Payoff
This article describes the process of business recovery planning specifically for local area networks (LANs) and the components that comprise the LAN. These procedures can be applied to companies of any size and for a recovery scope ranging from operational to catastrophic events.

Introduction
Today's organizations, in their efforts to reduce costs, are streamlining layers of management while implementing more complex matrices of control and reporting. Distributed systems have facilitated the reshaping of these organizations by moving the control of information closer to its source, the end user. In this transition, however, secure management of that information has been placed at risk. Information technology departments must protect the traditional system environment within the computer room plus develop policies, standards, and guidelines for the security and protection of the company's distributed information base. Further, the information technology staff must communicate these standards to all users to enforce a strong baseline of controls.

In these distributed environments, information technology personnel are often asked to develop systems recovery plans outside the context of an overall business recovery scheme. Recoverability of systems, however, should be viewed as only one part of business recovery. Information systems, in and of themselves, are not the lifeblood of a company; inventory, assets, processes, and people are all essential factors that must be considered in the business continuation design. The success of business continuity planning rests on a company's ability to integrate systems recovery in the greater overall planning effort.

Business Recovery Planning—The Process
Distinctive areas must be addressed in the formulation of a company's disaster recovery plan, and attention to these areas should follow the steps of the scientific method: a statement of the problem, the development of a hypothesis, and the testing of the hypothesis. Like any scientific process, the development of the disaster recovery plan is iterative. The testing phase of this process is essential because it reveals whether the plan is viable. Moreover, it is imperative that the plan and its assumptions be tested on an ongoing, routine basis. The most important distinction that marks disaster recovery planning is what is at stake—the survival of the business.

The phases of a disaster recovery plan process are:

- Awareness and discovery.
- Risk assessment.
- Mitigation.
- Preparation.
- Testing.
· Response and recovery.

Recovery planners should adapt these phases to a company's specific needs and requirements. Some of the phases may be combined, for example, depending on the size of the company and the extent of exposures to risk. It is crucial, however, that each phase be included in the formation of a recovery plan.

**Awareness and Discovery.**

Awareness begins when a recovery planning team can identify both possible threats and plausible threats to business operations. The more pressing issue for an organization in terms of business recovery planning is that of plausible threats. These threats must be evaluated by recovery planners and their planning efforts, in turn, will depend on these criteria:

· The business of the company.
· The area of the country in which the company is located.
· The company's existing security measures.
· The level of adherence to existing policies and procedures.
· Management's commitment to existing policies and procedures.

Awareness also implies educating all employees on existing risk exposures and briefing them on what measures have been taken to minimize those exposures. Each employee's individual role in complying with these measures should be addressed at this early stage.

In terms of systems and information, the awareness phase includes determining what exposures exist that are specific to information systems, what information is vital to the organization, and what information is proprietary and confidential. Answering these questions will help planners determine when an interruption will be catastrophic as opposed to operational. For example, in an educational environment, a system that is down for two or three days may not be considered catastrophic, whereas in a process control environment (e.g., chemicals or electronics), just a few minutes of downtime may be.

Discovery is the process in which planners must determine, based on their awareness of plausible threats, which specific operations would be affected by existing exposures. They must consider what measures are currently in place or could be put in place to minimize or, ideally, remove these exposures.

**Risk Assessment.**

Risk assessment is a decision process that weighs the cost of implementing preventive measures against the risk of loss from not implementing them. There are many qualitative and quantitative approaches to risk analysis. Typically, two major cost factors arise for the systems environment. The first is the loss incurred from a cease in business operations due to system downtime. The second is the replacement cost of equipment.

The potential for significant revenue loss when systems are down for an extended period of time is readily understood in today's business environment, because the majority of businesses rely exclusively on systems for much of their information needs. However, the cost of replacing systems and information in the event of catastrophic loss is often grossly underrated. Major organizations, when queried on insurance coverage for systems, come up with some surprising answers. Typically, organizations have coverage for mainframes and midrange systems and for the software for these environments. The
workstations and the network servers, however, are often deemed as not valuable enough to insure. Coverage for the information itself is usually neglected as well, despite the fact that the major replacement cost for a company in crisis is the recreation of its information data base.

Notably, the personal computer, regardless of how it is configured or networked, is usually perceived as a standalone unit from the risk assessment point of view. Even companies that have retired their mainframes and embraced an extensive client/server architecture, and that fully comprehend the impact of the loss of its use, erroneously consider only the replacement cost of the unit rather than of the distributed system as the basis of risk.

Risk assessment is the control point of the recovery planning process. The amount of exposure a company believes it has, or is willing to accept, determines how much effort the company will expend on this process. Simply put, a company with no plan is fully exposed to catastrophic loss. Companies developing plans must approach risk assumption by identifying their worst-case scenario and then deciding how much they will spend to offset that scenario through mitigation, contingency plans, and training. Risk assessment is the phase required to formulate a company’s management perspective, which in turn supports the goal of developing and maintaining a companywide contingency plan.

Mitigation.

The primary objectives of mitigation are to lessen risk exposures and to minimize possible losses. History provides several lessons in this area. For example, since the underground floods of 1992, companies in Chicago think twice before installing data centers in the basements of buildings. Bracing key computer equipment and office furniture has become popular in California because of potential injuries to personnel and the threat of loss of assets from earthquakes. Forward-thinking companies in the South and southern Atlantic states are installing systems far from the exterior of buildings because of the potential damage from hurricanes.

Although it is a simple exercise to make a backup copy of key data and systems, it is difficult to enforce this activity in a distributed systems environment. As systems have been distributed and the end user empowered, the regimen of daily or periodic backups has been adversely affected. In other words, the end user has been empowered with tools but has not been educated about, or held responsible for, the security measures that are required for those tools. One company, a leader in the optical disk drive market, performs daily backups of its accounting and manufacturing systems to optical disk (using its own product), but never rotates the media and has never considered storing the backup off-site. Any event affecting the hardware (e.g., fire, theft, or earthquake) could therefore destroy the sole backup and the means of business recovery for this premier company. Mitigation efforts must counter such oversights.

Preparation.

The preparation phase of the disaster planning process delineates what specific actions must be taken should a disaster occur. Based on an understanding of plausible threats, planners must determine who will take what action if a disaster occurs. Alternates should be identified for key staff members who may have been injured as a result of the event. A location for temporary operations should be established in case the company’s building is inaccessible after a disaster, and the equipment, supplies, and company records that will be required at this site should be identified. Preparation may include establishing a hot site for systems and telecommunications. Off-hours or emergency telephone numbers should be kept for all vendors and services providers that may need to be contacted. Moreover, the contingency plans must be clearly documented and communicated to all personnel.
Testing.

The testing phase proves the viability of the planning efforts. The recovery planner must determine, during testing, whether there are invalid assumptions and inadequate solutions in the company's plan. It is important to remember that organizations are not static and that an ever-changing business environment requires a reasonable frequency of testing. Recovery planners must repeat this phase of the plan until they are comfortable with the results and sure that the plan will work in a time of crisis.

Response and Recovery.

This final phase of the contingency plan is one that organizations hope never to have to employ. Preparing for actual response and recovery includes identifying individuals and training them to take part in emergency response in terms of assessment of damage, cleanup, restoration, alternate site start-up, emergency operations duties, and any other activities that managing the crisis might demand.

Every phase of the planning process, prior to this phase, is based on normalcy. The planning effort is based on what is perceived to be plausible. Responses are developed to cover plausible crises and are done so under rational conditions. However, dealing with a catastrophic crisis is not a normal part of an employee's work day, and the recovery team must be tested under more realistic conditions to gauge how they will perform under stress and where lapses in response might occur. Ideally, recovery planners should stage tests that involve role playing to give their team members a sense of what they may be exposed to in a time of crisis.

Departmental Planning

Often, consultants are asked to help a company develop its business resumption plan and to focus only on the systems environment to reduce the overall cost of planning efforts. Often, companies take action on planning as the result of an information systems audit and thus focus solely on systems exposure and audit compliance. These companies erroneously view disaster recovery as an expense rather than as an investment in business continuity.

A plan that addresses data integrity and systems survivability is certainly a sound place to begin, but there are many other factors to consider in recovery planning. Depending on the nature of the business, for example, telecommunications availability may be much more important than systems availability. In a manufacturing environment, if the building and equipment are damaged in a disaster, getting the systems up and running may not necessarily be a top priority.

A company's business continuation plan should be a compilation of individual department plans. It is essential that each department identify its processes and prioritize those processes in terms of recovery. Companywide operating and recovery priorities can then be established by the company's management based on the input supplied by the departments. Information technology, as a service department to all other departments, will be better equipped to plan recovery capacity and required system availability based on this detailed knowledge of departmental recovery priorities.

Information Technology's Role

Information technology personnel should not be responsible for creating individual department plans, but they should take a leadership role in the plan development. Information technology generally has the best appreciation and understanding of information flow throughout the organization. Its staff, therefore, are in the best position to identify and assess the following areas.
Interdepartmental Dependencies

It is common for conflicts in priorities to arise between a company's overall recovery plan and its departmental plans. This conflict occurs because departments tend to develop plans on their own without considering other departments. One department may downplay the generation of certain information because that information has little importance to its operations, but the same information might be vitally important to the operations of another department. Information technology departments can usually identify these discrepancies in priorities by carefully reviewing each department’s plan.

External Dependencies

During the discovery process, recovery planners should determine with what outside services end-user departments are linked. End-user departments often think of external services as being outside the scope of their recovery planning efforts, despite the fact that dedicated or unique hardware and software are required to use the outside services. At a minimum, departmental plans must include the emergency contact numbers for these outside services and any company account codes that permit linkage to the service from a recovery location. Recovery planners should also assess the outside service providers’ contingency plans for assisting the company in its recovery efforts.

Internal and External Exposures

Standalone systems acquired by departments for a special purpose are often not linked to a company’s networks. Consequently, they are often overlooked in terms of data security practices.

For example, a mortgage company funded all of its loans via wire transfer from one of three standalone systems. This service was one of the key operations of the company. Each system was equipped with a modem and a uniquely serialized encryption card for access to the wire service. However, these systems were not maintained by the information technology department, no data or system backups were maintained by the end-user department, and each system was tied to a distinct phone line. Any mishap involving these three systems could have potentially put this department several days, if not weeks, in arrears in funding its loans. Under catastrophic conditions, a replacement encryption card and linkage establishment would have taken as much as a month to acquire.

As a result of this discovery, the company identified a secondary site and filed a standby encryption card, an associated alternate phone line, and a disaster recovery action plan with the wire service. This one discovery, and its resolution, more than justified the expense of the entire planning effort.

During the discovery process, the recovery planner identified another external exposure for the same company. This exposure related to power and the requirements of the company’s uninterruptable power supply (UPS). The line of questioning dealt with the sufficiency of battery backup capacity and whether an external generator should be considered in case of a prolonged power interruption. An assumption had been made by the company that, in the event of an areawide disaster, power would be restored within 24 hours. The company had eight hours of battery capacity that would suffice for its main operational shift. Although the county’s power utility company had a policy of restoring power on a priority basis for the large employers of the county, the company was actually based in a special district and acquired its power from the city, not the county. Therefore, it would have power restored only after all the emergency services and city agencies were restored to full power. Moreover, no one could pinpoint how long this restoration period would be. To mitigate this exposure, the company added an external generator to its UPS system.
Apprise Management of Risks and Mitigation Costs.

As an information technology department identifies various risks, it is the department's responsibility to make management aware of them. This responsibility covers all security issues—system survivability issues (i.e., disaster recovery), confidentiality, and system integrity issues.

In today's downsized environments, many information technology departments have to manage increasingly more complex systems with fewer personnel. Because of these organizational challenges, it is more important for the information technology staff involved in the planning process to present management with clear proposals for risk mitigation. Advocating comprehensive planning and security measures, and following through with management to see that they are implemented, will ensure that a depleted information technology staff is not caught off-guard in the event of disaster.

Policies.

To implement a system or data safeguard strategy, planners must first develop a policy, or standard operating procedure, that explains why the safeguard should be established and how it will be implemented. The planners should then get approval for this policy from management.

In the process of putting together a disaster recovery plan for a community college's central computing operations, one recovery planner discovered that numerous departments had isolated themselves from the networks supported by the information technology group. These departments believed that the servers were always crashing, which had been a cause for concern in years past, and they chose to separate themselves from the servers for what they considered to be safer conditions. These departments, which included accounting, processed everything locally on hard drives with no backups whatsoever. Needless to say, a fire or similar disaster in the accounting department would severely disrupt, if not suspend, the college's operations.

The recovery planner addressed this problem with a fundamental method of distributed system security: distribute the responsibility of data integrity along the channels of distributed system capability. A college policy statement on data integrity was developed and issued to this effect. The policy outlined end-user security responsibilities, as well as those of the department administrators.

Establish Recovery Capability.

Based on departmental input and a company's established priorities, the information technology department must design an intermediate system configuration that is adequately sized to permit the company's recovery immediately following the disaster. Initially, this configuration, whether it is local, at an alternate company site, or at a hot site, must sustain the highest-priority applications yet be adaptable to addressing other priorities. These added needs will arise depending on how long it takes to reoccupy the company's facilities and fully restore all operations to normal. For example, planners must decide that the key client/server applications are critical to company operations, whereas office automation tools are not.

Restore Full Operational Access.

The information technology department's plan should also address the move back from an alternate site and the resources that will be required to restore and resume full operations. Depending on the size of the enterprise and the plausible disaster, this could include a huge number of end-user workstations. At the very least, this step is as complex as a company's move to a new location.
Planning For the Distributed Environment

First and foremost, planners in a distributed environment must define the scope of their project. Determining the extent of recovery is the first step. For example, will the plan focus on just the servers or on the entire enterprise's systems and data? The scope of recovery, the departmental and company priorities, and recovery plan funding will delimit the planner's options. The following discussion outlines the basics of recovery planning regardless of budget considerations.

Protecting the LAN

Computer rooms are built to provide both special environmental conditions and security control. Environmental conditions include air conditioning, fire-rated walls, dry sprinkler systems, special fire abatement systems (e.g., Halon, FM-200), raised flooring, cable chase-ways, equipment racking, equipment bracing, power conditioning, and continuous power (UPS) systems. Control includes a variety of factors: access, external security, and internal security. All these aspects of protection are built-in benefits of the computer room. Today, however, company facilities are distributed and open; servers and network equipment can be found on desktops in open areas, on carts with wheels, and in communications closets that are unlocked or have no conditioned power. Just about anything and everything important to the company is on these servers or accessible through them.

Internal Environmental Factors.

A computer room is a viable security option, though there are some subtleties to designing one specifically for a client/server environment. If the equipment is to be rack mounted, racking can be suspended from the ceiling, which yields clearance from the floor and avoids possible water damage. Notably, the cooling aspects of a raised floor design, plus its ability to hide a morass of cabling, are no longer needed in a distributed environment.

Conditioned power requirements have inadvertently modified computer room designs as well. If an existing computer room has a shunt trip by the exit but small standalone battery backup units are placed on servers, planners must review the computer room emergency shutdown procedures. The function of the shunt trip was originally to kill all power in the room so that, if operational personnel had to leave in a hurry, they would be able to come back later and reset systems in a controlled sequence. Now, when there are individual battery backup units that sustain the equipment in the room, the equipment will continue to run after the shunt is thrown. Rewiring the room for all wall circuits to run off the master UPS, in proper sequence with the shunt trip, should resolve this conflict.

Room placement within the greater facility is also a consideration. When designing a room from scratch, planners should identify an area with structural integrity, avoid windows, and eliminate overhead plumbing.

Alternate fire suppression systems are still a viable protection strategy for expensive electronics and the operational, on-site tape backups within a room. If these systems are beyond the company's budget, planners might consider multiple computer rooms (companies with a multiple-building campus environment or multiple locations can readily adapt these as a recovery strategy) with sprinklers and some tarpaulins handy to protect the equipment from incidental water damage (e.g., a broken sprinkler pipe). A data safe may also be a worthwhile investment for the backup media maintained on-site. However, if the company uses a safe, its personnel must be trained to keep it closed. In eight out of ten site visits where a data safe is used, the door is kept ajar (purely as a convenience). The safe only protects the company's media when it is sealed. If the standard practice is to keep it
closed, personnel will not have to remember to shut it as they evacuate the computer room under the stress of an emergency.

If the company occupies several floors within a building and maintains communication equipment (e.g., servers, hubs, or modems) within closets, the closets should be treated as miniature computer rooms. The doors to the closets should be locked, and the closets should be equipped with power conditioning and adequate ventilation.

**Physical Security.**

The other priority addressed by a properly secured computer room is control: control of access to the equipment, cabling, and backup media. Servers out in the open are prime targets for mishaps ranging from innocent tampering to outright theft. A thief who steals a server gets away not only with an expensive piece of equipment but with a wealth of information that may be prove much more valuable and marketable than the equipment itself.

The college satellite campus discussed earlier had no backup of the information contained within its network. The recovery planner explained to the campus administration, which kept its servers out in the open in its administration office area (a temporary trailer), that a simple theft of the $2,000 equipment would challenge its ability to continue operations. All student records, transcripts, course catalogs, instructor directories, and financial aid records were maintained on the servers. With no backup to rely on and its primary source of information evaporated, the campus administration would be faced with literally thousands of hours of effort to reconstruct its information base.

**Property Management.**

Knowing what and where the organization's computer assets (i.e., hardware, software, and information) are at any moment is critical to recovery efforts. The information technology department must be aware of not only the assets within the computer room but of every workstation used throughout the organization, whether it is connected to a network (including portables); what its specific configuration is; what software resides on it; and what job function it supports. This knowledge is achievable if all hardware and software acquisitions and installations are run through the IT department, if the company's policies and procedures support information technology's control (i.e., all departments and all personnel willingly adhere to the policies and procedures), and if the department's property management inventory is properly maintained. Size is also a factor here. If the information technology department manages an organization with a single server and 50 workstations, the task may not be too large; however, if it supports several servers and several hundred workstations, the amount of effort involved is considerable.

**Data Integrity.**

Information, if lost or destroyed, is the one aspect of a company's systems that cannot be replaced simply by ordering another copy or another component. The company may have insurance, hot-site agreements, or quick-replacement arrangements for hardware and global license agreements for software, but its data integrity process is entirely in the hands of its information technology specialists. The information technology specialist and the disaster recovery planner are the individuals who must ensure that the company's information will be recoverable. Based on the initial risk assessment phase, planners can determine just how extensive the data integrity program should be. The program should include appropriate policies and education addressing frequency of backups, storage locations, retention schedules, and the periodic verification that the backups are being done correctly. If the planning process has just begun, data integrity should be the first area on
which planners focus their attention. None of the other strategies they implement will count if no means of recovering vital data exists.

**Network Recovery Strategies**

The information technology specialist's prime objective with respect to systems contingency planning is system survivability. In other words, provisions must be in place, albeit in a limited capacity, that will support the company's system needs for priority processing through the first few hours immediately following a disaster.

**Fault Tolerance Versus Redundancy.**

To a degree, information technology specialists are striving for what is called fault tolerance of the company's critical systems. Fault tolerance means that no single point of failure will stop the system. Fault tolerance is often built in as part of the operational component design of a system. Redundancy, or duplication of key components, is the basis of fault tolerance. When fault tolerance cannot be built in, a quick replacement or repair program should be devised. Moving to an alternate site (i.e., a hot site) is one quick replacement strategy.

**Alternate Sites and System Sizing.**

Once the recovery planner fully understands the company's priorities, the planner can size the amount of system capacity required to support those priorities in the first few hours, days, and weeks following a disaster. When planning for a recovery site or establishing a contract with a hot-site service provider, the information technology specialist must size the immediate recovery capacity. This is extremely important, because most hot-site service providers will not allow a company to modify its requirements once it has declared a disaster.

The good news with respect to distributed systems is that hot-site service providers offer options for recovery. These options often include offering the use of their recovery center, bringing self-contained vans to the company's facility (equipped with the company's own required server configuration), or shipping replacement equipment for anything that has been lost.

**Adequate Backups with Secure Off-Site Storage.**

This process must be based on established company policies that identify vital information and detail how its integrity will be managed. The work flow of the company and the volatility of its information base dictates the frequency of backups. At a minimum, backup should occur daily for servers and weekly or monthly for key files of individual workstations.

Planners must decide when and how often to take backups off-site. Depending on a company's budget, off-site could be the building next door, a bank safety deposit box, the network administrator's house, the branch office across town, or a secure media vault at a storage facility maintained by an off-site media storage company. Once the company meets the objective of separating the backup copy of vital data from its source, it must address the accessibility of the off-site copy.

The security of the company's information is of vital concern. The planner must know where the information is to be kept and about possible exposure risks during transit. Some off-site storage companies intentionally use unmarked, nondescript vehicles to transport a company's backup tapes to and from storage. These companies know that this information is valuable and that its transport and storage place should not be advertised.
Adequate LAN Administration.

Keeping track of everything the company owns—its hardware, software, and information bases—is fundamental to a company’s recovery effort. The best aid in this area is a solid audit application that is run periodically on all workstations. This procedure assists the information technology specialist in maintaining an accurate inventory across the enterprise and provides a tool for monitoring software acquisitions and hardware configuration modifications. The inventory is extremely beneficial for insurance loss purposes. It also provides the technology specialist with accurate records for license compliance and application revision maintenance.

Personnel.

Systems personnel are too often overlooked in systems recovery planning. Are there adequate systems personnel to handle the complexities of response and recovery? What if a key individual is affected by the same catastrophic event that destroys the systems? This event could cause a single point of failure.

An option available to the planner is to propose an emergency outsourcing contract. A qualified systems engineer hired to assist on a key project that never seems to get completed (e.g., the network system documentation) may be a cost-effective security measure. Once that project is completed to satisfaction, the company can consider structuring a contractual arrangement that, for example, retains the engineer for one to three days a month to continue to work on documentation and other special projects, as well as cover for staff vacations and sick days, and guarantees that the engineer will be available on an as-needed basis should the company experience an emergency. The advantage of this concept is that the company maintains effective outsourced personnel who are well-versed in the company’s systems if the company needs to rely on them during an emergency.

Testing

The success of a business recovery plan depends on testing its assumptions and solutions. Testing and training keep the plan up-to-date and maintain the viability of full recovery.

Tests can be conducted in a variety of ways, from reading through the plan and thinking through the outcome to full parallel system testing, or setting up operations at a hot site or alternate location and having the users run operations remotely. The full parallel system test generally verifies that the hot-site equipment and remote linkages work, but it does not necessarily test the feasibility of the user departments’ plans. Full parallel testing is also generally staged within a limited amount of time, which trains staff to get things done correctly under time constraints.

Advantages of the Distributed Environment for Testing

Because of their size and modularity, distributed client/server systems provide a readily available, modifiable, and affordable system setup for testing. They allow for a testing concept called cycle testing.

Cycle testing is similar to cycle counting, a process used in manufacturing whereby inventory is categorized by value and counted several times a year rather than in a one-time physical inventory. With cycle counting, inventory is counted year long, with portions of the inventory being selected to be counted either on a random basis or on a preselected basis. Inventory is further classified into categories so that the more expensive or critical inventory items are counted more frequently and the less expensive items less frequently. The end result is the same as taking a one-time physical inventory in that, by the end of a calendar year, all the inventory has been counted. The cycle counting method has several advantages:
Operations do not have to be completely shut down while the inventory is being taken. Counts are not taken under time pressure, which results in more accurate counts. Errors in inventories are discovered and corrected as part of the continuous process.

The advantages of cycle testing are similar to those of cycle counting. Response and recovery plan tests can be staged with small manageable groups so they are not disruptive to company operations. Tests can be staged by a small team of facilitators and observers on a continual basis. Tests can be staged and debriefings held without time pressure, allowing the participants the time to understand their roles and the planners the time to evaluate team response to the test scenarios and to make necessary corrections to the plan. Any inconsistencies or omissions in a department's plan can be discovered and resolved immediately among the working participants. Just as more critical inventory items can be accounted for on a more frequent basis, so can the crucial components required for business recovery (i.e., systems and telecommunications). With the widespread use of LANs and client/server systems, information systems departments have the opportunity to work with other departments in testing their plans.

Conclusion
Developing a business recovery plan is not a one-time, static task. It is a process that requires the commitment and cooperation of the entire company. To perpetuate the process, business recovery planning must be a company-stipulated policy in addition to being a company-sponsored goal. Organizations must actively maintain and test plans, training their employees to respond in a crisis. The primary objective in developing a business resumption plan is to preserve the survivability of the business. An organization's business resumption plan is an orchestrated collection of departmental responses and recovery plans. The information technology department is typically in the best position to facilitate other departments' plan development and can be particularly helpful in identifying the organization's interdepartmental information dependencies and external dependencies for information access and exchange.

A few protective security measures should be fundamental to the information technology department's plan, no matter what the scope of plausible disasters. From operational mishaps to areawide disasters, recovery planners should ensure that the information technology department's plan addresses:

- An adequate backup methodology with off-site storage.
- Sufficient physical security mechanisms for the servers and key network components.
- Sufficient logical security measures for the organization's information assets.
- Adequate LAN/WAN administration, including up-to-date inventories of equipment and software.

Finally, in support of an organization's goal to have its business resumption planning process in place to facilitate a quick response to a crisis, the plan must be sufficiently and repeatedly tested, and the key team members sufficiently trained. When testing is routine, it becomes the feedback step that keeps the plan current, the response and recovery strategies properly aligned, and the responsible team members ready to respond. Testing is the key to plan viability and thus to the ultimate survival of the business.
Author Biographies

Steven P. Craig
Steven P. Craig is a Managing Partner of Venture Resources Management Systems in Lake Forest, California.