unplugging the equipment. Some OEMs may recommend that you leave it plugged in so that the equipment remains grounded through the power cord.

Either way, be careful of what you touch within the bowels of the machine because there are components, such as capacitors, that store electricity and can cause a fatal electrical shock under the right conditions.

Opening the patient up

Once you are working inside the computer, it is important to use the appropriate tool for the job and avoid adding an electrical charge to the system via static electricity.

Much of what needs to be done in the computer can be accomplished with either a flat- or Phillips-head screwdriver. Screwdrivers without magnetic heads are best suited for the job because a magnetized object can damage integrated circuit boards.

Force should always be avoided when dealing with components within the computer's box. When faced with a stubborn chip or board, the best way to remove it is to work it loose through a back-and-forth motion while holding the card by its edges.

If you are working on a computer that you haven't worked with before, you might want to sketch drawings of which wires plug into which sockets and where the number one wire in ribbon cables is connected. If you are installing new components, use the static-free bag the component came in to hold the component that is removed.

Avoid placing cards on monitors, which are infamous sources of static discharges and magnetic fields. Also, if you must stack cards, make sure you put something, such as foam, between them to prevent scratches.

There are a number of things you should do to prevent transferring static electricity from your skin to electrical components. Remember, if you can feel a static shock, the voltage of the static electricity you have stored on your body is many times what is needed to harm electronic components.

To prevent electrostatic discharges, you should:

- Use a grounding mat on your workbench.
- Wear a grounding strap when you can (the exception being if you are working on a monitor or the inner workings of power supply where the grounding strap could be a lightning rod for discharges from the powerful capacitors that are present in both devices).
- If you don't have a grounding strap handy, leave the equipment off, but plugged in, and touch the computer chassis frequently.
- Don't touch equipment if either you or it has just come from a cold, low-humidity environment.

Leave component cards in their static-free bags until you need them and then handle them only by their edges, avoiding the edge contacts.

Three rules for supporting laptops

May 28, 2001 | [Mike Walton](#) | [E-Mail](#)

With the advent of high-speed access from homes and hotels, more and more organizations are boosting workers' productivity by providing laptop computers.

Despite this trend, desktops computers still vastly outnumber laptops in today's corporate arena, in part due to the relative ease associated with supporting desktop computers. Nevertheless, there are still a number of companies that are ahead of their time when it comes to laptops. TechRepublic is one of them. According to Ted Laun, help desk analyst at TechRepublic, "We're a freak of nature, having more laptops than desktops."

Laun has three rules that he considers vital to supporting laptops. They include the following:

1. Laptops should be configured to use DHCP whenever possible.
2. Remote access should be made as simple, yet secure, as possible.
3. A spare laptop for every model supported must be kept on hand.

In this article, we will take a closer look at each of these rules.

Repeat after me: DHCP is my friend. DHCP is my friend.

Most users will be taking their laptops from your network and plugging them into networks in branch offices, client offices, and hotels that provide high-speed access. To facilitate this mobility, all corporate networks at the main headquarters and branch offices should be set up to allow dynamic IP address distributions.

"When I came to TechRepublic, three of the four remote offices at the time had static IPs," Laun said. "So every time someone came to our corporate offices from a branch office, the support staff would have to set their computers up for DHCP. Often, they would leave town to return to their branch offices without thinking to have their computer reset to the static IP. When they got back to their office, they wouldn't be able to connect to their LAN."

Remote access made simple

Laptop users often find themselves in hotels without high-speed access or at a client's location where they are unable to gain network access. In such situations, users need a backup communication method. This typically means a built-in or card modem on their laptop.

Because employees of TechRepublic travel to cities around the globe, TechRepublic chose a dialup ISP that has local connections throughout the world.

The ISP's dialup client is installed on every laptop and is configured for each individual user. All the user has to do is plug a telephone line into the RJ11 port on the computer's modem, launch the dialup client, select the city from which he or she is calling, and then hit the dial button.

There are a number of problems that support staff might encounter when helping a user who is making a telephone-line connection—and many of them are out of the support person's control.

Users often don't know when to use a 9 prefix to get an outside line, or they sometimes forget to change their settings to the correct city of origin. The telephone cables may not be connected properly. The user might be trying to call out on a digital system. The location's telephone service may be inferior.

Users need to understand that they must approach a dial-up connection patiently.

“It’s not going to be easy, and it isn’t going to be fast,” Laun said of dial-up connections.

Once users get connected, security becomes an issue if their traffic will be crossing the Internet via an ISP or through a high-speed LAN connection.

Virtual private networks (VPNs) are a perfect solution for many enterprises because they offer both security and the ability to access company resources from the field.

Don’t de-spare

One of the best ways to avoid major laptop problems is to keep a spare laptop on hand for emergencies. Even when portable computers are in-house, they still require special care and support.

Sometimes specific laptops will not mate well with certain docking stations, even when both come from the same manufacturer.

Compared to desktop computers, laptops have smaller versions of the same equipment. Smaller parts can be more delicate and prone to damage.

Then there are laptop-specific issues.

Laun remembers getting a call from a remote office one day, and the user was having a peculiar problem. The left and right mouse buttons by the computer’s touch-pad mouse had stopped working.

Laun shipped a spare laptop of the same make and model to the user’s office and had the hard drives swapped out. The nonfunctioning computer was sent back to the corporate offices.

Nothing appeared to be immediately wrong with the computer, but the buttons would not work. Laun called the user and during the course of the discussion learned that in preparation for a trip, the user had changed batteries in the laptop with a battery that had never been used before.

Laun popped the battery out of the laptop and, comparing it with another battery, noticed that there was a thicker edge on the replacement battery than the original. Laun took a knife and shaved off the extra plastic on the battery, put it in the malfunctioning laptop and sure enough, the mouse buttons worked perfectly. The extra plastic had distorted the case just enough to prevent the mouse buttons from working.

This problem was easily fixed thanks to the spare laptop that was available.

Keeping a spare laptop for every model in use in an organization has one drawback that bothers Laun. TechRepublic has five different models of laptop in circulation, so prudence demands five spares on the shelf.

“When someone needs a laptop, can I justify buying another at \$3,500 when I’ve got five sitting there on a shelf?” Laun asks.

Naming conventions ease the burden on support

Dec 10, 2001 | [Mike Walton](#) | [E-Mail](#)

There are a lot of creative minds at work in the IT field, and usually that's a good thing. When it comes to host names on both client and server computers, however, creativity should take a back seat to utility.

Unfortunately, useful host names are not always a first priority when a network is being built; sometimes machines are named with someone's personal interests in mind instead of the company's best interest.

For example, on our test network at TechRepublic, we have one editor who happens to be a Peanuts fan, so most of his machines are named after the Peanuts characters. His remaining machines' names have science-fiction connections.

If a support staff supported these machines, however, these host names would not be much help. TechRepublic's support tech Ted Laun has worked at places where machines were named willy-nilly.

"It was cute, but it didn't do you any good," he says. Every machine has to have a host name as part of its setup, according to Laun. "You can make those names a tool to make your life easier."

Even small companies should come up with a useful naming convention for their computers. "If you start out thinking big, then there isn't a conflict later when you grow," Laun says. You don't have to waste time arguing against "this is how it's always been" when your network grows so large that cute names become a burden.

Name your client

When it comes time to name client computers, you might consider the way we do it at TechRepublic. An example of our naming convention is L2ksdf00231.

Broken down, this convention is made up of computer type/operating system/airport code/asset tag number.

Here is the convention broken down even further:

- **Computer type** is either L or D for laptop or desktop. In our example, this machine is a laptop.
- **Operating system** is 2k, NT, 95, 98, or LX for Windows 2000 Pro, NT, Windows 95/98, or Linux. In our example, the laptop is running Windows 2000 Pro.
- **Airport code** is SDF (Louisville, KY), LAX (Los Angeles), or JFK (New York). In our example, this Win2k laptop is located in Louisville, KY.
- **Asset tag number** is something like 00231 or any other short set of numbers denoting the asset tag or serial number on the machine. In our example, this laptop running Win2k in Louisville has an asset tag of 00231.

Sorting out the details

Laun says the names of the computers used at TechRepublic help him support users in a number of ways.

If someone says they are calling from a hotel room, he can sort the names in his browser list and go directly to the laptop names that begin with L. When he finds the name in his list, he will know what type of OS it is running, helping him to focus on troubleshooting techniques for that OS.

The airport code describes the home base for the laptop or where the desktop is physically located. If TechRepublic had multiple offices in New York City, we could use JFK for the office closer to John F. Kennedy International Airport or LGA for another office closer to La Guardia.

Of all the parts of our naming convention, Laun likes including the asset tag number the best. "It's really the most useful piece of information in the name," he says. Not only does it ensure, by default, that every machine has a unique identity, but it also helps with inventory tracking.

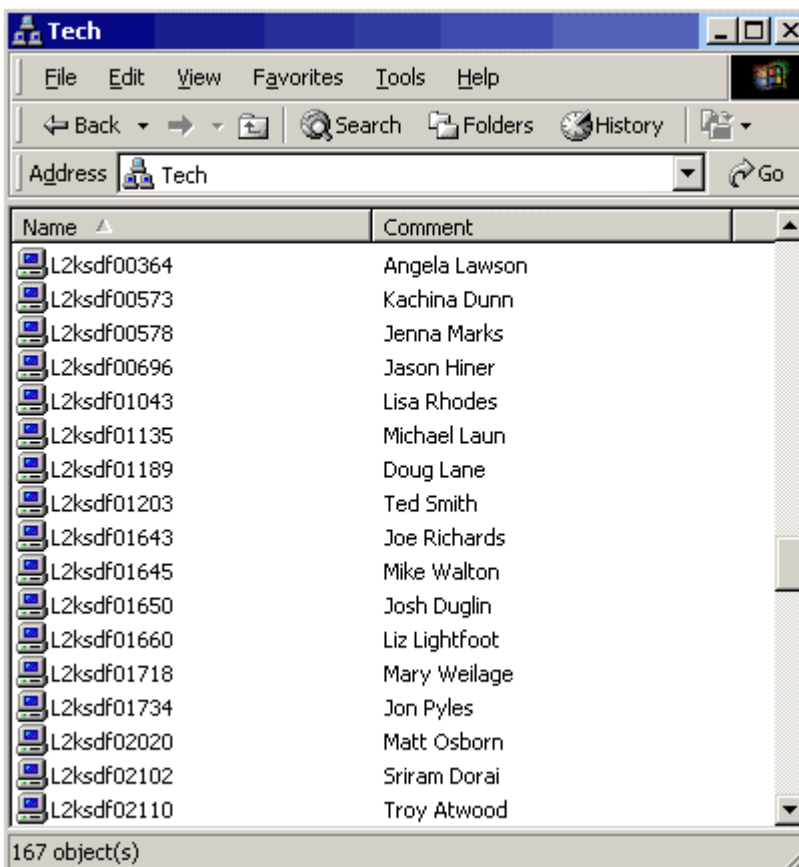
For locating computers, the asset number in the browse list is a great help. Not only do you know if the machine in question is in use, but where. It is also easy to track down the profile currently in use on the machine.

You can also add additional elements to the asset tag number if the situation warrants the extra information. For example, to help identify leasing expirations, a code letter could be added to the asset tag number.

Another place to add information about remote users' machines is the Comment field. To get to the Comment field in Windows 2000 Pro, right-click My Computer, click Manage, right-click Computer Management (Local), click Properties, and, finally, click the Network Identification tab. (Oddly enough, you can't take a shortcut by going directly to the Network Identification tab under Properties when you right-click on My Computer.)

Where the host name has ramifications on the server side of things, the Comment field doesn't have any negative effects. At TechRepublic, we use the Comment field to put the name of the client computer's user. In the network browser, in Windows 2000, when you hover over a host name in the list, the user's name appears. In the Details view in Win2k, or in the Windows XP browser list, the Comment field will show up as well. (See **Figure A.**)

Figure A



The network browser list shows both the host and user names in Details mode in Windows 2000.

Taking it server side

What works well on the client side works even better on the server side of the equation, Laun says.

Using an informative name for servers can save a lot of time and grief if your company is acquired or acquires other companies. Plus, it's much more important to get the server name right the first time because, while it may take 10 or 15 minutes to resolve problems on the server by changing a client name, a changed server name affects everyone in the organization.

At TechRepublic, we retired one of our oldest servers a month ago, and Laun is still helping people to find the new server. "I get calls every day," he says.

An example of the server-naming convention we use at TechRepublic is Tr2ksdfpdc.

Broken down, this convention is company name/operating system/airport code/main function of the server.

Server names differ from client names in their first and last elements. Here are the two different features:

- **Company name** is Tr or IBM for TechRepublic or IBM. In our example, Tr stands for TechRepublic.

- **Main function of the server** is PDC, BDC, or SQL for primary domain controller, backup domain controller, or SQL database. In our example, we have a TechRepublic Win2k server in Louisville that has a main function of serving as a primary domain controller.

The addition of the company name at the beginning may seem unnecessary, unless your company expands through acquisition. If several companies end up working under the same corporate umbrella, it will be easy to sort through the network browser list if the first few letters of the host name are unique to your organization.

You can also use the Comment field to add a short list of other functions that are housed there. For example, if your DNS services are run on your PDC, the host name would reflect the PDC part, but the Comment field could list DNS as a service.

Personal digital assistant support best practices

Aug 22, 2001 | Gartner | [E-Mail](#) | [Archive](#)

Personal digital assistants are the new personal computing revolution. Enterprises must develop support plans to minimize support costs and security risks.

The proliferation in mobile devices for immediate information access and work styles is quickly distorting the desktop/laptop hardware scenario. Consumer toys have invaded the enterprise—and users expect to perform their jobs with these toys. A few years ago, enterprises could ignore these devices because their entry cost was high. Now, however, the entry cost is dropping to less than \$150.

These devices seem to be impossible to manage in a business environment, when their configurations tend to be informal. However, most enterprises cannot afford not to attempt to manage them, because they are already having a massive effect on user productivity. Through adoption of multiple mobile-computing appliances, users are creating the age of the “personal area network.” But as every IT manager knows, user problems will eventually become IT problems, and the increase in complexity will be significant.

Best Practice No. 1: Every enterprise must develop a policy regarding PDAs.

Enterprises that decide not to support PDAs must issue a formal policy statement to their employees explaining the reasons for the decision. Any condition offered, such as “not suited to the needs of the job,” “security risk,” or “too expensive to manage,” is debatable in the minds of individual users, who will still buy PDAs on their own. Enterprises that wish to enforce the policy must give clear examples of acceptable personal use of PDAs vs. unacceptable links between PDAs and company systems. A comparison to a paper-based organizer might be considered. (See **Figure A.**)

Figure A

Comparing paper organizers to PDAs: A subjective example		
	Paper organizer	PDA
Basic entry cost	\$15-\$100	\$100-\$500
Life span	18-month life span (refillable)	Features obsolete in one year
Skill requirement	Basic reading and writing	PC-literate
Typical contents	Key contacts and appointments	10,000+ contacts, e-mails, appts., not prioritized
Fragility	Survives everything but fire	Prey to water, dust, heat, dropping, smashing, electric fields, etc.
Security	Possession	Optional, usually not activated
Add-ons	Maps, penholders, etc. (less than \$50)	Utilities, games, etc. (more than \$50)
Enterprise support	Order from office catalog	Training, sync, backup, security, network, audit, hardware/OS

In the paper analogy, employees can manually input or restrictively copy the most important items of their schedule into their personal PDAs but cannot link to a company PC and download e-mails, company

contacts/directories, etc. Enterprises that will support PDAs should review what they have learned from managing remote and mobile PCs, and then apply the rest of the recommendations in this Research Note.

Best Practice No. 2: Enterprises should purchase PDAs for employees, rather than wait for employees to purchase their own. The IS organization must educate management that ownership is a prerequisite for stability and lower TCO.

Today, most PDAs are purchased by individuals. However, as these devices begin to hold ever-more-sensitive corporate data, they must become managed assets. Enterprises should purchase PDAs for users to eliminate the uncertainty of who controls the data on the device. In this way, enterprises can ensure that their policies regarding personal and corporate information are implemented, thereby improving security and information management.

Best Practice No. 3: The IS organization should use Gartner TCO models to estimate the impact of PDAs so that expenditures on management solutions may be justified.

As PDAs are “asset tagged” and supported within the enterprise, they incur costs similar to those found on notebooks and other enterprise-owned devices. Thus, what may appear to be an inexpensive device adopts costs similar to other client computers due to the tasks required to support it. Through 2005, PDAs and other mobile appliances will raise enterprise TCO for client devices by 10 percent (0.7 probability). Individual PDAs can cost more than \$2,500 per year to maintain at a standard comparable to a workstation. IT management must demonstrate to upper management and business-unit management that PDAs are following the same life cycle that PCs followed in the 1980s and will have the same organizational impact. PCs were smaller than mainframes, but size didn’t matter when it came to TCO and work style changes. PDAs are smaller than PCs. Again, size doesn’t matter.

Gartner’s analysis of TCO for PDAs is based on a review of Windows CE and PalmOS platforms. Capital costs are based on a device costing \$450, in addition to a travel kit costing \$50. Provisions are included for lost devices. Administration costs are considered equal for both platforms. Technical support costs are slightly higher for Windows CE due to its more complex user interface. End-user operation costs represent about 40 percent of all costs, primarily due to the time investment required to keep PDAs synchronized with user desktops or servers. Even at as little as five minutes per day (Gartner estimate), synchronization is a new diversion of user time that costs enterprises hard productivity losses. By 2002, data synchronization will consume one hour per day, per end user, per personal area network (0.7 probability).

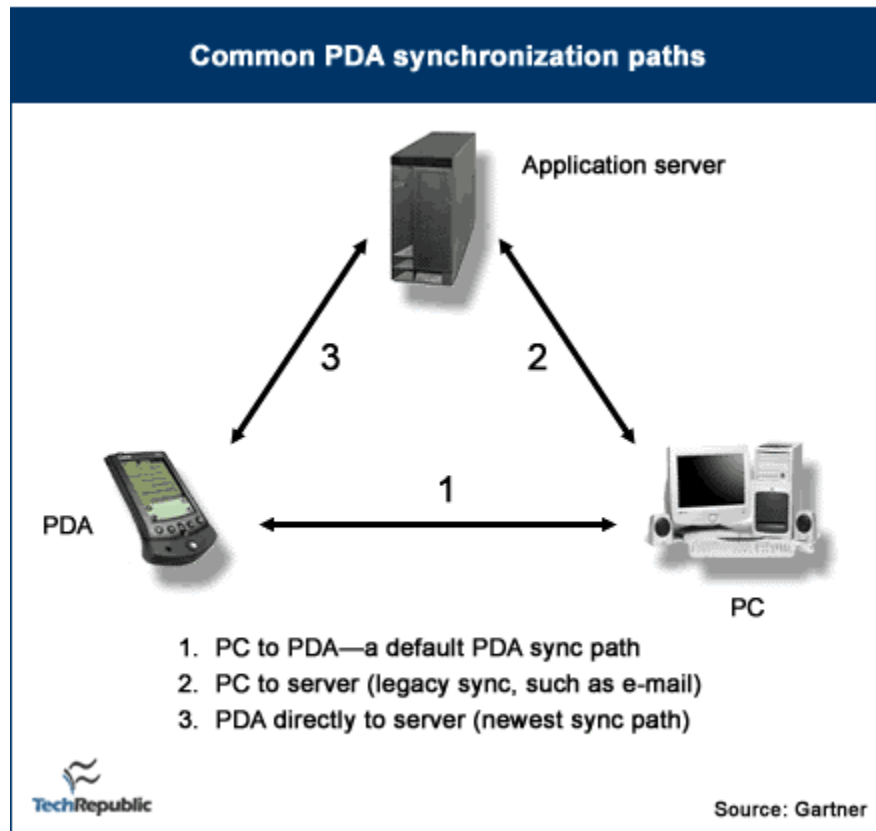
Best Practice No. 4: To constrain budget growth, the IS organization must move to a user-based budget for hardware deployment plan vs. the specific device profiles now in use.

IS organizations can consider a program from which users can select their own choices from an approved IT product list. Gartner compares this scenario to the methods used to offer healthcare options to employees. Each user is given a budget amount that should permit a sufficient number of productivity tools tailored to their individual needs. Users then select from a list of supported IT products, up to the amount of the budget. This plan should result in higher utilization of products and users who are more pleased with what they are given. Business units must, in turn, commit to allocate per-capita budget funds to support the selection of PDAs. Rather than forcing specific devices onto users, IS will be seen as giving users the choice of a range of devices, all of which happen to be configurations that are supportable by the enterprise help desk.

Best Practice No. 5: The IS organization must set standards for synchronization products that support a wide variety of consumer appliances. It should not permit users to install their own synchronization tools.

There are many popular products for general-purpose synchronization, available as independent retail products, as shareware, and bundled with PDAs at purchase time. All synchronization products are immature. Future products should manage referential integrity and authentication for all three common PDA synchronization paths and provide for an administrative console. (See **Figure B.**)

Figure B



Gartner recommends that PDA synchronization standards be set immediately to ensure that the line between the controlled enterprise and the uncontrolled personal world of the employee remains intact. More practices related to synchronization include:

- Synchronize regularly.
- Expect the unexpected.
- Discard all bundled software.
- Protect the data and encrypt it.
- Synchronize multiple devices in parallel.
- Control, test, and approve access methods.
- Control, test, and approve introduction of new device types and their OSs.
- Formalize the process—make it a user habit, but make it easy for the user to be successful.

Best Practice No. 6: The IS organization must set standards for device security.

Most PDAs power on by default with no security. Security settings for power-on passwords and hidden files have been mostly optional and can be turned off by the user. Default encryption may involve simple keys that are known to hackers. When placed on networks, PDAs may be vulnerable to DOS and spoofing attacks. To reduce these risks, enterprises must specify not only which brands of PDAs will be supported but also what OS versions will be supported, because over time, all OS vendors gradually fix the holes in their software. Ancient PDAs drawn from users' closets or handed down from friends are not suitable to withstand today's sophisticated hackers and thieves.

Enterprises must also specify what kind of power-on protection practices must be followed, as well as approved methods for file and network encryption. Products such as Communication Intelligence's (CIC's) Sign-On leverage the pen pad to enable users to sign on with their signature, or even a "secret doodle." VPN, authentication tokens, and PKI must be considered for sensitive applications, especially if they will be accessed over the Internet. More practices related to security include: 1) discard bundled security software and 2) provide all users with approved security software and training on how to use it. As with synchronization, formalize the process—make it a user habit, but make it easy for the user to be successful.

Best Practice No. 7: The enterprise help desk must create PDA-friendly services.

The enterprise should maintain swap pools of spares of the most popular PDAs, not as loaners, but as replacement systems. Employees must not send damaged or broken PDAs to retail service centers, because their PDAs are replaced, not repaired, and any data that was accessible on the PDA would then be potentially available to buyers of surplus equipment. The enterprise's synchronization plan must include the capability for the help desk to reimage the user's PDA from the last performed synchronization with the user's laptop, or vice versa. Any units to be discarded or returned to manufacturers need to have their memories erased before leaving company control.

Best Practice No. 8: When designing wireless online applications, enterprises should minimize the need for critical local data by using thin-client interfaces.

PDAs are capable of supporting open environments such as SSL-based Web screens, Java, and XML, as well as proprietary thin clients such as Citrix Systems' ICA and Symantec PC Anywhere. Whenever a user's application requirement dictates online access to services, thin-client displays should be given priority to reduce the amount of local application and data that will need to be developed for the PDA. The same TCO benefits of thin clients on PCs apply conceptually to PDAs.

Best Practice No. 9: Provide PDA-relevant training.

Enterprises will quickly acquire a baseline of experience with common problems, tips, and techniques. PDA users should be given access to this knowledge through courses, online "Webinars" (including playback), and FAQ files available online and downloaded to PCs and PDAs.

Bottom line

While still considered by many IT managers as consumer technology, PDAs have become the new-millennium equivalent of the PC revolution of the 1980s. IS organizations must begin to bring these devices into the PC support venue and thus must begin to assess TCO and its implications. Through 2005, PDAs will be the biggest challenge to manage and control among end-user platform choices, and the hardest on which to objectively prove ROI.

Gartner originally published this report on June 27, 2001.

Copyright: 2000-2001 by Gartner Group, Inc. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness, or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.