DATA SECURITY MANAGEMENT

BUSINESS CONTINUITY IN THE DISTRIBUTED ENVIRONMENT

Steven P. Craig

INSIDE
Business Recovery Planning: The Process; Departmental Planning; Information Technology's Role; Planning for the Distributed Environment; Testing

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 is placed at risk. Information Technology (IT) departments must protect the traditional system environment within the computer room, plus develop policies, standards, and guidelines for the security and the protection of the company's information base. Further, the IT staff must communicate these standards to all users to enforce a strong baseline of controls.

In these distributed environments, IT personnel are often asked to develop system 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 (IS), in and of itself, is 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.

PAYOFF IDEA
This article describes the process of business recovery planning with an emphasis on the considerations for LANs and the components that comprise the LAN. The considerations given in this article can be applied to companies of any size with a recovery scope from operational to catastrophic events.
BUSINESS RECOVERY PLANNING: THE PROCESS

Distinctive areas must be addressed when formulating a company’s business disaster recovery plan that follow the stages of the scientific process; namely, statement of the problem, development of a hypothesis, and testing of the hypothesis. Most importantly, as with any scientifically developed process, the Disaster Recovery Planning Process development is iterative. The testing phase of this process identifies whether or not the plan will work in practice ... not just in theory. It is imperative that the plan and its assumptions be tested, tested, and retested. The important distinction about disaster recovery planning, and the importance of its viability, is what is at stake — namely, the survivability of the business.

The phases of a viable disaster recovery plan process are:

- awareness and discovery
- risk assessment
- mitigation
- preparation
- testing
- response and recovery

Some of these phases can be combined, depending on the size of the company and the extent of exposure to risk. However, these phases are distinct and discussed more in length in the following sections.

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 is also education. Part of the awareness process consists of instructing all employees on what exposures exist for the company and themselves; what measures have been taken to minimize those exposures; and what their individual roles are in complying with those measures.

Pertaining to systems and information: what exposures are there; what information is vital to the organization; and, what information is proprietary and confidential to the business? Also with respect to sys-
tems, another question that needs to be addressed is, when is an inter-
ruption considered to be catastrophic as opposed to operational? Again,
this needs to be answered on a company-by-company basis. In an edu-
cational environment, the systems being down for two to three days may
not be considered catastrophic; however, in a process control environ-
ment (e.g., chemicals or electronics), a few minutes of downtime might
be catastrophic.

Discovery is determining the extent of the exposure and the extent of
recovery planning and of the security measures that should be taken.
Based on the response to the awareness question as to what is plausible,
there are more questions to be asked. What specific operations would be
impacted by the exposures? What measures are in place or could be put
in place to minimize those exposures? What measures could be taken to
remove the exposure?

Risk Assessment
Risk assessment is a decision process that weighs the cost of implement-
ing preventative measures against the risk of loss from not taking any ac-
tion. There are qualitative and quantitative approaches to risk analysis, of
which there are full text references written on the subject. Typically for
the systems environment, in terms of outright loss, two major cost factors
arise. The first is the loss from not conducting business due to system
downtime. The second is the replacement cost of the equipment. The
unavailability of systems for an extended period of time is the easiest in-
tuitive sell, as it is readily understandable by just about everyone in to-
day’s organizations as to how much they rely on systems.

The cost to replace systems and information, however, is often not
well understood, at least not from a catastrophic loss point of view. In
many instances, major organizations, when queried on insurance cover-
age for systems, come up with some surprising results. There will typi-
cally be coverage for mainframes and mid-range systems, as well as
coverage for the software for these environments, but when it comes to
the workstations or the network servers, they are deemed as not worth
enough to insure. Another gaping hole is the lack of coverage for the in-
formation itself. The major replacement cost for a company is the recre-
ation of its information base.

Further, the personal computer (PC), no matter how it is configured or
what it is hooked up to or how extensive the network, is still perceived
to be a stand-alone unit from a risk assessment point of view. Although
many companies have retired their mainframes and fully embraced an
extensive client/server architecture to fully manage their businesses, and
fully comprehend the impact of the loss of its use, they erroneously look
at the replacement cost of the unit rather than 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 additional effort the company will put forth on this process. Quite simply, companies with no plan are taking on the full risk of exposure, assuming that nothing, at least nothing severe, will ever happen to them. Companies that have developed plans have decided on the extent of risk assumption in two ways: (1) they have identified their worst-case scenario, and (2) they have made decisions based on how much they will expend in offsetting that scenario through mitigation, contingency plans, and training. Risk assessment is the phase required to gel a company’s management perspective, which in turn supports the goal to develop and maintain a companywide contingency plan.

Mitigation
Mitigation has two primary objectives: lessen the exposures and minimize possible loss. History teaches several lessons in this area. One can be sure that companies in Chicago now think twice about installing data centers in the basement of buildings after the underground floods of 1992. Bracing of key computer equipment and of office furniture has become popular in California due to the potential injuries to personnel and the threat of loss of assets from earthquakes. And, forward-thinking companies in the South and southern Atlantic states are installing systems far from the exterior of the buildings and windows because of the potential damage due to hurricanes.

Once again, from a more operational perspective, one can read story after story in the trade journals about backup schemes gone awry, if there was a backup performed at all! Although it is a simple concept, to make a backup copy of key data and systems, it is a difficult one to enforce in a distributed systems environment. To wit, as systems have been distributed and the end user has been empowered, the regimen of daily or periodic backups has diminished. The end user has been empowered with the tools but not given the responsibility that goes along with the use of those tools. This author recently went into a company, one of the leaders in the optical disk drive market, and found that it did perform daily backups to the optical disk (using its own product) of its accounting and manufacturing systems, but never rotated the media and never thought to take it off site! Any event impacting the hardware (e.g., fire, theft, earthquake) would have also destroyed the “only backup” and the means of business recovery for this premier company.

Preparation
This phase of the disaster planning process delineates what must be done in addition to the mitigation taken, should an event occur. Based on the perception of what could happen, who will take what actions?
alternates identified for key staff members that may have been injured as a result of the event? Can the building be occupied? If not, where will temporary operations be set up? What supplies, company records, etc. will be required to operate from a temporary facility? What computer support will be required at the temporary location? Will a hot site be used for systems and telecommunications? What vendors and services providers need to be contacted; and further, is there access to their off-hours phone numbers, emergency numbers, or home phone numbers? These are all questions that need to be addressed, contingencies established, and the plans documented as an integral part of the disaster preparedness process.

Testing
As mentioned above, the testing phase proves the viability of the planning efforts. If there are omissions in the plan, or invalid assumptions, or inadequately postulated solutions … this is when one wants to find these things out. Not at the time of an actual event! Additionally, organizations do not remain static; the elements of change within an organization and its environment dictate a reasonable frequency of testing. This is the phase of the plan that one must afford to reiterate until one is comfortable with the results and that the plans will work in time of crisis. A subsequent section in this article covers testing more in-depth and proposes a testing strategy made available by the use of distributed systems.

Response and Recovery
Most everyone carries auto insurance, home insurance, professional liability insurance and life insurance, yet one hopes never to use it or rely on it. Well, this is the phase of the contingency plan one hopes to never use! This part of the plan details which individuals will take on specific roles as part of predetermined teams, trained to address the tasks of emergency response, assessment of damage, cleanup, restoration, alternate site start-up, emergency operations center duties, and whatever else managing through a 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 envisioned to cover those perceptions, and are done so under rational conditions. Remember that people are an integral part of the response and recovery effort. Dealing with a catastrophic crisis is not a normal part of everyday life or of someone’s work load.

Expect very different reactions from individuals you may think you knew well under severe stress. A simple example, one may have experienced is being trapped in an elevator for several minutes. Within a couple of minutes, an individual’s personalities, anxieties, and fears start to surface. Some will begin to panic; others will start taking control of the
situation. Here again, testing the plan can afford some insight as to how team members will react. Ideally, one will be able to stage some tests that will involve role playing so as to give team members a sense of what they may be exposed to and the conditions they will have to work under.

DEPARTMENTAL PLANNING
Time and time again this author has been asked to help a company develop its business resumption plan, only to be asked to focus just on the systems and ignore everything else; for the most obvious reason — cost. As it turns out, if a company receives an action item as a result of an audit, it is typically a part of an EDP audit and thus only targeted at the systems of a company. In turn, the company focuses only on the audit compliance, thus viewing disaster recovery as an expense, rather than as an investment in business continuity.

Having a plan that addresses data integrity and systems survivability is a good start, but there is a lot more to consider. Depending on the nature of the business, telecommunications availability, as an example, may be much more important than systems availability. In a manufacturing environment, if the building and equipment were damaged, getting the systems up and running would not necessarily be the most important priority.

A company’s Business Continuation Plan is, in fact, a compilation of its departmental plans. It is essential that each department identify its own processes and subsequent priorities of those processes. Overall companywide operating and recovery priorities are then established by the company’s management, based on the input supplied by the departments. Information Technology (IT), as a service department to all other departments, is subsequently in a much better position to plan recovery capacity and required system availability based on their inputs, priorities, and departmental recovery schedules.

Information Technology’s Role
IT should not be responsible for creating the individual departmental plans for the rest of the company, but it can and indeed needs to take a leadership role in the departmental plan development. IT has generally been the department that has the best appreciation and understanding of information flow throughout the organization. IT is therefore in the best position to identify and assess the following areas.

Interdepartmental Dependencies. Many times in reviewing a company’s overall plan and its departmental plans and their subsequent priorities, conflicts in the priorities will arise. This occurs because the departments tend to develop their plans on their own without the other departments in mind. One department may downplay the generation of
certain information, knowing it has little importance to its own operations, but it might be vitally important input to the operation of another department. IT can typically identify these priority discrepancies simply by being able to review each of the other department’s plans.

**External Dependencies.** During the discovery process, recovery planners should determine with what outside services end-user departments are linked. End-user departments often tend to 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, make sure the departmental plans include the emergency contact numbers for the services and any company account codes that would permit linkage to the service from a recovery location. Also inquire as what provisions the outside service provider may have to assist the company in its recovery efforts.

**Outsourced Operations.** A 1990s trend in corporate strategic directions has been the outsourcing of entire department operations. The idea is to focus the company’s resources on what it does best, and outsource the functions that it believes other companies could better handle as part of their expertise and focus. The idea sounds good in theory, but in practice this has been a mixed bag of tricks. The bottom line of this strategic direction was that it would add to the bottom line. Based on what is being published on the subject, the savings may only be a short-term result, and in fact be very costly in the long run. From a contingency planning perspective, what happens if the idea does not work? How does a company rebuild an Information Systems department from scratch?

With respect to recovery planning, this is a key area that requires involvement at the earliest stages possible, including the review of contract wording and stipulations. This is an area in which the contractor has to be an integral partner, with as much ownership and jointly owned risk as the acquiring company. In many disasters, the Information Systems staffs are the first responders for business recovery. Will the contractor be as willing to take on this role? The recovery planner needs to validate that the on-site outsourced contractors are as well trained on response and recovery as the other internal departments. The area of systems is so integral to the recovery capability of the other departments that is it imperative that the outsourced information systems personnel be well versed in the recovery needs and response priorities of all of the departments they are there to support.

Collectively, the outsourcer may have considerably more resources available to it than the customer; however, it must be agreed to contractually that the contractor will bring its resources to bear in the event of the customer’s catastrophe. Normally, these outsourced arrangements start off with the greatest of intentions, but once things get under way
and the conditions of systems, documentation, and operations are established, anything outside the scope of the contract is doable, but with incremental cost. Costs were what was intended to be cut when the outsourcing direction was decided on; raising these costs will be a tough sell. So, the recovery planner must be involved early in the development of any such outsourcing contract and be sure to protect the company’s contingency planning interests.

Internal and External Exposures

Stand-alone 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 stand-alone 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. As one might guess, these systems were not maintained by Information Technology; there were no data or system backups maintained by the end-user department; and, each system was tied to a distinct phone line. Any mishap involving those three systems could have potentially put this department several days, if not weeks, in arrears in funding its loans. A replacement encryption card and linkage establishment would have taken as long as a month under catastrophic conditions to reestablish.

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

Another external exposure was identified for the same company during the discovery process, dealing with power and the requirements of its UPS capabilities. The line of questioning was on the sufficiency of battery back-up capacity and whether an external generator should be considered as well for longer term power interruption. An assumption had been made that, even in the event of an area-wide disaster, power would probably be restored within 24 hours. The company had eight hours of battery capacity, which would suffice for the main operational shift of the company. At first, this author was in agreement with them, knowing that the county’s power utility company had a program of restoring power on a priority basis for the larger employers of the county. When this observation was mentioned to them, the author was corrected. They were in a special district and actually acquired their power from the city and, as a business, would have power restored only after all the emergency services and city agencies were restored. The restoration period was unknown. The assumption of power restoration within
24 hours was revised and an external generator was added to the uninterruptable power supply system.

Systems themselves should not be the only type of exposure one looks for: In a recent client discovery walkthrough, a protracted construction project was under way. The existing computer room (on the eighth floor of a 20-story highrise) was being remodeled to house the company's latest generation of computers and telecommunications equipment. The room had originally been designed with stand-alone air conditioners, a UPS system, secured entry, and a raised floor. Sprinklers had been eliminated from the room to avoid potential water damage and a Halon fire suppression system had been installed.

As a result of the construction, the computer equipment was temporarily moved to the adjoining computer technician's room. As one might guess, the technician's room had none of the protections that had been developed for the computer room. However, while there were short-term exposures (for length of the construction period), this was a known calculated risk. The actual exposure discovered was the computer room itself. During construction, the Halon fire suppression system and alarms had been turned off, as well as the stand-alone air conditioning systems within. In addition, a considerable amount of packing material had accumulated within the room, so much so that it was stacked from floor to ceiling. The room was hot, from the lack of air conditioning. This was a fire waiting to happen. A fire needs fuel, oxygen, and heat — all three readily existed in the room. If a fire were to start, there were no active fire suppression capabilities within the room and, with the alarms being turned off, it would have been well under way before the other building detection systems would have been alerted. A fire located here would have easily knocked out the central computing capability and telecommunications for the entire corporation, as well as potentially destroying several floors of this corporate tower. Transition periods can be the times of greatest vulnerability for any company, as existing detection and protection systems are temporarily shut down. The recovery planner needs to know that the planning process is reiterative; if the assumptions of the plan change, a review of all of the process steps is in order.

Apprise Management of the Risk

It is entirely management's decision on how much risk it is willing to take or deem what risks are unacceptable. However, as IT identifies the various risks, it is their responsibility to make management aware of those risks. This holds true across the board on all security issues, be they system survivability issues (disaster recovery) or confidentiality or system integrity issues.

A company having its key system client files breached from the outside, or a sales representative's laptop stolen with those key client files
contained within, can be potentially more devastating to a company’s operations than a prolonged power outage.

Apprise Management of Mitigation Cost

There seems to be a tremendous amount of frustration in IT departments these days, as departments have been right-sized and yet have to manage more complex systems than ever before. Many of the things that one will uncover will have such an obvious risk that obtaining approval for any mitigation campaigns should be relatively easy to obtain. Other system-related topics are more intangible or in some cases deemed as being a “nuisance,” and are admittedly a tougher sell.

To cope with today’s organizational demands and yet still feel good about the job it is performing, IT personnel responsible for this planning effort must adapt to the changing times, anticipate the risks, and present to management the mitigation options and their associated costs — knowing that management will make a decision with the company’s best interest in mind.

POLICIES

The best approach to begin an implementation of a system or data safeguard strategy is to first define and get approval from management on the policy or standard operating procedure that requires the safeguard be established. In assisting a community college in putting together a disaster recovery plan for its central computing operations, it was discovered that numerous departments had isolated themselves from the networks supported by the IT group. The reason for this departure was the belief that the servers were always crashing, which was a cause for concern some three years ago, but is no longer true. Yet, to date, these departments (including Accounting) were processing everything locally on their hard drives with no backups whatsoever. This practice, now three years old, needed to be dispelled, as a disaster such as a fire in the Accounting department would severely disrupt, if not cause a cessation of, the college’s operations altogether. One of the other satellite campuses of the district went entirely its own route, setting up its own network with no ties to the central computing facility — with absolutely no backups at all.

The plan basically went back to the fundamentals: distribute the responsibility for data integrity along with the distributed system capability. A college policy statement on data integrity was made to the effect that:

- The recoverability and correctness of digitized data, which resides on college-owned computer systems and media, is the responsibility of the individual user. The ultimate responsibility of ensuring the data integrity for each departmental workstation rests with the department/division administrator.
• Information Technology will provide the guidelines for data back-ups. Adherence to these guidelines by the users of the college-owned workstations is mandatory.

Establish Recovery Capability
Based on the inputs from the departments of the company and the company’s overall priorities, IT is challenged with designing an intermediate system configuration that is adequately sized to permit the company’s recovery, immediately following the event. This configuration — whether it be local, at an alternate company site, or a hot site — needs to initially sustain the highest priority applications, yet be adaptable to expand to address other priorities, depending on how long it may take to reoccupy the company’s facilities and fully restore all operations back to normal. One needs to consider, for example, that the key client/server applications may be critical to company operations, whereas office automation tools may not.

Restore Full Operational Access
Information Technology’s plan also needs to address the move back from an alternate site and what resources will be required to restore and resume full operations. Depending on the size of the enterprise and the disaster being planned for, this could include hundreds to thousands of end-user workstations. At a minimum, this step will be as complex as moving the company to a new location.

Planning for the Distributed Environment
First and foremost, what are the marching orders? What is the extent the plan is to cover? Is it just the servers? Is it just the computers directly maintained by the IT department? Or is it the entire enterprise’s systems and data your responsibility? Determining the extent of recovery is the first step; that is, defining the scope of the project. The project scope, the overall company priorities, and the project funding will bracket the options one has in moving forward. But what follows in the next sections are some of the basics no matter what the budget. As one reads through them, one will find that many of these ideas are founded in sound operational management — as they should be.

Protecting the LAN. There are two primary reasons why computer rooms are built: (1) to provide special environmental conditions, and (2) for control. Environmental conditions include air conditioning, fire-rated walls, dry sprinkler systems, special fire abatement systems (Halon, FM-200), raised flooring, cable chaseways, equipment racking, equipment bracing, power conditioning, and continuous power (UPS systems), etc.
Control includes a variety of factors, namely access, external security, and internal security. All these aspects of protection (mitigation steps taken to offset the risk of fire, theft, malicious tampering, etc.) are built-in benefits of the computer room. Yet if one walks around company facilities today, one is likely to find servers and all sorts of network equipment on desktops in open areas, on carts with wheels, in communication closets that are unlocked or with no conditioned power — yes, they are truly distributed and open. What is on those servers or accessible through those servers ... just about anything and everything important to the company.

Internal Environmental Factors. A computer room is a viable security option, although there are some subtleties to designing one specifically for a client/server environment. If the equipment is to be all rack mounted, racking can be suspended from the ceiling, which still yields clearance from the floor; thus avoiding 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 stand-alone battery backup units are placed on servers, planners must review computer room emergency shutdown procedures. The idea of the shunt trip was 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. However, when there are individual battery backup units that sustain equipment in the room, the equipment connected to them will continue to run, even after the shunt is thrown, until the batteries run out.

Rewiring the room for all wall circuits to run off the master UPS, in proper sequence with the shunt trip, is one way to resolve this conflict. However, if the computer room houses mainframe, mid-range, and client/server equipment, a different strategy might be required. Many of the client/server systems are designed to begin an orderly shutdown once the cut-over to battery power has been detected. This is not the case with all mid-range and mainframe systems.

There are instances when it would be better to allow an orderly shutdown to occur, a short-term power outage for example. While other times, an instant shut-off of all power would be required, as in the case of a fire or an earthquake.

The dilemma rests with the different requirements of the system platforms; the solution lies in the wiring of the room. One option is to physically separate the equipment into different rooms and wire each room according to the requirements of the equipment it contains. Another solution is a two-stage shunt approach: a red shunt would immediately
shut off all power, as was always intended; a yellow shunt would cut all power except from the UPS, allowing the servers to initiate an orderly shutdown on their own.

Room placement within the facility is also a consideration, as pointed out earlier. If designing a room from scratch, identify an area with structural integrity, avoid windows, and eliminate overhead plumbing.

Alternate fire suppression systems are still a good protection strategy for all the expensive electronics and the operational, on-site tape backups within a room. If these types of systems are beyond the budget, consider multiple computer rooms (companies with a multiple-building campus environment or multiple locations can readily adapt this as a recovery strategy). Equip the rooms with sprinklers, and keep some tarps handy to throw over the equipment to protect it from incidental water damage (a broken sprinkler pipe, for example). A data safe may also be a worthwhile investment for the backup media maintained on site. However, if one goes through the expense of using a safe, train personnel to keep it closed. In eight out of ten site visits where a data safe is used, this author finds the door ajar (purely as a convenience). The safe only provides the protection to the media when it is sealed. If the standard practice is to keep it closed, then personnel will not have to second-guess, under the influence of adrenaline, whether or not they shut it as they evacuated the computer room.

If a company occupies several floors within a building and maintains communication equipment (servers, hubs, modems, etc.) within the closets, then treat them as a miniature computer room as well. Keep the doors to the closets locked and equip the closet with power conditioning and adequate ventilation.

**Physical Security.** The other aspect of a secured computer room is control: control (both internal and external to the company) of access to the equipment, cabling, and backup media. Servers out in the open are prime targets for a range of mishaps — from innocent tampering to outright theft. A thief, in stealing a server, not only gets away with an expensive piece of equipment, but a potentially large amount of information, which, if the thief realizes it, may be several times more valuable and marketable than the equipment.

With regard to the previously mentioned college satellite campus that had no backups of the information contained within its network, this author explained to the campus administration, which by the way kept their servers out in the open of their administration office area that was in a temporary trailer, that a simple theft (equipment with a street value of $2000) would challenge their viability of continuing to operate as a college. All their student records, transcripts, course catalogs, instructor directories, financial aid records, and more were maintained on their
servers. With no backups to rely on and their primary source of information evaporated, they would be faced with literally thousands of hours to reconstruct their information bases.

**Property Management.** Knowing what and where the organization’s computer assets (hardware, software, and information) are, at any moment in time, is critical to recovery efforts. This may sound blatantly obvious; but remember, one is no longer talking about the assets just within the computer room. Information Technology needs to be aware of every workstation used throughout the organization; whether it is connected to a network or not (this includes portables); what its specific configuration is; what software resides on it; and what job function it supports. This is readily doable if all hardware/software acquisitions and installations are run through the IT department, the company’s policies and procedures support that control (meaning that all departments and all personnel willingly adhere to the policies and procedures), and property management inventory is properly maintained. Size is a factor here. If one manages an organization with a single server and 50 workstations, this may not be too large a task; however, if one supports several servers and several hundred workstations, then one can appreciate the amount of effort this can entail.

**Data Integrity.** Information is the one aspect of a company’s systems that cannot be replaced, if lost or destroyed, simply by ordering another copy or another component. One may have insurance, hot-site agreements, or quick replacement arrangements for hardware and global license agreements for software, but the data integrity process is entirely up to the Information Technology Specialist and the Disaster Recovery Planner; they are the individuals that need to ensure that the company’s information will be recoverable when needed. It all goes back to the risk of loss as to how extensive a data integrity program one needs to devise — from policies, to frequency of backups, to storage locations, to retention schedules, to the periodic verification that the backups are being done correctly. If just starting the planning process, mitigation efforts should focus on this area first. None of the other strategies to be implemented will count if there is no possible recovery of the data.

**Network Recovery Strategies.** As Information Technology, one’s prime objective with respect to systems contingency planning is system survivability. This means that one has provisions in place, albeit limited capacity, to continue to support the company’s system needs for priority processing through the first few hours immediately following the disaster.

**Fault Tolerance vs. Redundancy.** To a degree, what one strives for is fault tolerance of the company’s critical systems. Fault tolerance means
that no single point of failure will stop the system. This is many times built in as part of the operational component design of the system. Examples include mirroring of disks, use of RAID systems, shadowed servers, and UPSs to multiple T1s for wide-area communications. Redundancy, duplication of key components, is the basis of fault tolerance. Where fault tolerance cannot be built in, a quick replacement or repair program needs to be devised. Moving to an alternate site, either one of the company’s, or a facility that is under contract for emergency support (i.e., a hot site), is a quick replacement strategy.

**Alternate Sites and System Sizing.** Once the priorities of a company are fully understood, sizing the amount of system capacity required to support those priorities, in the first few hours, through the first few days and weeks after a disaster can be accomplished. If planning one’s own recovery site using another company location, or establishing a contract with a hot-site service provider, one will want to adequately size the immediate recovery capacity. This is extremely important, as most hot-site service providers will not allow requirement modification your requirements once a disaster is declared.

The good news with respect to distributed systems is that the hot-site service providers offer options for recovery — from using their recovery center; to bringing self-contained vans to your facility, equipped with your required server configuration; to shipping replacement equipment for what was lost, assuming facility is still operable.

**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 workflow of the company and the volatility of its information base will dictate the frequency of backups. At a minimum, backup should occur daily for servers, and weekly or monthly for key files of individual workstations.

Workstation-based information continues to be one of the greatest vulnerabilities for most companies. There is so much vital information stored locally on these workstations with little or no backup. If individuals have taken the precaution of creating backups, they are typically stored right next to the workstations, leaving the company exposed to any type of catastrophic disaster. The recovery planner must insist that the company proactively address this issue through policy and through providing the means for effective workstation backups.

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 a company that is in the business of off-site media storage. Once the company meets the objective of separating the backup
Adequate LAN Administration. Keeping track of everything the company owns — with respect to 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 periodically run on all workstations. This assists in maintaining an accurate inventory across the enterprise, as well as providing a tool for monitoring software acquisitions and hardware configuration modifications. The inventory can be extremely beneficial for insurance loss purposes. It also provides accurate records for license compliance and application revision maintenance.

Personnel. The all-too-often-overlooked area of systems recovery planning is the system’s personnel. Will there be adequate system personnel resources to handle the complexities of response and recovery. What if a key individual is impacted 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 an emergency staffing contract. A qualified systems engineer hired to assist on a key project that one never seems to get completed (e.g., the network system documentation) may be a cost-effective security measure. Once that project is com-

A 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 also of vital concern. Security has several facets: if at a branch office, where do they safeguard the copy; if at the network administrator’s house, where is it kept; and what about the exposure to the media during transit? There are off-site storage companies that intentionally used unmarked, nondescript vehicles to transport a company’s backup tapes to and from storage. This makes a lot of sense because information is valuable and in an attempt to secure it, one does not want to be advertising who one is using and where one is storing the complete system backups.

Several products have come to market (1998) that will assist the LAN administrator with these backup issues. Several of the products offer highly compressed, encrypted backups of workstations and other servers. The compression techniques require very little in the way of bandwidth, and thus even work very effectively in remote backups of laptops using the Internet. The concept of vaulting, running mirrored data centers in separate locations, has been implemented by larger corporations that traditionally had the means to invest in the communications capabilities and the system redundancy. This type of capability is now made possible through these new tools. It is possible today to either work with off-site storage vendors to remotely back up at their facility or, if the company has multiple locations, to readily implement vaulting at the client/server level. Either way, recovery options are facilitated via dial-up access to key recovery systems and data.
pleted 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. The contract could also stipulate coverage for staff vacations and sick days, and should guarantee that the engineer will be available on an as-needed basis should the company experience an emergency. The advantage of this concept is the maintenance of a well-trained and well-versed resource of the company’s systems, should one need to rely on them during an emergency; one has coverage for the company during employee personal leaves, and one has systems documented.

TESTING
The timeless adage with regard to business success being “location, location, location” is adapted here. The pro forma success of a business recovery plan will be most influenced by the extent of the “testing, testing, testing” of its plan. Testing and training are the reiterative and necessary components of the planning process that keep the plan up-to-date and maintain the viability of recovery.

Tests can be conducted in a variety of ways: from desk checking, reading through the plan and thinking through the outcome, to full parallel system testing, setting up operations at a hot site or alternate location, and having the users run operations remotely. The full parallel system test does generally prove that the hot-site equipment and remote linkages work, but does not necessarily test the feasibility of the user department’s plans, as it is a system test. Full parallel testing is also generally staged with a limited amount of time, which adds the pressure of “getting it done” and “passing” because of the time restriction.

Advantages of the Distributed Environment for Testing
Distributed client/server systems — because of their size and modularity — permit a readily available, modifiable, and affordable system setup for testing. They allow for a testing concept that can be coined “cycle testing.”

For those readers with a manufacturing background, this draws a direct parallel to cycle counting: a process whereby inventory is categorized by value and counted several times a year rather than a one-time physical inventory. With cycle counting, inventory is counted all 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, such 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: by the end of a calendar year, all the inventory has been counted. However, the cycle counting method has several advantages: (1) operations do not have to be completely shut down, while the inventory is be-
ing taken; (2) counts are not done under the pressure of “getting it done,” which can result in more accurate counts; and (3) errors in inventories are discovered and corrected as a part of the continuous process.

The parallels to cycle testing are straightforward. Response and recovery plan tests can be staged with small manageable groups so as not to be 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 the pressure of “getting it done” — allowing the participants the time to fully understand their role and critically evaluate their ability to respond to the test scenarios and make necessary corrections to the plan. Any inconsistencies or omissions in a department’s plan can be discovered and resolved directly amongst the working participants.

Just as the 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 throughout companies today, the Information Systems department is afforded more opportunity to work with the other departments in testing their plans and … getting it right.

SUMMARY
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. In order to perpetuate the process, Business Recovery Planning must be a company-stipulated policy as well as a company-sponsored goal. The organizations that adopt this company culture-oriented posture are the ones whose plans are actively maintained and tested, and whose employees are well trained and poised to proactively respond to a crisis. The primary objective of developing a Business Resumption Plan is the survivability of the business.

An organization’s Business Resumption Plan is, in fact, an orchestrated collection of its Departmental Response and Recovery Plans. Information Technology’s plan is also a departmental plan; however, in addressing the overall coordination of the departmental plans, IT is typically in the best position to facilitate the other departments’ development of their plans. With respect to the continuing trend of distributed processing permeating throughout organizations, IT can be of particular help in identifying the organization’s interdepartmental information dependencies and external dependencies for information access and exchange.

There are some basic protective security measures that should be fundamental to the IT plan, no matter what the scope of disasters being planned for. From operational mishaps, to industrial espionage, to area-wide disasters, the Information Technology plan must addresses the following:
• 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

Last, in support of an organization’s goal to have its Business Resumption Planning process in place to facilitate its quick response to a crisis, the plan must be sufficiently and reiteratively tested and the key team members sufficiently trained. When testing is routinely built into the planning process, it becomes the feedback step that keeps the plan current, the response and recovery strategies properly aligned, and the responsible team members postured to respond. Once a plan is established, testing is the key process step that keeps the plan viable. Plan viability equates to business survivability.

Steven P. Craig is Managing Partner for Venture Resources Management Systems in Lake Forest, CA.