BACKGROUND
September 11, 2001, will be indelibly stamped upon all our memories. It taxed our emotional foundation and tested the very mettle upon which our country was built. It also provided a most compelling reason for having a viable and executable business continuity planning (BCP) process. No longer will most corporate executives question the need for recovery planning. In fact, the very opposite is unfolding in corporations around the world. Boards of directors are now asking for an assessment of their recovery capabilities and want to understand their exposure.

With this new emphasis on business continuity planning and disaster recovery (traditionally the information technology or IT portion of business continuity planning), there is a sense of urgency to “take immediate steps” to be prepared for the next crisis. What we learned from September 11 should serve as a guideline for addressing these requirements. What worked and what did not work are lessons that should be examined and applied to our planning process.

THERE IS NO SUBSTITUTE FOR BEING PREPARED
The first lesson we learned is that those who prepared and prepared

PAYOFF IDEA
Companies’ ability to respond to the events of September 11, 2001, and its aftermath varied greatly. This occurred not only from a technology perspective, but also from an organizational and business perspective. While we focused on the human tragedy, there were recovery success stories as well as failures. The lessons learned should provide valuable insight into how we can all be better prepared.
extensively fared far, far, far better than those who did not. This should come as no surprise, yet for some it came as a shock. Despite the 1993 World Trade Center bombing, there has been a feeling among those who control funding for business continuity planning that bright, dynamic, and dedicated people will intuitively make the right decisions in the event of a crisis. In fact, the events of 1993 emboldened such thinking. There were a number of companies that had vague, untested, and even no plans at all. They congratulated themselves on their ingenuity and the fact that they responded well to the crisis. Actually, the circumstances of that event dictated their success for some very distinct reasons:

- It took place on a Friday. This gave them the entire weekend to gather people and resources; form strategies; and seek aid from vendors, business associates, and other sources of help.
- They were able to reenter the building during the weekend to remove documents, servers, equipment, and other resources vital to recovery.
- The loss of lives did not impact the ability to recover.
- Mobility was not severely impaired. Transportation was readily available, equipment and supplies were accessible, and personnel could easily get to sites designated for recovery.
- The resources of internal and commercially provided recovery sites were not overly taxed. There were fewer than 15 disasters declared, and the average stay at a recovery sight was less than two weeks.

The September 11 disaster was in stark contrast to that of 1993. The disruption was of a proportion not seen in this area. Resources were scarce, commercial recovery centers handled more than 100 disaster declarations, mobility was curtailed, and there was a severe emotional reaction that took precedence over recovery operations.

**ORGANIZATIONAL CONSIDERATIONS**

Good BCP starts with having a strong emergency organization with detailed roles and responsibilities. For those that had such an organization, in response to September 11, it helped delegate responsibility and eliminated ad hoc decisions made by less-prepared companies. There was little duplication of effort as each part of the organization understood and performed its function efficiently, despite the turmoil surrounding the events. The basic organization consists of:

- Steering committee
- Damage assessment/emergency response
- Business continuity leader
- Corporate support team
The steering committee is made up of senior officials from operations, technology, risk management, finance, legal, and administration. It is this committee's responsibility to authorize disaster declarations, allocate resources, and communicate to recovery teams (including corporate support, business, and technology). In addition, this committee is responsible for determining and communicating responses to internal and outside organizations.

Regarding September 11, the steering committee was the focal point for information gathered by damage assessment and emergency response personnel who were tasked with providing information concerning the extent of damage to the facility, the equipment located at the facility, and its occupants.

Once the recovery operations were approved, the tactical responsibility for implementation of recovery plans was delegated to the business continuity leader who oversaw three distinct sets of operations:

- **Business recovery**: responsible for restoring operations to business organizations in a predetermined order
- **Technical recovery**: responsible for IT and communications (voice and data) recovery
- **Corporate support**: responsible for supporting the recovery operations of the business and technology and consisting of such functions as:
  - Crisis management desk
  - Finance
  - Human resources
  - Insurance
  - IT
  - Legal
  - Logistics
  - Facilities and maintenance
  - Public relations
  - Real estate
  - Vital records

With these operations in place, the business and technology recovery personnel were free to address their own recovery requirements.

**CRISIS MANAGEMENT**

Preparation for handling emergency situations starts with a strong crisis management structure. This consists of incident management, emergency response, disaster declaration procedures, and recovery and
post-recovery activities. It is important that crisis management be a part of every-day activities, and not materialize only in the face of a disaster. If the crisis management structure only exists as part of an exception processing mentality, it will become outdated, stale, and difficult to invoke at the time of an emergency. Rather, organizations should make it part of everyday problems whereby, for example, IT problems would be reported to a help desk for assessment and possible escalation. Similarly, facility incidents (including fire alarms, smoke, water leaks, etc.) would be reported to a central control monitoring point (usually the security monitoring arm of the building). This would then be evaluated and if escalation were required (such as evacuation, closing of the facility, intervention by municipal authorities, etc.), it would trigger the emergency response portion of the crisis management model. It is important to remember that an incident started the process, and very, very few incidents turn out to require emergency response activities. However, crisis management proved to be critical to many companies on September 11.

At that time, the thoroughness and depth of planning of a number of companies not only helped them reduce the impact to their business, but also proved essential in reducing the human toll. It was the evacuation and assembly portion of the crisis management plan that proved to be a major contributor to safety.

For most buildings that test evacuation (fire drills being the most common test), the exercise ends when people have left the building. This usually means that occupants of the building are left standing in front of it. This is certainly not the optimal place to be, even if the actual incident was a small fire. Personnel standing in front of a building are subject to glass that may break and fall, actual flaming materials, and other debris that might be propelled from the building.

On September 11, good crisis management planning called for personnel to go to an assembly or staging area location. It was located about one-quarter mile from the incident site. The distance was based on lessons learned from the London terrorist and Oklahoma City bombings, as well as from high-rise fires and other large-scale disasters. Best practices firms actually had two assembly points: a primary one and a secondary one. This option allowed flexibility in determining where to go after evacuation. For example, one assembly point could have been a quarter-mile north of the impacted site, while the other one could have been one quarter-mile south of it. It was this type of planning that saved lives.

We were all mesmerized and horrified at the sight of the towers collapsing and people running in all directions to escape the miasma of smoke, dust, and debris. We also heard stories of the tragic cases where people got out of the Trade Center but did not know where to go, and thus were killed by the falling skyscrapers. The simple expedient of having safe distant staging areas would have saved them.
Staging areas were designed for distinct purposes: to ensure that personnel are out of harm’s way, to be able to determine if anyone is left behind, to get first-hand information as to the nature of the damage, and to determine which personnel will partake in the first stage of recovery activities. The last item is the one that allowed many companies to quickly implement recovery procedures. Without a predetermined safe distance staging area, personnel tended to scatter. This made it particularly difficult to assemble recovery teams and to transport them to the recovery sites. On September 11, this proved to be particularly true. The magnitude of the catastrophe created an enormous amount of chaos. This in itself made the act of finding and identifying recovery personnel extremely difficult. The problem was compounded by the lack of telephone service, which hampered the ability to contact staff. The old reliable telephone tree proved to be totally ineffective. With no or limited phone service and no prearranged assembly points, it became almost impossible to gather staff to man recovery sites. Some firms were not able to contact their staff for a number of days following September 11, and this detracted from their ability to perform recovery activities. By contrast, those who did define staging areas were able to proceed with their recovery activities much sooner.

The location of recovery sites proved to be a telling consideration in determining response times to implement recovery procedures. There was a misconception that having a recovery site a great distance from the one impacted by the disaster was an effective strategy. Those who followed this strategy found that accessing their site was extremely difficult, because transportation restrictions slowed or halted efforts to gather staff and transport them to the recovery site. Many firms in lower Manhattan have arrangements with transportation companies (including buses, vans, car services, etc.) to pick up personnel and take them to the recovery site. This is particularly true for recovery sites not served by mass transportation. In New York City, the vast majority of employees rely on railroads, subways, buses, ferries, van services, and other public means of conveyance to get them to work. They do not use their personal vehicles as their primary means of getting to work. With the emergency travel restrictions imposed upon entry into the city after the disaster, companies that had planned on using private bus and car services to transport personnel to a distant recovery site had to improvise. Some companies were able to get people out of Manhattan by having them walk over the Brooklyn Bridge, and then arranging for their transportation to the recovery site. Others abandoned their plans and simply relocated personnel to areas within the city.

Many of those companies that had no assembly area found that personnel just wandered into offices that were not affected. Some walked three and four miles to get there. This added to the chaos and further delayed recovery efforts. One firm had a completely equipped and ready
recovery site that they built and maintained at a cost of several million dollars. The site remained unoccupied because personnel could not get to the rural location. On the other hand, recovery sites that were located near mass transportation were more quickly occupied, and companies using this strategy were able to start recovery activities sooner.

TECHNICAL RECOVERIES

While many companies scrambled to provide recovery facilities for personnel, the technology community was far better prepared. Over the past ten years, IT organizations have made great strides in their preparedness process. This applies to mainframes, servers, networks, and even telephone recovery planning.

One of the major problems that became immediately evident was the inability of displaced companies to reroute their phones to offices and recovery sites that were not affected by the events of September 11. Almost two months after the event there were still phone numbers that went unanswered and callers receiving a message that the number was out of service.

Planning for telephone rerouting is one of the first measures that should be taken as part of any technical recovery. Services provided by local and long-distance carriers make the process relatively painless and inexpensive. It is always surprising to see how much effort is spent on rerouting data lines, and how little is spent on the lifeblood of any organization — keeping in contact with clients.

The process is very similar for most service providers. The customer defines one or more schemas (the destination for each individual phone line or trunk). For example, many firms reroute their phone lines nightly from their primary office to a service bureau or fulfillment agent that will interface with customers during off-hours. This means that after-hours, when a person dials the same telephone number that is answered by normal office staff during business hours, the call is routed to the service bureau (or in some cases another office in a different time zone) and is answered there. This is transparent to the caller and provides for seamless customer service.

Another use of this service is for recovery. Planners define a schema that will allow them to reroute calls (via a call to the service provider or through a secure PC connection) to their recovery site. The calls can be routed to a private branch exchange (PBX), where the call is matched to a location and phone set at the location. This requires extensive table maintenance and capacity in the PBX to manage this extra set of phone lines. A simpler alternative is to have the calls routed to a set of operators who will switch the calls to the person’s new location. In either case, the call is rerouted away from the affected area. For recovery purposes, this process should take place at the phone company (commonly
referred to as the central office or CO), as opposed to a company’s locally located PBX. The reason is simple: if the disaster is of such a magnitude that it destroys or renders the PBX inoperable, then the access required to invoke the alternate schema will be unavailable and the strategy will be rendered ineffective.

With the enormous pressure placed upon New York City’s phone service providers (which themselves suffered severe damage, reducing capacity by an estimated one million-plus phone lines), it was understandable that they were not able to help companies that had not prepared by having preprogrammed call rerouting.

Another shortcoming of many technology recovery plans was the reliance upon ad hoc purchases of equipment, including such items as desktop PCs, printers, cabling, hubs, routers, and the like. Having a local computer or office supply store on every other block provided an ineffective security blanket. A run on equipment took place, and it took several days for technology to become available. This shortage was not an attempt by suppliers to increase profits; in truth, suppliers made Herculean efforts to meet customer demand. It was simply a matter of supply and demand. Those that actually had agreements with vendors fared far better. If the recovery site was located outside the New York City area, deliveries were made within contractual limits. Recovery sites within the city suffered delivery delays because of travel restrictions. But here again, preparedness paid off.

The major technology problem was the recovery of data. Firms that used less frequent, inconsistent, and sometimes indeterminate data backup programs had major control problems. This not only impacted the ability of the company to obtain accurate financial and production information, but led to a state of confusion that added to the problem.

The three major means of performing data backups are:

- **Mirroring**: having data written to two separate devices located some distance apart at the same time
- **Replication**: periodically transmitting data (based on a preset time or amount of data) from its primary device to another device located some distance away
- **Daily backups**: data is backed up to tape, removable disk, or CD at the end of the day, either done locally and removed to an off-site location, or transmitted to a remote site

In the case of September 11, the backup frequency resulted in lost data that ranged from inconvenient (loss of data for a short period of time) to major reconciliation efforts (data lost for a day or more). As an example, take the case of a firm that backs up its data nightly and moves it off-site. If it becomes necessary to relocate IT operations to another site, it will use the backups to restore the data portion of the operation.
Say it backed up the data on Monday night and moved it off-site, assuming that the incident causing relocation took place on Tuesday, before the Tuesday backups were taken off-site. Then, when systems were restored on Wednesday, the data would not reflect any of the activities performed on Tuesday. This in itself would not present that great a problem, except that certain activities have repercussions beyond the processing within a system.

Consider an organization in the September 11 example, on Tuesday, before the disaster took place. An internal scheduler that issued checks for accounts payable that day initiated a program to start this process. The checks were printed in the mailroom and mailed to vendors. The system was updated to reflect that these accounts were paid. However, when the system was restored, it showed that these accounts were not paid. The scheduler recognized this and issued new checks. These checks were then sent to the mailroom (again) and mailed to vendors. The result was a double payment.

Conversely, on the accounts receivable side, data on restored systems did not reflect payments that were made on the day of the incident. This resulted in sending customers notices for non-payment of accounts and adding late fees. This not only showed a lack of control and accuracy of accounting records, but also increased the number of calls from irate customers to an already overburdened customer service staff.

What was most disconcerting about these series of events is that many companies did not realize that they were occurring. They never considered the implications of restoring systems with non-current data. This led in turn to confusion, control problems, and an inability to respond quickly and accurately to customer issues.

Happily, this was not true for all companies. There were some that not only knew that they would lose data, but had, as part of their business continuity plan, a process in place to collect and restore this data. Once their IT was restored, they immediately began the data reconciliation process. They started contacting their bank, customers, trading partners, and other outside organizations to obtain the lost information and enter it into their recovered systems. Because they had done substantial preparation in anticipation of an occurrence such as this, they also had a process by which they could update internal records without generating duplicate output. For example, they were able to enter wire transfer information (for wires that were sent the previous day, but were not reflected on their restored system) without regenerating the wire transfers. This ability to make “memo entries” quickly helped them close the data gap.

By being prepared, they were able to manage the expectations of the system users. This helped bring a sense of calm to the reconciliation and customer service areas. Personnel understood the nature of the problem and were able to respond to the situation.
LIVING WITHOUT TECHNOLOGY

It became very evident following the events of September 11 that a technology recovery was going to take much longer than most companies expected. It was not unusual for recovery of even basic computing (desktop installation, e-mail, Internet access, word processing, and spreadsheet capabilities) to take days — even weeks. Business processes took even longer. The more complex the interfaces and data recovery, the longer the process took.

As a result, the companies that had relocated staff to alternate facilities were trying to conduct business without IT support, as were companies that were not located in the affected area but whose IT function was housed there. Phones began to ring, customers were trying to get information or wanted to place orders, checks were being cashed, bills were being paid, and trades were settling. In short, business was still moving ahead. The question was whether companies could continue and maintain control without their IT security blanket. As in the general case of recovery, the answer for some was yes; but many other companies had moved into uncharted waters.

Companies that had considered an extended IT outage had prepared detailed instructions for dealing with this kind of situation. They created manual workarounds to function in a non-IT environment. By the manual workaround process, a decomposition of IT processes was mapped to alternate manual procedures. To do this successfully, the mapping was done on an end-to-end process basis. For example, the clearing and settlement process was analyzed to ensure that U.S. Treasury operations, clearing bank and depository interfaces, trading and repo desks, and risk management were included in the process. This enabled the continuation of business of operations, as well as the control of risk. In an uncertain situation, companies elected not to trade with those whose financial position represented more risk than they were willing to take under these circumstances.

In addition to detailing the manual activities, the companies that were prepared created control logs to ensure that the transactions that were being manually recorded would be entered in the proper sequence when systems became available. This added a control mechanism to the process.

They also prepared the resources they would require to deal with this contingency. In addition to fax machines (to send and receive orders), copiers, etc., they also had some IT data available in the form of reports from the previous day’s close of business. These reports were identified as critical to operating in a manual mode. So, every night, these reports were either printed or spooled for printing at recovery sites. If the report was small enough, it was actually mailed to an external (non-company) but secured e-mail address, allowing it to be recovered from another office, home, or even the local library. This information was used as a
baseline for validating information and managing such things as the beginning-of-day cash position. With the addition of manually recorded transactions and some information about pre-disaster transactions (in the form of peoples’ memories, as well as calls to banks and other business partners), companies were able to maintain reasonable controls over their operations.

The rest of the organizations fell into two categories: those that had some intra-day manual processes and those that had no documented processes. The former had only envisioned a scenario in which there was an IT failure but the facility was unaffected. They also assumed that IT would be available for entry of data and overnight processing on the day of the occurrence. This may have helped them accumulate data but they were totally unprepared to carry this practice into a second day, much less a second week, thus causing confusion and major control problems. As a result, the latter group had difficulty in providing any controlled operations. They provided inconsistent and, in some cases, contradictory processing. Without an understanding of what their counterparts in other organizations within the company were doing, they may have actually done more damage than good.

Consider how the latter group must have fared when systems were finally restored and the data may have been one day, two days, or in some cases a week, out of date. It is not surprising then that they continue to have reconciliation issues.

CONCLUSIONS
What the events of September 11 proved was something that professional business continuity planners have always known: there is no substitution for preparation. Those companies that prepared and tested, tested, and tested some more, recovered quicker with greater control and accuracy. Those that did not prepare may take months to fully reconcile their business operations — at a cost to their bottom line as well as their reputation.

The question companies are asking is: What should I do now? The answer should start with not looking for a quick fix. Software will not provide a silver bullet. The issues are complex and require planning and structure. But there is a course that should be followed:

1. Ensure that there are clearly defined corporate recovery objectives. This will serve as the governance for creating effective strategies and resource allocations.
2. Create a BCP organization with clear-cut roles and responsibilities.
3. Create an incident/crisis management model for reacting to problems.
4. Determine the business case for recovery.
5. Understand your current capabilities.
6. Define strategies for closing the gap between requirements and current capabilities.
7. Explore strategic options.
8. Create plans for IT, business relocation, manual workarounds, and data restoration.
9. Ensure that the deployment of plans makes them easy to maintain.
10. Test, test, test….

Alan Berman is a senior vice-president in the risk consulting practice of Marsh, Inc. He has more than 14 years of experience in business continuity planning, and more than 25 years of senior management corporate experience. His clients have utilized plans he helped create in recovering from actual disasters. He is a Certified Business Continuity Professional and has been a keynote speaker for the American Red Cross, IBM, NYSSA, and SIA, among others. His articles have appeared in Contingency Planning & Management, and WSTA Ticker and Securities Operation Forum. He is often quoted in publications, ranging from healthcare to financial services.