



Preventing Data Loss & Preparing for Disaster White Paper

Keeping Information Assets Secure

© 2004 Technical Research Group All rights reserved. 2850 Red Hill Ave. Suite 110, Santa Ana, CA 92705, 949.296.8380
Reproduction in whole or in part without written permission is prohibited. All product names are trade and service marks of their respective companies.

949.296.8380 • 949.756.0029 Fax • 2850 Red Hill Ave • Suite 110 • Santa Ana, CA 92705
www.picktrg.com

Table of Contents

Preventing Data Loss & Preparing for Disaster	1
Keeping Information Assets Secure	1
Table of Contents	1
Table of Contents	2
Executive Summary	3
Advantage:	8
Disadvantage:	8
Advantage:	10
Disadvantage:	10
Advantage:	10
Disadvantage:	10
Appendix A: About TRG	20
Why Choose TRG	21
Philosophy	21
Technology Partners	22
Software Products	22
Hardware Products	22
Business Partners	23
TRG Qualifications	24
Technology Marketplace	25
Contact Information	25
More Information	26

Executive Summary

In many organizations, data loss disasters are becoming increasingly commonplace. Ironically the value of a company's information asset is usually not appreciated until its gone. Hardware can be replaced as can software but unless properly backed up and secured once data is gone it could be gone forever. This becomes even more apparent as companies move to more paperless environments. The increases in data loss disasters is do in part to the quickly changing computer technologies, the tremendous volume of data generated by organizations, staff downsizing, lack of computer technicians, and the decentralized way that data is produced, assembled and put in safekeeping locations. As organizations continue to access the Internet more frequently and use electronic mail (e-mail), apprehensions with data integrity and data security are compounded daily. Lost data and disaster recovery is understandably a top concern today for most organizations. While many organizations may have disaster backup and recovery plans in place, a surprising few have yet to test backup plans and security mechanisms.

As organizations realize the importance of data protection, most organizations do not realize that data has been lost or corrupted until it is too late. This accentuates the emphasis organizations must place on fully understanding the professional, financial and legal implications of data loss, while proactively exploring the options available for maintaining data integrity and information security before data loss occurs. As data is one of an organization's greatest assets, preventing devastating data loss should be the primary goal of Information Technology (IT) management.

This paper provides an outline of the necessary steps to setup backup plans and the follow-through required to ensure that recovery plans can restore the organization's data when the unexpected occurs. Additionally, a list of items to safeguard your valuable data and computer system are detailed in this paper, along with an outline on the steps and necessary follow-through required to ensure that recovery plans can restore data.

This paper provides what industry analysts report on disaster recovery and the dynamic aspects if there is not a program in place to prevent data loss, in addition to a well-tested data recovery program for your organization.

The following topics are covered in this paper:

- What are the causes of data loss?
- When is data recovery necessary?
- Personnel and training regarding data loss
- Security strategies and mechanisms
- Data backups
- Testing of data backups
- Power protection
- Restoring data strategies
- Storage devices
- Media types
- Collection of media and system information
- Procedures for system maintenance
- What the industry experts report
- What is the future?
- Who can help?

What are the causes of data loss?

There are many causes of data loss. Listed below are a few of the most common causes for lost data:

- Human error
- Hardware failure
- Software failure
- Natural disasters
- Viruses
- Vandalism
- Theft

When is data recovery necessary?

Recovering data might be necessary when the following occurs:

- A new system is installed to replace the existing system.
- Hardware failure, such as disk crash or faulty power, where data on disk is no longer there or is corrupted.
- The organization falls victim to a computer system crime.
- Viruses are introduced in a system.
- Human error causes deletion of important data.

Personnel and Training regarding Data Loss

Unintentional employee error is believed to be the single largest factor behind data losses. Inform your computer users of the importance of your organization's data and reference this paper. Identify one person as the computer system administrator and have another person assigned as the backup person if the system administrator is unavailable. These individuals should know how to perform backups, shutdown the computer system and bring up the computer system. These procedures should be documented and placed near the computer system.

Be sure that your employees know what software they can load onto the computer system and what e-mail attachments they can access safely. Instruction should be given on why it is important to never run, or even download, a program from an un-trusted source. It is critical to instill the proper discipline and mindset in your organization, to adhere to resilient security procedures, and devote the necessary resources to the security infrastructure.

In minimum-security and medium-security networks, grant backup rights to one user and restore rights to a different user. Train personnel with restore rights to perform all of the restore tasks if the administrator is unavailable. In a high-security network, only administrators should restore files.

If training is necessary, please contact a company that has proven experts and experience in the necessary technology and procedures. Training should begin immediately following an employee's start at the organization and continued on a regular basis. Employee training is well worth the investment.

Security Strategies and Mechanisms

It is important to keep the organization's computer systems secure. Unfortunately, there are individuals that try to get into computer systems and destroy the data. Have passwords on all logons, including seldom used or demo accounts. If you have a Web site, make sure to properly set up the firewall. Be sure that all security patches are loaded. Make sure that you have current virus protection software loaded and running on your computer system. An organization needs to realize that they are at war with individuals who are trying to steal intellectual property or disrupt business operations for their own purposes, regardless of whether the organization is a small startup or a large well-established organization. Secure both the storage device and the backup media. It is possible for someone to access your data from stolen media, such as a backup tape, by restoring the data to another server for which they are an administrator.

Data Backups

Several steps are required to enhance the security and operation of your backup-and-restore operations. When you develop a backup plan, consider the following methods:

- Secure both the storage device and the backup media. The storage device (usually part of the server) should be in a locked room. Backup media, such as tapes, should be in a locked cabinet or fireproof safe. Data can be retrieved from stolen media and restored to another computer.
- Keep at least three current copies of backup media. Store one copy at an off-site location in a properly controlled, secure environment.

Data can be backed up onto media such as tape or to disk including disk that is on another computer system.

Perform a backup of your computer system on any day that there is activity on the computer system. Keep a log of backups and verify that the backup was successful. Maintain a tape backup library. Do not use the same tape over and over again. Have a different tape for each day of the week. Month-end and year-end tapes should be put away and not used again, except for emergencies.

How do you ensure continuity? Two options include duplicating and storing data at a second location and using a data backup service to prevent data loss when disaster strikes. One strategy is to maintain two identical stores of your organization's data. Placing two stores in separate locations, or data co-location, requires that you duplicate and routinely back up

your organization's data and store it in a place other than the organization's main office. Subsequently, if the organization's main office is destroyed, users in other locations can access the stored data and continue operating with your organization. Data co-location is a good way to be prepared for a disaster, as you are spreading your risk of loss on two locations. The strategy makes sense for organizations of all sizes.

The following are suggestions for backup strategies:

- ***Performing a backup whenever the system changes***
Always create a backup when the operating system changes. For example, whenever you install a new driver, or apply a Service Pack. This will allow you to more easily recover from a system failure.
- ***Creating a backup log***
Always create and print a backup log for each backup. The backup log is helpful when restoring data; you can print it or read it from any text editor. Also, if the tape containing the backup set catalog is corrupted, the printed log can help you locate a file.
- ***Retaining copies***
Keep three copies of the media. Keep at least one copy offsite in a properly controlled environment. It is not recommended to keep backup tapes in an automobile that has the potential of becoming very hot.

Whether you run remote backups from a local computer or a server, you should place the storage device on the portion of your network that has the greatest bandwidth or highest transmission frequency.

There are several types of backups:

Normal (Full)

A normal backup copies all files and marks each as backed up. With normal or full backups, you need only the most recent copy of the backup file to restore all the files.

Advantage:

Easy-to-find files because they are always on a current backup of your system or on one medium. File restoration from only one medium or set of media.

Disadvantage:

Most time consumed. Redundant backups if files do not change frequently. Requires more disk, tape, or network drive space.

Incremental

An incremental backup copies only those files that were created or changed since the last normal or incremental backup, and marks files as backed up. If you implement a

combination of normal and incremental backups, you must have the most recent normal backup set, as well as all the incremental backup sets, to restore your data.

Advantage:

Least required data storage space. Least time consumed.

Disadvantage:

Difficult to find files, because they can be on several types of media.

○ ***Differential***

A differential backup copies files that were created or changed since the last normal or incremental backup, but does not mark files as backed up. If you implement a combination of normal and differential backups, you must have the last normal and last differential backup sets to restore your data.

Advantage:

Need for only the last normal backup medium and last differential medium. Less time consumed than normal backups.

Disadvantage:

Longer restoration time than if files were on a single medium. If large amounts of data change daily, longer backup time.

Copy

A copy backup copies all selected files; however, this does not mark each file as backed up. This type of backup is useful between normal and incremental backups, because it does not affect other backup operations.

Daily

A daily backup copies all selected files that have been changed on the day the daily backup is performed. The backed up files are not marked as backed up.

Four Golden Rules of Data Protection

Listed below, and in summary of Data Backups, are four simple rules of data protection that should methodically be followed by every organization.

1. *Have a backup plan and back up every day.*
2. *Have a tape rotation plan.* Do not use the same tape cartridge two days in a row. If your system fails, you might lose both your disk data and the tape data—a disaster!
3. *Store a complete backup copy off site.* Always ensure that a backup, less than a week old, is kept at a different location.
4. *Test to make sure you can restore from your backup tapes.*

Testing of Backups

The best way to ensure that your storage devices and media are working correctly is to regularly verify your backups by restoring files from different locations on the backup media or from multiple tapes. Perform a trial restoration periodically to verify that your files are properly backed up. It is recommended to do this at least twice a year. Complete verification of the entire backup and restore process is critical.

Power Protection

A plan should be initiated to develop backup and restore strategies with appropriate resources and personnel, and then test them. Testing backup strategies also shows how much time is required to restore data, and a good backup plan ensures fast restoration of lost data. Additionally, a trial restoration can uncover hardware problems that do not show up during software verification.

It is important to remember to periodically perform a test of your Uninterruptible Power Supply (UPS) or battery backup. Often, this is overlooked in the data protection program. With surges and spikes, if you are reading or writing to disk when a spike is received, it will corrupt the data transfer and could, if strong enough, damage the media. Power Harmonics /EMI/RFI—these come through the AC line and they can be caused by large non-linear loads starting and or stopping, motors. Noisy inductive loads, like a coil in a coke

machine radiate RF, as it does from a TV or transmitter. RF can be introduced directly into the computer if it is close enough and or strong enough.

Loss of power, or a dip in power, is the same as not shutting down properly. A power dip, if it is low enough, is where the power supply hang time is exceeded and will cause data transfer to be interrupted and corrupted. A good UPS will protect against brown-outs (power dip) and blackouts. The best UPS's also have surge and EMI/RFI built into them. A good surge strip will also protect against EMI/RFI.

Restoring Data Strategies

Listed is a summary of valuable tips for restoring data:

- Before you restore from tape, create a bootable floppy disk tape and an emergency repair disk. You never know when they will be needed. It is recommended that this is stored in a known and secure area.
- Store a print screen of Disk Administrator and a printout of Boot.ini off-site with your tapes. If possible, when you start to recover a server, duplicate the entire disk configuration. The target server should have the same number of logical drives. Partitions should be located on the same disks as the original system and be assigned the same drive letters. Whenever you change the disk configuration, make certain you update this information.
- If possible, log off the server during the restore. This will reduce the number of files in use at the time of the restore. If you do not, errors will be received when the current user profile is restored.
- It's a good plan to have your system and boot partitions on a standard SCSI controller without hardware RAID (Redundant Array of Independent Disks). You can use software RAID to provide fault tolerance. Using standard (natively supported) drivers for your boot and system drives makes recovery much smoother. It is recommended to have more than one disk with information on it, just in case one disk fails. Recommended are RAID 1 (mirroring) or RAID 5.
- Document your current service pack level and all hot fixes applied to the server. Store this information off-site with your tapes. Applications can be inconsistent about the service pack they run. Disaster recovery is not the time to be testing an application with a new service pack.
- Make a custom CD with your Operating System (OS), service packs, hot fixes, and backup software on it. Store it with the tapes and the rest of your systems documentation off-site. Remember to update it as your system changes.
- Store the account name and password for the local administrator account off-site with your tapes. A local administrator account will be needed on the server. If the server was a member of a domain, and the domain controller is not available, having a local account is the only way you will be able to log on. If your password has changed since the backups were created, you will need to know the old password.

Storage Devices

Storage technology changes rapidly, so it is important to research the merits of various media before making a purchase. When deciding on a storage device, consider drive and media costs, as well as reliability and capacity. An ideal storage device has more than enough capacity to back up your largest server and can also detect and correct errors during backup and restore operations. Be certain your storage device on your backup server, if you have one, is the same as the storage device on your primary server. This will enable you to restore data to your backup server.

Media Types

The most common type of storage medium is magnetic tape. The primary tape drives used for backup include quarter-inch cartridges (QIC), digital audio tapes (DAT), 8-millimeter (mm) cassettes, and digital linear tapes (DLT). High-capacity, high-performance tape drives normally use small computer system interface (SCSI) controllers. Other types of media include hard disks, magnetic disks, and network drives. The preferred method of backup is a combination of disk and tape.

Never trust floppy type media for backups or long-term storage. Bad media mostly happens on floppy type material going bad.

Collection of Media and System Information

It is important to collect basic information about your system and store it in a safe place before a disaster occurs. Any important information should be documented and easily accessible, such as disk configurations, computer names and IP Addresses. This information is vital when restoring your system.

Locate key software media (diskettes, CDs, tapes) and store them in a secure area near the computer. This software should include operating system, database and application. If you need to reload your computer system, then this software along with your backup tapes will be necessary. These procedures should be documented and placed near the computer system.

Procedures for System Maintenance

As the old adage states, "An ounce of Prevention is worth a pound of Cure." If you adhere to the following procedures, it will be well worth the time invested:

- Never turn off your computer system without executing a proper shutdown. Not shutting down properly could cause file(s) to be left open and data to become a lost chain, or totally unreadable.
- Clean your tape drive periodically. Refer to the tape drive manual for frequency and procedure.
- Check the amount of disk space available on your computer system periodically. The time to add disk space or delete unnecessary files is before the computer system runs out of room.
- Check the sizes of your files periodically. Improper file sizes can affect the performance of your computer system.
- Perform a trial restoration periodically to verify that your files were properly backed up. A trial restoration can uncover hardware problems that do not show up with software verifications.
- Keep your computer room clean from dirt and dust. Dirt and dust might affect your computers.
- Maintain the proper temperature in your computer room. Hot temperatures could affect your computers.

What the Industry Experts Report

All of the industry experts agree that an organization must have a program in place to prevent data loss, along with a well-tested data recovery program. Listed below are a few interesting and amazing statistics:

- Human error accounts for approximately 80 percent of data loss.
- The cost of data replacement is estimated at an astounding 100 to 500 thousand dollars per gigabyte.
- Most organizations without a reliable back-up system never recover from significant data loss.

- A recent research report by an IT management consulting firm, Compass, stated that only 25 percent of UNIX midrange data centers have a disaster recovery plan in place. Moreover, one-third of those surveyed with a recovery plan in place have yet to test it. The research was based on performance analyses of approximately 150 midrange data centers over 18 months.
- According to a Gartner report, after September 11, 2001, "...enterprise decision makers understand why business continuity is important: The survival of the enterprise depends on it."
- Experts agree that lack of follow-through on IT testing and mock-scenario response is mainly due to human nature, and not an intentional oversight. Bill Van Emburg, cofounder and COO of Quadrix Solutions in Piscataway, NJ points out that fully tested disaster recovery programs are the primary reason why New York organizations were back to work so quickly after being the target of terrorist acts.

What is the Future?

Implementing a data protection and disaster recover program today is the first point, experts stress. It is never too late to put an IT disaster recovery and response program together. The other, and significantly important point that is really overlooked, is that some organizations put programs in place, however, they never test the plan.

Because more and more employees work from home and travel with laptop computers, top priorities for organizations are ensuring that all their desktop and laptop users are saving critical files to a shared network, where the files can be backed up. Employers are also ensuring that they have up-to-date, standard hard drive images for all the computers in use by employees. Having data available will not help employees much if the office is gone; however, one way many organizations are preparing for the loss of a facility is by giving their employees a way to access their networks from home computers.

Recent years have seen the development of less expensive and more powerful hardware. In addition, there is now software that harnesses the hardware to open new vistas for computer users, as well as advancements in cryptography and other high technology sciences. It is enticing to believe that technology can produce a risk-free world; however, this is just not realistic.

Perfect security requires a level of perfection that does not exist and, in all likelihood, probably never will exist. Software development is not a perfect science and all software has bugs, which can be exploited to cause security violations. Therefore, it is essential to maintain solid security and recognize that this is an ongoing process.

In today's business environment, the loss of critical business assets can have serious negative impact in real dollars, lost opportunity, customer dissatisfaction, shareholder insecurities, and damaged corporate image.

Computer downtime costs U.S. organizations billions of dollars every year. An organization can protect itself by developing and maintaining the proper infrastructure for data backup and recovery internally; however, a professional should be consulted to ensure all safe guards are in place and that include the latest technologies.

Who can help?

Not all organizations can implement a data protection and disaster recovery program on their own. Therefore, a knowledgeable, responsible company should be used. Selecting the best company for protecting your organization's valuable asset is an important decision for your organization. It should be someone you trust, is agreeable to work with, is experienced, and has the ability to work through challenges.

Whenever in doubt, or if you have any questions, contact your IT support supplier. If your computer system is not performing normally, contact your IT support supplier promptly and allow their experts to investigate the situation. For easy and convenient access, please have your IT support supplier's phone number located near the computer.

Conclusion

True, your backup data is worthless—until you need it. Then it is priceless. When you need to recover your business data, the success of your backups becomes most critical. Maintaining the integrity of your data can be challenging; however, one of your most valuable business assets may be at risk. A good backup program ensures that you can quickly recover your data if it is lost.

Regular backup of local hard disks prevents data loss from a disk or drive failure, disk controller errors, power outages, viruses, and other serious problems. Careful planning of backup operations and reliable equipment can make file recovery easier and faster.

Since servers are as individual as people, with each one having its own quirks and whims, each system needs to be tested. A good rule of thumb is that, until the data is recovered and tested on the recovered server several times, it is probable that all of the possible problems have not been discovered. Therefore, it is suggested to follow these guidelines:

- **Be prepared.** Take time to consider the possibilities of what could happen, envision the worst-case scenario, and plan accordingly. This will ensure that all measures are incorporated, which could also be applied to lesser emergencies.
- **Document your plan.** Put the plan on paper and go over the plan with the appropriate personnel. Your employees need to know the procedures that are in place in order to carry out the plan. Documentation, training and education are critical to ensuring that people are ready to act when a crisis occurs.
- **Back up the data.** Part of the day-to-day activity within the organization should include backing up data and documents. It is recommended to keep one copy of the backup media and documentation in a fireproof box on-site and keep duplicate sets off-site.
- **Define roles and responsibilities.** Designate emergency managers within the organization to handle procedures in case of a disaster. Define their roles and make sure everyone knows their responsibilities in case of an emergency.
- **Select alternate locations.** Identify, in advance, where the organization would relocate in a disaster scenario. Select primary, secondary, and third-choice options, any of which could possibly mean relocating to a different building, another city, or another state.
- **Educate & train employees.** Be sure that everyone in the organization knows emergency evacuation exits and processes in place for shutting down systems in an emergency situation.
- **Review.** Review the disaster recovery plan at least once every year and update the plan with current information.

People, not computers, recover from disasters. Because of this, your data loss and disaster recovery plan must be detailed enough so that employees know their responsibilities, what resources they will need, how they are to accomplish them, who they can expect to assist them, and the timeframe they have to complete their responsibilities.

TRG's Approach to Protecting Your Information

TRG's approach to improving the safeguarding of your company's critical information insures that the effort is successful. The process consists of the following:

- Formal Assessment of the Client's Needs

During this phase of the effort TRG meets with top management and other key personnel to identify the gaps between existing information asset safeguards and the level of safeguards needed to protect the business. The business disruption risks are assessed and a program tailored to fit the company's specific issues and requirements is developed.

- Creation of a Report & Plan Detailing
 - Current Areas of Risk,
 - Backup Practices
 - Fault Tolerance of Network
 - Remote Hot Site Evaluation
 - Security, Virus and Firewall Quality
 - Evaluation of Alternatives,
 - Costs
 - Benefits
 - Technology Required
 - Software Required
 - Management Processes
 - Recommended Approach
 - Work Plan for Deployment
 - Training, and
 - Ongoing Support

TRG works closely with the client to schedule and implement each step of the plan. Throughout the process TRG insures that the implementation goes smooth and without disruption of client's workforce.

Appendix A: About TRG

Why Choose TRG

Technical Resource Group (TRG), headquartered in Santa Ana, California, was formed in 1995. TRG has a group of dedicated expert consultants who work together to align information technology with the business needs of its clients. TRG is highly respected in the business technology arena as well as being known for their service and support integration expertise. TRG has a long and successful proven track record. TRG's growing team of professional, high technology experts includes individuals that work together to solve business needs in today's ever-changing marketplace. TRG also has an outside team of nationally recognized experts in areas of strategic planning, business process improvement and key industry consultants that are available when their individual expertise and knowledge is required to assist the TRG team to solve client business challenges. Over the years, TRG has successfully partnered with its clients to deliver solutions in the areas of

- Strategic IT Planning and Deployment
- Business Process Improvement
- Application Evaluation, Selection & Implementation
- Custom Application Design and Development
- Infrastructure and Network Planning, Implementation & Management
- IT Facilities Management
- IT Security Administration
- Business Intelligence and Data Warehousing
- Document & Workflow Management

TRG has over 400 clients throughout the United States with a majority in the Southern California area. The company's loyal client base ranges from single user installations to the Los Angeles Unified School District that has a 1000-user installation. Talent, variety, size and stability—TRG has all the qualities and expertise that create a successful IT service company.

Philosophy

TRG's philosophy is to give its clients a personal touch; however, still have a company structure and strength behind that personal touch.

Goal

TRG's goal is to be the company our clients and prospects call for all their information technology and computing needs. TRG wants leverage its client's growth and sustained prosperity. TRG's team strives to deliver the best services, products and information possible to their clients and to provide them with in-depth insight, technical knowledge and solutions for the success of the organization.

Technology Partners

TRG is proud to offer excellent powerful and high performance products and specialized services from these industry-leading technology companies:

Software Products

- **Microsoft**—Windows Operating Systems: 2000/2003/XP and related products such as Office, Exchange, IIS, VB & SQL Server
- **IBM**—Database Products & Tools such as UniVerse, UniData, wIntegrate & SB+
- **SurfControl**—E-mail and Web Filtering
- **Raining Data** (formally Pick Systems)—Database Products & Tools such as D3, mv.BASE, mv.ENTERPRISE & FlashCONNECT
- **jBASE**—Database Products & Tools
- **MITs**—Business Intelligence Products
- **Accusoft**—AccuTerm Terminal Emulator
- **Esker Software**—DeliveryWare & VSI-FAX Fax Server
- **Keynet**—Imaging Solutions
- **Symantec**—pcAnywhere & Norton AntiVirus
- **Veritas**—Backup Exec
- **Via Systems**—Viaduct Terminal Emulator
- **AcuPrint**—Secure Printing

Hardware Products

- Hewlett-Packard/Compaq—Intel-based Servers
- IBM—RS/6000 (pSeries) Servers
- Wyse—Wintertms/Thin Clients
- APC—Uninterruptible Power Supplies
- PF Micro— Intel-based Servers

Business Partners

- ***The Natural Intelligence Group (TNIG)***—Management Consultancy for business process improvement and reengineering
- ***Hartley & Associates***—Professional Services include Interim Management, Organization Building, Recruiting, Sales, Marketing & Advertising

TRG's account managers, technicians and consultants work closely with its partners to develop solutions for specific clients' needs and to assist with every challenge for all types and sizes of organizations.

TRG Qualifications

- Windows Terminal Server professionals on staff. At recent and upcoming trade shows, TRG is giving presentations on the benefits of Citrix, Windows Terminal Services and Thin Clients. Internally, TRG uses Thin Clients and Windows Terminal Services.
- Microsoft Certified Partner that has expertise in supporting Windows NT/2000/2003/XP, Exchange Server, Proxy Server, IIS and Excel. TRG has full-time Microsoft certified staff members (MCSE, MCP, MOUS).
- Authorized IBM reseller including UniVerse and UniData database products and tools and MITS business intelligence product and have on staff AIX operating system experts.
- Over 175 years of MultiValue/Pick application design, programming and support.
- Single Source for Hardware, Software and Services, if client desires a single source. Or, if client chooses, TRG can provide one piece of the puzzle if the client has coverage in other areas.
- Authorized Hewlett-Packard/Compaq Reseller (VAR) with Certified professionals (ASE) on staff.
- Value Added Reseller for all Raining Data products and tools including D3, mv.BASE, mv.ENTERPRISE and FlashCONNECT.
- Reseller of numerous supplementary products such as APC uninterruptible power supplies (UPS), Esker VSI-FAX faxing software, Keynet Imaging, AccuTerm terminal emulator, print servers, etc. that are important and necessary for TRG clients' IT requirements.
- Windows application and Web development teams that are knowledgeable in Visual Basic, SQL Server, FrontPage, HTML, etc.
- Professional Service employee consulting staff, in addition to specialized outside consultants to assist TRG employees when appropriate to solve the business needs of TRG's Clients.

TRG meets all the necessary qualifications for implementing data protection technology and processes in an organization and has excellent references. In addition to referenceable clients such as Aloha Freight Forwarders and Pindler & Pindler, TRG has implemented data protection technology and processes internally for all the same reasons mentioned in this paper.

TRG has dedicated and experienced resources to work with an organization to define needs, costs, options, and possible cost savings. TRG has experts in solving interoperability issues between existing desktop hardware, operating system platforms and Windows NT/2000/2003-based applications. Additionally, TRG has a proven track record after years of innovation and achievement and, as a technology leader, can bring more overall market understanding to data protection technology. With TRG's unparalleled experts in business solutions, TRG can assure organizations a greatly enhanced protected environment. For more information on data protection technology, visit www.picktrg.com.

Technology Marketplace

Organizations can choose a large and expensive consulting company that may not take the time to know the organization or their current technology. Organizations can choose a one-man shop that does not have the technology expertise in all the areas the organization needs and cannot keep pace with the ever-changing technology. A single person cannot possibly be knowledgeable in all areas of Information Technology (IT). There is also the high probability that the one-man shop might be out of business tomorrow.

TRG's team specializes in emerging technology solutions. TRG's service offerings include advisory, consulting and assessment services. TRG's close-knit team can bridge the gap between complex non-Windows based IT infrastructures such as UNIX and Windows NT/2000-based environments. TRG has the expertise that can provide cost-effective solutions that are specific to organizations in all their IT needs and business-critical applications.

Contact Information

Technical Resource Group (TRG)
2850 Red Hill Ave. Suite 110
Santa Ana, CA 92705
949.296.8380— Fax 949.756.0029
E-mail: asktrg@picktrg.com
Web Site: www.picktrg.com

More Information

For the latest information about our products and services, please see the following:

www.picktrg.com