

**FOR PUBLIC
RELEASE**

CHAPTER

1

Introduction

It is perhaps inevitable that for an entire generation of Americans, the word “disaster” will be inexorably linked to the horrific events that shattered a pleasant morning in New York City and Washington, D.C., on September 11, 2001. No other single incident, save perhaps the attack on Pearl Harbor, struck so profoundly or so deeply into the consciousness of the nation.

For most, the experience was a vicarious one—but one made more tangible by the video footage of commercial aircraft smashing into the twin towers of the World Trade Center (WTC) and the subsequent reduction of those buildings—and a wing of the Pentagon—into twisted masses of debris that CNN and other news agencies repeated over and over in the days and weeks that followed. For those who were actually at ground zero, who were working in the buildings when the terrorists struck or sifting through the rubble of the WTC or the Pentagon in the aftermath of the attacks, the reality of the disaster was overwhelming.

There had been other disasters before 9/11, and some had taken an even greater toll in terms of human life. However, none had generated such resonance in the minds of those who were not directly affected by the calamity.

It could be argued, of course, that this disaster was different from any other event, both in terms of its emotional impact on a nation and also in a number of other eminently practical ways. The fact that the attacks had been deliberate and intentional acts undertaken in accordance with a carefully thought-out plan, rather than a natural and random event, touched off an emotional whirlwind that for a time impacted the energy and attention spans of everyman. Moreover, as the government braced itself for the possibility of more attacks, air transportation and stock markets were shut down for several days. These actions changed the

milieu in which business recovery plans must execute and increased the scope and duration of the disaster.

Aside from the social and political consequences of 9/11, perhaps the most extraordinary thing about the disaster was that so many of the impacted organizations appeared to lack any sort of disaster recovery plan. Of the 440-odd businesses occupying the WTC, the thousands of businesses in Lower Manhattan affected by the interruptions in power, telecommunications and access to facilities, and the numerous governmental entities in the Pentagon, only a small subset—perhaps as few as 200—evidenced preplanned continuity strategies.

This estimate is based on press accounts of the number of firms that formally declared a disaster and activated their contracts with any of the several leading “hot-site” vendors. (A hot-site contract provides for a facility, computer equipment and networks that can be put rapidly into service to replace a subscriber’s “production” IT infrastructure when and if normal operations are interrupted by a disaster event.)

To be generous, a few organizations may not have needed the services of a hot-site vendor in the wake of the disaster. In some cases, only “branch office operations,” rather than a primary headquarters or important data center, were hosted within or around the WTC, or inside the Pentagon. In a few more cases, organizations may have activated “homegrown” recovery strategies that didn’t require the participation of a commercial service provider.

Even with these exceptions factored in, however, the number of companies that were not prepared for the possibility of a disaster like 9/11 were likely the majority. The sad truth is that, as in the case of the 143 companies that simply disappeared in the months and years following the 1993 bombing of the WTC, many of the companies that endured the 9/11 tragedy without a continuity plan will likely not see the end of the decade. These companies will learn their lessons about the importance of disaster recovery planning the hard way, adding further pain and anguish to the already sad memory of that awful event.

Once the immediate sense of threat had ended and the period of mourning had subsided, stories began to emerge about the efforts of organizations to recover from the disasters—to restore business critical operations to some semblance of normalcy. Specific lessons were learned that will be referenced where appropriate in the discussion that follows.

Perhaps the most important lesson to be learned from 9/11, from a disaster recovery perspective, is one of business dependency on information technology and, by extension, its vulnerability to the unplanned interruption of access to information technology (IT) of infrastructure.

Driven by the incentives of cost-efficiency and competition, business has placed more and more of its critical information assets into automated systems and networks. This, in turn, has made business dependent upon the uninterrupted function of the machine, a dependency rarely perceived by those within the corporation who have no direct contact with the IT infrastructure itself. The

consequences of a loss of access to the IT infrastructure to the business may never be considered—until a disaster occurs. By then, it is often too late.

Recent business experience—both before and after 9/11—is replete with examples of companies that failed to recover from a disaster. Some were consumed by a flood or fire that demolished offices and data centers, leaving skeletons of twisted metal and smoking rubble. Others died gradually over several years, after being crippled by a catastrophe from which they could never fully recover.

However, in the same historical experience, there are also examples of companies that suffered disasters of the same magnitude and survived. They emerged from the crisis, with critical operations intact, to regain their position in the marketplace and to continue their commercial pursuits.

One must ask the reason for the different outcomes. Why do some companies survive when others fail? Is it simply fate or chance that determines success or failure in disaster recovery?

The word *disaster* connotes chance or risk. It is derived from the Latin word for “evil star”—a metaphor for a comet, once thought to be a harbinger of some impending doom. While the word embodies a fatalistic view of the unavoidable and inexplicable nature of disaster, it also communicates a positive corollary: Forewarned is forearmed. Knowing in advance that a disaster might happen provides the ability to prepare and to mitigate its consequences.

The insights of the ancient Romans continue to hold truth for modern organizations. Mounting evidence supports the contention that companies can take measures that will improve the likelihood of full recovery following a disaster. Companies that plan for the possibility of a disaster—that implement preventive measures to avoid predictable events and formulate strategies for recovering critical business processes in the wake of events that cannot be prevented—generally do survive disasters.

WHAT IS DISASTER RECOVERY PLANNING?

This book is about disaster recovery planning. As defined here, disaster recovery planning consists of a set of activities aimed at reducing the likelihood and limiting the impact of disaster events on critical business processes.

This preliminary definition may raise a few eyebrows. In the past few years, there has been an effort in some quarters to distinguish the concept of disaster recovery from a related concept, business continuity planning.

To some commentators, disaster recovery pertains to a specific domain of disaster events: recovery from natural disasters such as floods, hurricanes, and earthquakes. Business continuation planning, some argue, covers a broader domain of events, many of which may be less cataclysmic and life threatening in nature. Software viruses, hard disk failures, malicious attacks on systems and networks by hackers or disgruntled employees, and many other factors can and do cause interruptions in normal business processes without necessarily result-

ing in the widespread regional damage that might be left in the wake of a hurricane.

At the level of semantics, a measure of clarity is contained in the term “business continuity planning” that may not be present in the term “disaster recovery planning.” Business continuity more concisely describes the objective of this type of activity, which is to sustain mission-critical business processes during an unplanned interruption event. By contrast, some would argue, the term “disaster recovery” is semantically flawed. By its nature, a disaster is a nonrecoverable event. If recovery is possible, because of the implementation of some planned strategy, then an unplanned interruption event does not, strictly speaking, constitute a disaster.

This book does not seek to contribute to the semantic debate. Suffice it to say that the use of the term disaster recovery planning in this book encompasses the objectives attributed to all of the other forms. Namely, it is a set of activities intended to prevent avoidable instances of unplanned interruption, regardless of cause, and to minimize the impact of interruption events that cannot be avoided.

PURPOSE OF THIS BOOK

This book is designed to equip company planners with the background knowledge and skills they need to develop an effective disaster avoidance and recovery capability for their companies. It is also intended to serve as a primer for information technology managers and business executives in the critical and sometimes mysterious discipline of disaster recovery planning. It may be useful as a guide for managing the activities of the planning project, whether such a project is undertaken by internal personnel or outside consultants. Finally, it is a pragmatic reference describing the products, practices, and politics of the disaster recovery industry that has emerged over the past three decades.

After reading this book, the reader will understand the principles of disaster recovery planning and will be equipped with a generic model for a DR planning project that he or she may emulate to develop a workable disaster recovery plan. Along the way, the reader will be exposed to some of the current debates and emerging technologies of disaster recovery as well as firsthand experiences of numerous business planners in both the preparation and implementation of disaster recovery plans. All that will remain is for the reader to select and apply what has been learned to develop a workable plan for his or her own company.

A WORKING DEFINITION OF DISASTER

The term disaster, as used in this book, means the unplanned interruption of normal business processes resulting from the interruption of the IT infrastructure components used to support them. This definition includes information systems and networks and their hardware and software components—as well as data itself.

Of IT infrastructure-related business process interruptions, those resulting from a loss of data itself are arguably the most devastating. Whether a loss of data results from accidental or intentional erasure and/or the destruction of the media on which data is recorded or from any of a number of manmade or natural phenomena, data is the most difficult of all infrastructure components to replace. As a result, interruptions of business processes resulting from data loss may be the most difficult to surmount.

In addition to data loss, business process interruptions can also result from a loss of IT infrastructure components used to transport, process, and/or present data for use. A broad range of factors can lead to infrastructure component loss. These may include events that cause the destruction of key system, network or storage hardware or software, such as fires or floods. Component “loss” may also be the by-product of disruptions in regional infrastructure supports such as power or telecommunications outages.

These infrastructure interruptions have the potential to wreak as much havoc within a company as the loss of the data itself. However, their effects can generally be minimized through the application of recovery or continuity strategies that are the result of advanced planning and preparation.

The above description of disaster may suggest that only a major calamity—a terrorist bombing, an earthquake, or even a war—would qualify as a disaster. The term disaster conjures to mind a smoking data center at Goliath, Inc., rather than an accidental hard disk erasure at the small business office down the block. In either case, if the result is an unplanned interruption of normal business processes, the event may be classified as a disaster. Disasters are relative and contextual.

THE TIME FACTOR IN DISASTER RECOVERY

However, despite contextual diversity, there are some constants about disasters. One is time.

Because of business’ growing dependency on customized information systems and networks, alternatives to system-provided functions and information cannot be implemented readily. Yet, for a business to survive a disaster, the time factor for restoration of system functions is critical.

In the past, interruptions in normal processing could be withstood by most companies for a protracted period of time. A 1978 study by the University of Minnesota depicted the resilience of business to system interruptions, suggesting that most companies could survive interruptions of 2 to 6 days in length.¹

Given the increased dependency of business today on information technology, it is hard to imagine a company withstanding an outage of more than 48 hours without incurring serious difficulties for its market position. Indeed, for companies ranging from brokerages and banks to e-commerce vendors and just-in-time manufacturers, the costs associated with even minimal system or network interruptions may be extremely high.

This is underscored by data from the Meta Group, describing the cost of downtime by industry segment. The Meta Group study looked at downtime costs from the perspective of employee idle time and suggested that the average cost to an organization an hour of downtime exceeded \$1 million. (See Table 1–1.)

While industry- and application-specific averages for downtime cost are poor indicators of specific business vulnerabilities, they do point out the growing dependence of business processes on IT infrastructure. In view of business' dependence upon its information technology infrastructure and its vulnerability to an unplanned interruption of normal information processing activity, it makes sense for a company to plan and prepare for this possibility.

Recent events attest to the fact that those who plan for unplanned interruptions fare better than those who do not. A brief listing of some disaster recovery successes illustrates this point. In the last decade, publicized business process interruptions (excluding 9/11 attacks) included:

Table 1–1 The Cost of Downtime from the Perspective of Lost Revenues and Employee Idle Time

Industry Sector	Revenue/Hour	Revenue/Employee Hour
Energy	\$2,817,846	\$569.20
Telecommunications	2,066,245	186.98
Manufacturing	1,610,654	134.24
Financial Institutions	1,495,134	1,079.89
Information Technology	1,344,461	184.03
Insurance	1,202,444	370.92
Retail	1,107,274	244.37
Pharmaceuticals	1,082,252	167.53
Banking	996,802	130.52
Food/Beverage Processing	804,192	153.10
Consumer Products	785,719	127.98
Chemicals	704,101	194.53
Transportation	668,586	107.78
Utilities	643,250	142.58
Healthcare	636,030	142.58
Metals/Natural Resources	580,588	153.11
Professional Services	532,510	99.59
Electronics	477,366	74.48
Construction/Engineering	389,601	216.18
Media	340,432	119.74
Hospitality/Travel	330,654	38.62
AVERAGE	\$1,010,536	\$205.55

Source: *IT Performance Engineering & Measurement Strategies: Quantifying Performance Loss*, The Meta Group, Stamford, CT. October 2000.

- An anthrax scare in November 2001 temporarily closes Empire Blue Cross/Blue Shield's data center.
- Tropical Storm Allison floods the Texas Medical Center Campus in June 2001, closing 54 medical institutions.
- Rolling power outages in California leave hundreds of companies in the dark during the summer of 2001.
- An earthquake measuring 6.9 on the Richter scale in the Seattle area hits numerous companies including Boeing Corporation in March 2001.
- A computer glitch causes Delta Airlines subsidiary, Atlantic Southeast Airlines, to cancel or delay over 400 flights in February 2001.
- In 1999, pipe break floods Charles Schwab and Company offices in San Francisco, California.
- In 1998, roof collapses and floods at Landstar Systems in Jacksonville, Florida.
- A tornado hits on Bank of America Corporation's Nashville, Tennessee, operations center in 1998.
- Hurricane Georges causes the evacuation of Degussa Corporation in Theodore, Alabama, in 1998.
- A 1996 data center fire occurs at Humana Inc. headquarters in Louisville, Kentucky.

The above examples, and many others, provide empirical evidence of the efficacy of disaster recovery planning. In virtually every case, companies that experienced potentially devastating disasters implemented tested contingency plans and survived to continue operating in the marketplace.

By contrast, as mentioned above, nearly 150 companies without disaster recovery plans were dealt a death blow in February 1993, when a bomb wracked the World Trade Center in New York.² These firms learned too late that when a company does not have a tested set of procedures for reacting to and recovering from a catastrophe, it places all of its other plans and objectives in jeopardy.

Business Continuity Planning Consultant Philip Jan Rothstein correctly observes that documented information about the outcomes of system or network interruption events, both in the presence and absence of recovery plans, remains very limited. He bristles at the use of gross estimates of downtime cost as a substitute for factual industry statistics.³ The point is well-taken, especially as it pertains to business failures following disaster. In many cases, the relationship between a disaster event and business failure is not discussed publicly at all. Moreover, failures of businesses that are rooted in a disaster event may not occur until several years after the event, making the relationship difficult to document.

Based on available evidence, the time required to recover critical business processes following an interruption is a universal determinant of successful recovery. Unplanned interruption can cost a business dearly in revenues, reputation, customers, and investors. The objective of DR planning is to recover mission-critical processes as quickly as possible following the interruption event to mitigate its duration and costs.

However, evidence also suggests that interruption costs do not remain constant following a disaster event. They may rise exponentially, then decline over time. Assuming that a company can sustain itself through the initial high-cost interruption period, even those without tested DR plans may be able to recover their operations and live to fight another day.

While this may seem to contradict the recovery time factor argument cited above, in fact it confirms it. Companies can elect to expend time, effort, and resources in advance of a disaster to reduce the risk of business failure, or they can do nothing, accept the risk, and hope that their IT infrastructure can be repaired “on the fly” following an unplanned interruption.

Even in the absence of a statistical DR planning nirvana—the availability of exacting data on outage costs and business failure rates that would provide an airtight case for planning—numerous case studies can and do make a persuasive argument. Proactive planning can avoid certain risks and mitigate the impact of others.

THE NEED FOR DISASTER RECOVERY PLANNING

The need for disaster recovery planning is usually self-evident to an IT professional. Who, after all, has a more personal stake in the survival of a company’s information systems than the manager whose position, prestige, and salary directly depend upon system performance?

In addition to self-interest, information managers often manifest a protective, almost parental attitude toward “their” systems. This is especially true when systems have been developed in-house. Effective IT managers and chief information officers (CIOs), like good parents, take a personal interest in the safety and health of their charges.

Beyond self-interest and psychological factors, the IT professional has an ethical mandate to protect data integrity and ensure system and network survivability. Service level agreements between the IT department and company’s end user departments are one manifestation of this commitment to quality and excellence in IT services. Contingency plans must exist if service level agreements are to be made in good faith.

Given all the compelling arguments for undertaking disaster recovery planning, it may seem redundant for auditors and federal law to require it. Unfortunately, a 1998 survey of 4,255 IT and information security managers conducted by Ernst & Young and Computerworld revealed that over half had no disaster recovery plan in place for their companies.⁴ The study further showed a decline in attention to disaster recovery planning generally, despite increasing downtime-related costs:

While over 59% of this year’s respondents said they experienced financial loss due to system downtime or failure within the past 12 months, only 41% of the organizations surveyed have a [disaster recovery] plan, compared to 55% last year; of that number, 34% have never tested the plan. In approximately 45% overall, there was no

budget for [DR planning] activities. . . . In 45% of the organizations surveyed, there were no full-time employees dedicated to [DR planning], while 26% had none last year. The number of part-time employees allocated has also decreased: in 1997, 20% had no part-time [DR planning] employees; this year it is 53%.⁵

One year before the Ernst & Young survey, the Meta Group interviewed 100 of its Fortune 1000 company clients and discovered that fewer than 5% had “back-to-front” disaster recovery plans in place. Missing were provisions for the recovery of client/server systems, even in those companies that were in the process of migrating mission critical legacy applications onto distributed platforms.⁶

In the absence of effective planning, it has fallen to auditors, and in some cases legislators, to apprise corporate information managers of disaster recovery planning requirements and to enforce them as a matter of law.

THE AUDITOR'S VIEW

Auditors tend to view disaster recovery planning as a facet of an organization's efforts to guarantee the security and integrity of its data processing capability. While in the past auditors may have been content with a regular schedule for off-site storage of backup tapes and a paper plan gathering dust on the IT manager's bookshelf, their level of sophistication has grown. Documented and tested disaster recovery plans are increasingly regarded by IT auditors as a necessary component of business operation integrity.

Internal auditors are also taking a more active role in helping develop business recovery plans, often to ensure that corporate management (for whom they serve as the “eyes and ears”) is not exposed to lawsuits or regulatory censure in the event of a disaster. Another reason for their interest is a well-founded concern that the integrity and security of corporate information assets will be maintained as contingency plans are rolled out and critical business applications and data are transitioned to backup platforms. The importance of this aspect of contingency plan auditing was underscored in the late 1990s as auditors and IT managers alike troubled over the possibility of hacker attacks during the recovery of Y2K-related application failures.⁷

External auditors, especially the “Big Five” consulting/accounting firms such as Deloitte Touche Tohmatsu, Arthur Andersen, PricewaterhouseCoopers, KPMG International, and Ernst & Young, offer disaster recovery planning services to clients. The auditor-as-contingency-planner opens some controversial issues that will be explored later in this chapter.

IT audit handbooks now contain chapters devoted entirely to auditing the IT department's disaster recovery plan. Auditors are paying increasing attention to the following areas as they examine a company's disaster recovery plan.

- Plan revisions. While IT auditors may have no way to determine a plan's solvency or workability (unless they are invited to participate in an actual

test), they may look to see when the plan was last revised. They are also interested in procedures providing for the regular review and revision of the document and for the regular reporting of system changes that must be accommodated within the plan. A list of revision dates should appear in the back matter of the plan document to answer these questions.

- Plan test schedule and results assessments. An untested disaster recovery plan cannot be assumed to provide an adequate measure of recoverability to corporate data assets. Tests provide the means for assessing the workability of strategies for evacuation and recovery that appear to work well on paper but may not perform well in real life. A schedule of regular testing and documentation of methods and results are important indicators to the auditor of management's attentiveness to the disaster recovery requirement. This is also typically added to the back matter of the plan.
- Training and awareness. It is often said at IT Security and Disaster Recovery Planning seminars that DR plans are "living documents." A disaster recovery plan addresses two time frames: the future time frame, when the plan will be implemented to cope with some manmade or natural catastrophe, and the present time frame, when the plan is maintained and tested, plan participants are trained, and every corporate employee is made aware of the principles of disaster preparedness and prevention. This dual focus of disaster recovery planning presumes an ongoing training effort. Thus, auditors may ask to see a schedule indicating the dates, topics, and attendance by key recovery personnel at training sessions covering the many aspects of the plan. They may also wish to see evidence of provisions made to increase safety awareness within the company as a whole. Awareness posters in dining areas and elevators, handouts for new employees, and even designated "disaster awareness days" may be some of the ways that this audit requirement can be satisfied.

In addition to these general items, there are many specific requirements of a disaster recovery plan that may be checked or verified by the auditor. These may include:

- A fully articulated planning rationale, providing an overview of threats and exposures and prioritization of risks based on potential business impact and other factors (e.g., likelihood of occurrence), plus a discussion of mitigation strategies considered and selection criteria applied.
- Effective disaster prevention and mitigation measures for all critical business process infrastructure components, including strategies for system, network, and end user work area recovery and evidence that these measures can be implemented in whole or part in response to various interruption scenarios.
- Documentation of relationships with other companies for backup of system platforms in the event of a facility disaster, including contracts with vendors

of system backup facilities and services (hot sites, shell sites, mobile recovery facilities, etc.).

- Contracts and schedules for regular off-site storage for paper files and magnetic media backups, schemes for electronic tape vaulting, and/or remote data mirroring with off-site entities.
- Provisions for network recovery including contracts with network vendors for on-demand rerouting or automatic switching of voice and data communications services to a designated alternative work site.
- Specifications for fire protection systems, power continuation systems, water detection systems, and automated detection and alarm systems for other contingencies (disaster prevention capabilities).

AN IMPERFECT LEGAL MANDATE

In many industries, the dictates of common sense and audit requirements are supplemented by legal mandates for disaster recovery planning. The U.S. government has enacted legislation or issued regulations that require a broad range of contingency planning and related activities to be undertaken by businesses. A partial list of these provisions is provided in Table 1–2. In addition, many states are currently deliberating legislation pertaining to contingency planning, and some, including Florida and Maryland, have already passed laws requiring demonstrated disaster recovery capabilities for certain industry segments. Readers are urged to consult a lawyer specializing in computer and business law to determine the requirements that pertain in their respective states.

Federal mandates for disaster recovery planning affect various industry segments unevenly. Financial institutions, particularly those participating in the various components of the federal banking system, must comply with a well-rooted regimen of regulations on DR.

National banks, for example, must comply with Comptroller of the Currency Banking Circulars and Federal Financial Information Examination Council (FFIEC) guidelines that require them to develop means to reduce the impact and/or risk of losing IT support for business-critical applications.

In many cases, bank management is made directly responsible for determining critical functions at the bank, assessing the risk and potential impact of a loss of IT support for those functions, and developing plans to reduce the risk and/or impact of such a loss. Moreover, boards of directors are obligated to review the plans of bank management annually, approve them, record their approval in the board minutes, and provide the minutes for review by the bank examiners. The intent is to make both the board and bank management legally liable for a bank failure arising from inadequate preparation for an IT outage.

Other banking regulations extend management accountability for disaster recovery planning to include the performance of service bureaus. Banks using service bureaus to process information are required to investigate the financial

Table 1-2 Partial Business Recovery Regulatory Profile

Regulation	Industry	Description
Comptroller of Currency BC-177 (1983, 1987)	Banking	Amended since original in 1983; requires banking institutions to develop and maintain Business Recovery Plans
Federal Home Loan Bank Bulletin R-67 Inter-Agency Policy from Federal Financial Institutions Examination Council (FFIEC—1989, 1996)	Banking Banking and any related service bureaus	Follows intent of BC-177 Requires business-wide data and IT protection planning for banking institutions and extends regulation to require contingency plans from any service bureaus or outsourcing companies which service such banks.
Financial Institution Letter from Federal Financial Institutions Examination Council (FFIEC—1997)	FDIC Supervised Banks	Emphasizes to the board of directors and senior management the importance of corporate data protection functions, also addresses issues that management should consider when developing a viable IT security plan
Fair Credit Reporting Act	Reporting Agencies	Ensures credit information is accurate and up-to-date
Foreign Corrupt Practices Act (1977)	Cross-Industry	Management accountability through record keeping
IRS Procedure 86-19	Cross-Industry	Legal requirements for protecting computer records containing tax information
IRS Procedure 97-22, Cumulative Bulletin 1997-1	Cross-Industry	Compliance requirements for electronic storage systems used to maintain record-keeping information
IRS Procedure 98-25, Internal Revenue Bulletin 1998-11 Federal Response Planning Guidance (1994) FRPG 01-94	Cross-Industry Federal depart- ments and agen- cies	Requirements for documentation of machine-readable recordkeeping system processes Outlines responsibilities and objectives of data protection planning
GAO/IMTEC-91-56 Financial Markets: Computer Security Controls	Financial	Security guidelines for stock markets
Gramm-Leach-Bliley Act of 1999	Financial	Requirements for guaranteeing information privacy and security
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Healthcare	Requires adequate provisioning for health information privacy and security
Accreditation Manual for Hospitals (1994)	Healthcare	Guidelines for information management including security
Clinical Laboratory Information Act (1988)	Healthcare	Specifies requirements protection of critical laboratory data

Source: U.S. Government sources and William P. Dimartini, "What Drives Business Recovery Planning—The Carrot or the Stick?," *Contingency Planning & Management Magazine*, March/April 1996, © 1996 Witter Publishing Corp.

condition of their servicers annually and to develop alternate processing strategies if the servicer's financial condition is deteriorating or unsound. They are also required to prepare their own contingency plans for mitigating exposure to a failure of the service bureau's processing capability.

The focus of federal regulators on the disaster preparedness of financial institutions in particular originated in the wake of an actual disaster. Following a computer failure at the Bank of New York in 1985, senior officials of the bank were summoned to appear before a Congressional investigating committee that, at one point in its hearings, considered the possibility of removing senior managers from their positions for not adequately preparing for a disaster.⁸

Bank of New York, reputedly the state's largest broker for government securities, experienced an IT outage that lasted approximately 27 hours. To continue operations, the bank was forced to borrow \$22 billion from the discount window of the Federal Reserve Bank. It did so at an interest rate well below prime. The huge loan briefly destabilized the weighted rate of federal funds and cost the bank (or its insurer) \$4 to \$5 million in interest.⁹ While Congress did not remove management in this case, the Federal Reserve did issue a circular that set the rate for borrowing in the face of an IT failure at prime plus two.

Not all federal regulations are reactive, however. In the late 1990s, the Year 2000 (Y2K) problem focused the attention of some regulators on corporate contingency planning as a proactive measure—a hedge against widespread economic calamity.

The Securities and Exchange Commission (SEC), for example, required all publicly held companies to disclose the details of their Y2K remediation projects, including contingency plans, as part of their SEC filings. Presumably, this requirement was intended to pressure companies to deal with their Y2K vulnerabilities by making the status of their preparedness a matter of public record.

The regulation cajoles companies to perform Y2K remediation by providing prospective investors with an additional criterion for making investment decisions. It may also provide a basis for shareholder lawsuits in the wake of Y2K outages if false claims are made by companies about their preparedness.

The regulation further incites companies to remediate their application code or risk being dropped as suppliers by business customers who depend upon their products within their own supply chains. As the 1990s drew to a close, many companies were actively reviewing their supply chain providers and selecting new, Y2K-ready providers for critical supply sources.

The close attention paid to the disaster preparedness of the financial industry (and to Y2K remediation across all industries) by federal lawmakers and regulators is not indicative of a comprehensive DR planning mandate, however. In many cases, disaster recovery planning requirements must be interpreted from legal language pertaining to recordkeeping requirements.

The Foreign Corrupt Practices Act of 1977, for example, requires only indirectly that companies undertake contingency planning. The post-Watergate-era

legislation was conceived as a mechanism for prosecuting companies that routinely used bribes to obtain business advantage in foreign markets. However, the recordkeeping provisions of the law are sweeping and have been adopted by the SEC and applied to all publicly held companies.

The recordkeeping provisions of the Act require companies to keep and safeguard records that clearly indicate how their assets are used. The original intent was to eliminate vaguely labeled accounting entries, such as “slush funds,” which investigators found were often used to disguise bribery payments. According to the legislation, any accounting system that fails to indicate clearly how money is disposed of violates the Act. The SEC has since used the Act in several cases to prosecute wrongdoers who have not engaged in bribery of foreign officials, but whose actions technically violate the Act’s accounting requirements (much like the federal government has used tax laws to prosecute organized crime figures whose “real” crimes cannot be proven).¹⁰

The Foreign Corrupt Practices Act pertains to any company using manual or computerized ledger, accounts receivable/accounts payable, or other accounting systems. Under the law, a business must take measures to guarantee the security and integrity of its recordkeeping system—a provision that has been widely interpreted as a requirement to undertake contingency planning. The Act further provides the means to prosecute individual managers and corporate executives who fail to comply with the Act. By legal extension, management can be prosecuted for failing to plan adequately for recordkeeping system recovery following a disaster.

Individual fines of up to \$10,000, 5 years in prison, and corporate penalties of more than \$1 million have been established. To date, however, no penalties have been exacted under the provisions of this law against companies or their executives simply for failing to develop disaster recovery plans.

Another government regulation, from the Office of Management and Budget, requires government agencies to take adequate measures to safeguard the operations of their IT processing facilities. This rule has been interpreted to extend to government contractors and subcontractors and is being rigidly enforced as a matter of national defense. Proponents of the regulation argue that because the design and production of military equipment and other contracted goods are being conducted or controlled using computer systems, the inadequate safeguarding of these systems represents an economic and military threat to the security of the United States. Plans must be made by federal contractors and subcontractors to ensure the availability and integrity of these systems.

The assignment of the ultimate responsibility—in legal terms—for the protection and preservation of corporate assets to corporate management has precedents. The Internal Revenue Service (IRS), for example, has articulated a number of strict rules pertaining to secure storage of business records. Management is often liable if IRS rules have not been observed and the records are lost.

For example, IRS Procedure 64-12 requires that recorded and reconstructable data be maintained in accordance with the Internal Revenue Code of

1954 and that program and source documentation be securely stored so that an audit trail from source documents to final accounting balances and totals may be demonstrated in the event of an IRS audit.¹¹ IRS Ruling 71-20 goes further to describe the requirements for retaining and safeguarding machine-readable records (including punched cards, disks, and other machine-sensible data media) that may become material in the administration of any IRS law.¹² Corporate officers are subject to penalties if these rulings and regulations are not observed.

Besides making provisions for disaster recovery and secure storage of data, the U.S. government further requires all businesses to safeguard the health and safety of employees and to refrain from activities that could harm the community in which facilities are located. The Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA) have issued enforceable codes and regulations aimed at “disaster avoidance” that make company management prosecutable if avoidable disasters occur.¹³ At the state level, numerous agencies and departments have followed the federal government’s lead with fire, building, and emergency management codes that impact on disaster avoidance and recovery planning.¹⁴

BUILDING MANAGEMENT CONSENSUS FOR DISASTER RECOVERY PLANNING

This brief survey demonstrates that the disaster recovery planning project is propelled by a number of considerations, ranging from a common-sense business impetus to safeguard corporate assets from loss or damage to a natural desire to reduce legal exposure and personal loss. This is not to say, however, that corporate management is aware of all of the legal penalties, or even the risks, associated with not having an effective disaster recovery capability. In some cases, management consensus must be cultivated by an information manager or auditor.

The above observation may seem out of step with the current elevated level of attention being paid to disaster preparedness in the wake of 9/11. However, history has demonstrated over and over again that there is a tendency for interest in DR to spike in the aftermath of a disaster, then to diminish rather quickly as the memory of the disaster fades.

Even after a consensus is built to support the planning for business interruption and recovery, sustaining the consensus when it comes time to implement the paper plan—to install the recovery capability—can be difficult. The reasons for the breakdown of the consensus are numerous. In some cases, management exhibits reluctance to spend money acquiring the services and products that are intrinsic to the plan. This often occurs when management does not fully understand the risks and exposures a company faces without a recovery capability.

To address this dilemma, DR consultants recommend that a formal risk analysis process be undertaken early in the disaster recovery planning project.

An assessment should be made of the impact of unplanned interruption events on the business as a whole—including a detailed assessment of tangible and intangible costs accrued to the unplanned interruption of each automated application that supports a mission-critical business process.

As an adjunct to this analysis, any legal requirements that compel management to undertake planning should be cited and clearly communicated. Where the law does not directly mandate disaster recovery planning, other strategies have to be found to convince reluctant senior managers of plan benefits. Effective strategies are often difficult to find.

Convincing corporate management to shoulder the costs of a disaster recovery capability can often be a greater challenge than surmounting the technical problems involved in backing up critical systems and networks. In the final analysis, however, management will play the most critical role in the planning effort—the role of underwriter.

Following are some typical problems reported by the information managers who had to sell their plans to senior management, and the successful strategies they developed to overcome them.

- “You haven’t cost-justified the plan.”

This criticism usually reflects the disaster recovery planner’s failure to document adequately the exposures and risks of not having a plan. Often, planners first encounter this objection when they seek management approval to conduct an analysis of risks and exposures. That is, management may ask the planner to cost-justify the plan before they have authorized an investigation of whether such a disaster recovery capability is necessary!

How does one cost-justify a capability that, in the best circumstances, will measure its success in nonevents? This dilemma was perhaps best expressed in a humorous anecdote that followed January 1, 2000 in which a chief executive officer railed at his IT manager, “You mean we spent all that money on Y2K preparations and nothing happened?!” A good disaster recovery plan, after all, sets the stage for disaster avoidance by providing the means to detect and react to potential problems, in many cases, before they become disasters. Strategies for successfully addressing this problem generally fall into two categories.

One strategy for responding to this criticism is to assign a dollar value to an hour of downtime. Calculate the average hourly earnings of employees who use an application that provides a business process for which a recovery capability will be planned. This provides an estimate of the cost of an hour of lost productivity were an application outage to occur. Assuming that the data could be entered at a later time without other adverse consequences, repeat the above calculation for 1 hour of average overtime salary (i.e., the amount of time all system users would need to work to make up for lost time). Then, add the two dollar costs as the total average labor cost for one hour of downtime.

For applications used by greater numbers of end users, this number by itself could be sufficient to demonstrate the benefit of a disaster recovery capability that would avoid outages or minimize the duration of unavoidable outages. By multiplying the number to reflect 10 hours, 24 hours, 48 hours, and so on, the statistic could be quite compelling.

This approach, while simplistic, can be augmented by citing any documented costs associated with outages that have previously been experienced by the company. However, the planner must keep in mind what was said earlier about the tendency of outage costs to decline over time.

In some cases, the better case can be made by referencing intangible costs. The loss of customer satisfaction, the abrogation of service level commitments, potential legal liability, lost sales opportunities, negative press, and a host of other non-dollar-based factors may hold significant meaning for management. Arguments based on these non-quantifiable factors may actually be more compelling than cost-justification and other quantitative methods. The latter are inherently flawed, in any case, by the lack of reliable data on the likelihood of occurrence for any given disaster potential.

Another way to justify the plan is to demonstrate the collateral benefits of such a plan. An effective disaster recovery capability can actually reduce business insurance costs in some situations. Premiums for facility or business interruption insurance may be substantially reduced in many cases where disaster recovery planning identifies the specific coverages required and blanket insurance policies are replaced with targeted and less-expensive plans.¹⁵

Some disaster recovery capabilities, such as uninterruptible power supplies (UPS), actually do double-duty. They can sustain critical business systems or network devices for a time so that organized shutdowns can be accomplished or independent generators started up in the event of a disastrous power outage. In addition to its use in a disaster, the UPS also supports equipment during the occasional surges, dips, and flickers of a typical business day. In so doing, the UPS can actually prolong the useful life of connected equipment.

Another dual-use scenario may apply to an end-user or workgroup operations center—a facility designed to house users if the main business facility becomes uninhabitable for a period of time. Such a facility may also be used during non-disaster periods as a training or conference facility.

A practical example of dual-use may be found in the case of a certain Midwestern state government's IT department. In the wake of 9/11, the politicians in the state made compelling speeches about the need for disaster recovery but allocated no money for building such a capability. The IT manager for the government did, however, manage to receive funding for an "application development and testing center." Determined to build a redundant facility for disaster recovery, the savvy IT manager replicated virtually all critical production systems and networks at the alternate site and

created an internal hot site while also providing a location for developing and testing new systems before they were deployed into production for the state. Sometimes, as this case suggests, planners may need to become downright sneaky to overcome obstacles to effective planning.

Dual-use benefits can usually be discerned for most disaster recovery plan components, given sufficient time and creative energy. When a particularly compelling benefit cannot be found to outweigh a cost, the impact of the cost may be softened if it is examined from the perspective of tax deductions, health and safety of personnel, or good corporate citizenship.

- “Our insurance will cover an outage, so why do we need the plan?”

Even if a consensus exists for developing a plan on paper, management may resist spending money for implementation, especially if the disaster recovery capability is viewed as just so much more insurance. According to spokespersons for two data processing insurers, the right insurance policy will cover operating costs that are above the normal costs of business operations, provided that the appropriate “extra” costs are spelled out in the policy. This business interruption insurance, however, should not be viewed as business resumption insurance.¹⁶ An information manager may need to educate management in the following facts.

Insurers can readily cover the costs of facility damage (and, in some cases, replacement), and they can provide coverage for hardware and media. However, while insurers are willing to underwrite the reconstruction of data lost to a natural or manmade disaster, it would be cost prohibitive to the client to underwrite the value of the data.

Without a disaster recovery plan, the client would be hard pressed to estimate the cost of reconstructing data or to buy adequate insurance for doing so. In all likelihood, without a disaster recovery capability, there would be nothing with which to reconstruct the data: no extant records, no systems, no location for personnel to work. Purchasing extra coverages under these circumstances would be pointless.

In a disaster situation, a company protected only by business interruption insurance is placed in the unenviable position of relying on the progress of the claims adjustment cycle to drive the recovery. While top insurers generally provide excellent turnaround on disaster claims and may even provide support services to facilitate the insured’s recovery activities, this is generally less desirable than controlling recovery within the business itself and capitalizing on the determination and commitment of trained recovery teams who are employees of the company.

If management does not understand the problems inherent in depending on insurance to recover from disaster, planners should provide information about the experience of companies that have experienced disasters firsthand. The aftermath of Hurricane Andrew—the subsequent flight (and, in some cases, bankruptcies) of property and casualty insurers from the state of Florida—attests to the impact of a regional disaster on insurance compa-

nies as well as the potential problems companies confront in obtaining the timely handling of insurance claims.

The bottom line is that business interruption insurance is properly regarded only as a supplement to a tested disaster recovery capability. It is never a substitute for planning.

- “The purpose of the plan is to satisfy the auditors.”

While it may seem blasphemous, managers often express this sentiment in spoken or unspoken terms. One manager of a national financial concern remarked, off the record, that the best disaster recovery plan he could get his company to fund was an up-to-date resume. Sadly, in the absence of rigidly enforced laws, auditors’ comments are often the only incentive for management to undertake disaster recovery planning. Auditors seldom have the power to compel management to do anything it is not inclined to do.

One strategy for surmounting management indifference is to barrage corporate officers with news clippings about business disasters, although this may ultimately cost the sender some prestige or power. The object of this strategy is not to aggravate or frighten, but to create awareness in senior management that disasters do happen and that those who prepare for them generally recover normal operations far more readily than those who do not.

Another method for reducing senior management indifference is to demonstrate that the planner understands and participates in management’s priorities and objectives. This may be reflected in the methods used to create and articulate the plan. For example, every effort should be made to maximize the plan’s protection while minimizing its cost. Despite his or her personal investment in systems and networks, the planner should strive to assess IT resources dispassionately for their criticality to the corporation. Certain applications are more vital than others, a fact that is underscored by carefully analyzing the impact of an unplanned interruption on business applications. It needs to be clearly communicated to senior management that the plan will target the largest share of budget expenditures for the most important applications.

Furthermore, plans must ultimately encompass not only the recovery of IT and network resources but also the user departments. It makes little sense to restore applications if no provision is made to restore the user community. By involving the managers of user departments in the planning project, the planner may be able to cultivate a corporate climate of support for disaster recovery planning. This, in turn, may reinforce senior management’s perception of the value of the disaster recovery planning effort and result in a more comprehensive and effective recovery capability.

Only a few years ago, the Y2K Bug, and the legal exposure it created for a company, captured the attention of senior management. In some companies, it provided an opportunity for DR planners to demonstrate to senior

management that what they do is motivated by concern for the business and for management. While Y2K was merely another software-related disaster potential from the DR perspective, some savvy DR planners were able to leverage management concern to gain political capital that could be used later to expand the scope of DR planning into other areas. The same opportunities exist in the wake of 9/11 and should not be overlooked.

These are only a few of the common problems and strategies used by DR planners to obtain senior management approval for disaster recovery planning costs. Other problems may develop that reflect the particular circumstances of a business, the distribution of information systems, or even the individual personalities of senior managers themselves. Whenever possible, disaster recovery planning should be depoliticized and depersonalized. Since the initial focus of the planning effort is on information systems, the information manager will play an important role in setting the stage for the entire corporate disaster recovery plan.

WHO SHOULD WRITE THE PLAN?

Once the decision has been made to undertake disaster recovery planning, the information manager must first determine the method to be used to develop the plan. One option is to hire a consultant to perform this task. Another is to develop the plan in-house. Valid arguments exist to support each option.

At first glance, hiring a consultant with X years of experience in developing this type of project may seem the best choice. Indeed, this approach has several distinct advantages.

First, the disaster recovery planning project is just as complicated as a major system development project and, in fact, parallels the systems development life cycle (SDLC). (Figure 1–1 depicts the similarity.)

Like a system development project, a disaster recovery planning project begins with analysis. A risk analysis process is undertaken to identify potential threats and vulnerabilities, while business impact analyses and application impact analyses are undertaken to identify critical business processes and their IT infrastructure supports and to discern recovery priorities, objectives, and requirements.

Recovery strategies are then outlined and tasks are prioritized much in the same way that an analyst would set forth a general system design. This general design is subjected to user review and, if it is approved, a detailed system description is articulated. At this point, development costs are specified and a project time-and-money budget is developed.

In systems development, the project would be approved by management, and coding would begin. Similarly, the disaster recovery planning budget is presented to senior management and, if approved, vendors are contacted, products and services purchased, and recovery procedures developed and documented.

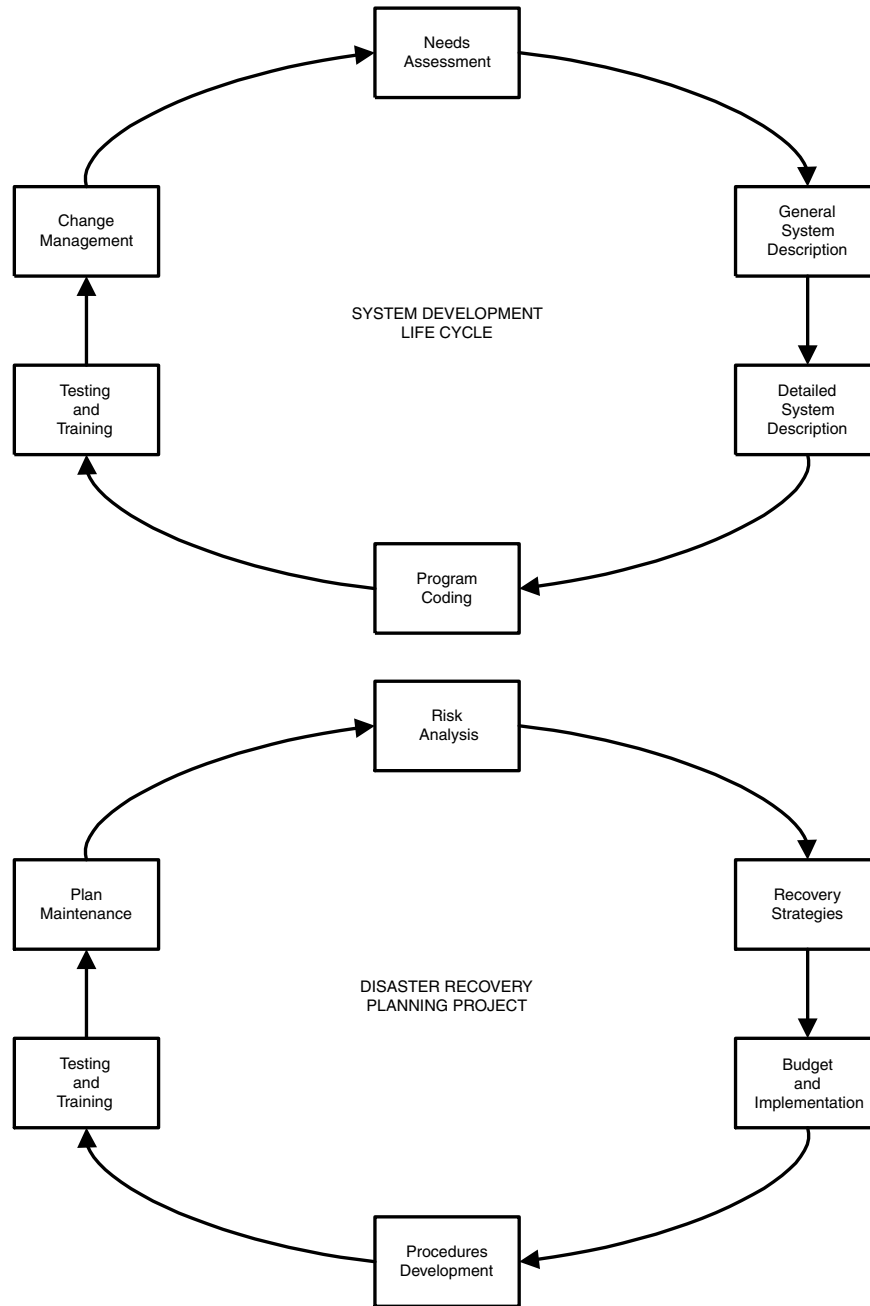


Figure 1-1 Comparison of systems development life cycle (SDLC) to disaster recovery planning project.

Plan testing and user training follow, just as comparable activities would follow the conclusion of coding. Finally, when the system is released or the plan is placed into effect, it is integrated into a change management system to provide for periodic review, revision, and maintenance.

An IT manager, realizing the scope and complexity of the planning project, may decide that a consultant is needed to manage it. The IT manager either cannot reassign an employee to manage the project or feels that no employees are equal to the assignment. There may also be other factors that favor the consultant option.¹⁷

- Consultants bring specialized knowledge to the planning project that may facilitate the speedy development of an effective plan. An experienced consultant knows how a disaster recovery plan is constructed, knows the right questions to ask, and typically knows who's who in the disaster recovery products and services industry. Consultants who work within a specific industry may combine an understanding of the industry with a methodology for disaster recovery planning. This reduced learning curve, in turn, can help to speed plan development.
- Consultants can bring a fresh eye to the project, noticing recovery requirements that may be overlooked by someone who is too close to the data center he or she is seeking to protect. One consultant relayed a story about a client who had hired her to perform a risk analysis of a data center. In conferences, the client confidentially reassured her that all vital processing equipment had been identified. Then, during a preliminary visit to the data center, the consultant nearly tripped over an ancient time card reader. She asked what it was and learned that no payroll checks could be generated without its use. A vital piece of equipment, yet it had not been mentioned anywhere in the lists that otherwise documented completely the state-of-the-art hardware installed in the shop.
- Consultants are expensive. While this may be viewed as a drawback of the consultant option (and will be discussed later in this chapter), it may actually favor plan development in certain cases. Disaster recovery planning requires the interaction of users and information systems and network technical personnel. Within a large information systems shop, where rivalries frequently exist among applications support personnel, systems administrators, and operations, disaster recovery planning will also require the interaction of these groups. Often the only way to get all of the relevant parties to sit down as a group and discuss critical issues is to make it clear that a great deal of money is being spent for the consultant's time. Similarly, senior management, having invested a considerable sum of money for a consultant-developed plan, may be less inclined to withdraw support for the implementation of the plan.

Consultant-driven plans are similar to computer hardware acquisitions: They are usually available with a maintenance agreement. For a fee, the consult-

ant will return on a semiannual basis to aid in the testing and updating of the original plan. Furthermore, since the plan usually reflects the “favored” (read “proprietary”) methodology of the consultant, many consulting firms offer a training service to educate personnel in the client company who will maintain or use the plan.

Good consultants usually produce good plans and provide competent maintenance and training services. Unfortunately, not all consultants are good consultants. As of this writing, the disaster recovery planning consultancy is an unpoliced field. In the late 1960s, there were only handfuls of disaster recovery consulting firms. Since that time, the number has increased exponentially. It is not uncommon for consulting firms to open and close their doors within the same year. This bodes ill for the industry as a whole.

Consultants may attempt to demonstrate their competence by referencing a certification from a DR planning certification body. Several certification organizations have evolved over the past decade with the stated objective of training novice planners and, for a fee, “certifying” the skills of those who have learned their trade “on the job.” Contrary to the view of many who have obtained certifications, the kindest thing that this author has to say about certification programs is that, at present, they provide little assurance about the capabilities of those who hold them.

This assertion is likely to draw fire from several quarters, so it merits further discussion. In the early 1990s, the originator of one of the first certification programs for DR planning contacted this author to solicit his participation in promoting a “marketing concept”: disaster recovery certification. The proposal consisted of selling certifications for a fee to anyone who could pass a multiple-choice test consisting of easy-to-answer questions such as the meanings of familiar acronyms and the definitions of DR-specific concepts such as “dial backup” and “hot site.” Not to be exclusionary, DR practitioners would also be invited to participate. They would be “grandfathered in”—that is, provided the certification without testing in exchange for dues payment. The fellow was clearly delighted with the concept, which he viewed as a “sure money-maker” on three grounds:

1. Many individuals responsible for disaster recovery planning for their organizations suffered from a lack of confidence. They feared that they were not as professional as consultants who developed DR plans for many companies. The certification program would not make them better planners, but it would give them the appearance of professionalism when they interacted with other professionals and with management. Basically, the certification program was a confidence game.
2. The certification program would become a discriminator between consultants in a highly competitive and totally unregulated disaster recovery consulting industry. The revenue potential for the program based on “grandfathering” fees alone was enormous, even if the certification program was meaningless.

3. The certification program would be a great way to amass the world's best database of DR planner names and addresses, which could subsequently be resold to vendors of DR products and services, producing another revenue stream.

Demonstrating a lack of business acumen, the author declined to participate. Nevertheless, the program was launched and became one of the most successful certification programs today.

Recently, an acquaintance of many years, who had retired as the chief disaster recovery planner for a major financial institution, complained that he was required to obtain a certification before he could join the consulting group of a major systems integrator. The fellow was told that in spite of his extensive experience in DR planning, his intimate familiarity with planning methods and tools, his thorough knowledge of vendors and their offerings, his former senior role within a major disaster recovery planning user group, and his numerous references, he was unmarketable without the letters of a certification program following his name on his business card. The situation has achieved the status of a mind-boggling absurdity.

While numerous organizations, including the well-respected National Fire Protection Association, are working to develop objective DR planning standards, effective DR planning remains at this writing a mixture of art and science. Effective planners require a broad base of knowledge across a variety of technologies and business practices. For this reason, disaster recovery planning is not a skill set that is easily tested or certified.

Thus, this book contends that, despite the fact that a consultant's business card contains an acronym for a disaster recovery certification body, this alone is insufficient evidence that the consultant is competent to do an acceptable job for the business client. Some of the best consultants in the field do not have letters following their names on a business card or brochure.

Speaking of credentials, over the past decade, many "Big Five" accounting firms entered the contingency planning business. In other words, the same firm that performs the company's annual audit probably offers a disaster recovery planning service as well.

Despite claims by these organizations that their audit and planning organizations are entirely separate, it is not uncommon, following an audit that discovers a missing or inadequate disaster recovery plan, for a representative of the planning services arm of the firm to pay an impromptu courtesy call on the IT manager, CIO, or other business manager. The accounting firms argue that there is nothing incestuous about this practice, but concerned observers have asked how an auditor can objectively assess a DR plan bearing the label of his or her own firm.

Undoubtedly, there are good and bad consultants in "Big Five" accounting firms just as there are in the "pure" disaster recovery consultancies. The business or IT manager should use the same criteria when evaluating either type of consulting service. The following guidelines may be useful when considering the hiring of consultants to develop the disaster recovery plan.

1. Check the qualifications of the consultant. It is important to know the name and background of the consultant who will be providing services. Find out how many and which companies the consultant has served and check directly with the clients for recommendations and criticisms. Be wary of using an inexperienced consultant, even if he or she reputedly has access to more experienced hands. Ideally, the consultant will be able to demonstrate a knowledge of the IT and network technology used at the prospective client's company, will understand the specific requirements within a prospective client's industry, and will have developed satisfactory disaster recovery plans for at least two other businesses within the same industry.
2. Ask for a project roadmap. Ask for a proposal that shows the phases and tasks of the planning project. The consultant should not view this as an illegitimate request. Over the past few years, with the increasing availability of excellent DR planning project models and improved information on the techniques and methods of recovery planning, consultants have been hard pressed to portray what they do as secret, mysterious, or otherwise beyond the reach of nonconsultants. Most consultants have planning methodologies that they adapt to accommodate specific client requirements. All the manager needs is enough information about techniques and methods to evaluate the validity of the methodology. (For this reason, even if a manager elects to use a consultant, this book will help the manager to evaluate the consultant's planning methodology.)
3. Check and validate proposed time and cost estimates. Read consultant proposals carefully and note, first, whether time and dollar cost estimates have been assigned to parts of the project. Unless consulting services are packaged as fixed-price contracts, there is no way that a consultant can develop meaningful time and cost estimates. The manager should be especially wary if the consultant quotes exact prices or times before knowing anything about the particular requirements of the company.

Estimates provided by the consultant can be of value to the information manager in other ways. For example, valid time and cost estimates can provide a useful benchmark for comparing various consultant proposals, especially if each consultant states that he or she is basing estimates on similar projects performed for similar businesses. This is about the only way "comparison shopping" can be performed for this type of service.

To ensure that the data being collected from each candidate is not skewed by anything other than unknown factors, ask whether all predictable costs, including the consultant's travel and lodging, are reflected in the estimated cost.

IT managers should be aware that some consultants tend to push their premium service initially, and offer less-expensive shared responsibility approaches only if they sense that they may be pricing themselves out of a contract. Faced with the prospect of losing a potential client, some consultants can become very creative in finding cost-saving measures. One manager re-

ported that he cut the cost of consultant-aided plan development in half by offering to provide “administrative assistance” (someone to do word processing, etc.) to the consultant, and by allocating one of his employees to work with the consultant on a full-time basis, replacing the assistant to be provided by the consulting firm. Other managers have discovered that they could purchase the consultant’s PC-based disaster recovery planning tool and utilize the consultant’s personal services only in the up-front analysis and data collection phases of the project. Substantial cost reductions resulted in each case.

Another manager reported that the business ethics of the consultant could be discerned from the way in which he reacted to the manager’s reluctance about costs. In one instance, a consultant offered to reduce costs by dropping the final two phases of the proposed project. These phases consisted of training personnel who would play key roles in the plan and maintenance of the plan document itself. Implied in this offer was the consultant’s willingness to develop a paper plan that would sit on a shelf and satisfy a casual audit but provide no meaningful recovery capability!

Cases such as the one described above are certainly the exception rather than the rule. No stereotyping of disaster recovery consultants is intended—some of the author’s best friends are disaster recovery planners.

4. Ask about the consultant’s relationships with vendors of disaster recovery products and services. Managers who are considering the use of consultants also need to be aware that many consulting firms have formal or informal relationships with vendors of disaster recovery products and services. These relationships can profit the consultant’s client in some cases. Using a particular consultant, for example, may qualify the client for discount rates on fire protection systems, off-site storage, or hot sites (subscription-based system backup facilities).

There is, however, a potential for misuse of these relationships. An unethical consultant may be willing to sacrifice the objective analysis of client requirements in favor of recommending a product or service from which the consultant receives a kickback. It is valuable to know whether and with whom the consultant has marketing agreements, and how these agreements may result in price advantages for the client. Most vendors will openly admit to any special arrangements, particularly when they may profit the client and improve the marketability of their service. Some consultants argue that it is partly their extensive knowledge of the disaster recovery industry that qualifies them for the rates they command.

Should the manager decide to use a consultant, whether or not the consultant admits having special marketing arrangements with vendors, he or she should pay particular attention to soliciting competitive bids for any product or service that the consultant recommends.

For many managers, the cost of a consultant-driven disaster recovery plan is the major drawback. Plans can range from \$20,000 to upwards of \$120,000. This is

generally perceived as a cost over and above the cost for in-house plan development. Consultants respond that their price is reasonable from many perspectives.

A company electing to use in-house personnel to develop a plan must patiently wait for the novice disaster recovery coordinator to acquire knowledge that the consultant already possesses and finance the coordinator's education and pay his or her salary while doing so. Plan development is a slower process when performed by a novice in the field. In the meantime, the company's vital information asset remains exposed. Consultants also point to the fact that most plans begun by in-house personnel are never completed.

Despite these arguments, many companies elect to use in-house personnel. Even consultant plans ultimately require that in-house skills and knowledge be developed. Someone must coordinate plan revisions and maintain the plan between visits by the consultant. In addition, much of the consultant's work must be overseen by in-house personnel since the consultant is essentially an outsider who does not participate in day-to-day business operations. Also, in-house personnel must perform all evaluations of products and services to be used in the plan, partly to ensure the honesty of the consultant.

Finally, in-house personnel now have access to information about disaster recovery planning techniques and methods through special training courses, published articles and books, the Internet and World Wide Web, and by participating in "sharing" groups. So, the learning curve for the in-house planner is drastically reduced.

Generic PC-based planning tools are also now available, and several consulting firms market their own software package containing their proprietary planning tool. These tools provide a structured approach to planning for common equipment configurations. They need to be modified by the purchaser to account for specific applications, networks, decentralized processors, and other characteristics peculiar to the customer site.

Although the PC-based planning tool does not provide comprehensive answers for the novice planner, it can offer valuable models that the planner can imitate when customizing the plan to meet his or her requirements.

Another change that is supporting the development of disaster recovery plans by in-house personnel is the improvement of project management skills across all industries and business activities. The development of a disaster recovery capability is essentially a project with discrete tasks, milestones, resources, and budget. Once the principles peculiar to disaster recovery planning are understood, any person skilled in the techniques of project management can develop a competent disaster recovery plan. Many, including this author, have found that the only tools they require are old-fashioned research and communication skills; email and web browser; a word processor; and a generic, off-the-shelf, spreadsheet, database, or PC-based project management software package.

A final word on the consultant versus in-house development strategy is suggested by consultant Philip Jan Rothstein, who notes that there are other roles for consultants than performing or managing the plan development process.

Consultants can be used in connection with in-house planning efforts “to perform or support certain planning phases” (such as analysis or testing) with specialized methods or techniques, “or to serve as a true consultant—meaning, a knowledge base or coach.”¹⁸

Given the right consultant, such an approach has the potential to deliver the best of both the in-house and the consultant-driven planning project models.

A STRAIGHTFORWARD, PROJECT-ORIENTED APPROACH

This book presents a straightforward project-oriented approach to DR planning. Each chapter provides cogent, practical information about the major tasks involved in developing a disaster recovery capability. Each chapter clearly defines the objectives of a development task, describes typical methods used to realize objectives, defines what resources are typically required, identifies sources for specific products and services, and discusses methods for evaluating task fulfillment.

In some cases, the IT manager or his or her designee serves as the disaster recovery coordinator for the company. In other cases, planning is undertaken by a group of users representing both information systems and the user community. If planning is undertaken by a group, however, it will need a person who will serve sometimes as researcher, sometimes as data collector, sometimes as honest broker, and ultimately as the person responsible for maintaining the plan in the face of almost daily shifts in recovery requirements. All these responsibilities are implied in the title DR coordinator.

In many cases, the IT or business manager will either hire a new employee to serve as disaster recovery coordinator or transfer an employee to fill the position full-time. The critical phrase is full-time. In very small companies, the IT manager is likely to serve as disaster recovery coordinator. In medium to large companies, developing and maintaining the disaster recovery plan is a full-time job.

Who is the ideal disaster recovery coordinator? There is no pat answer to this question. The coordinator does not require the highly technical skills set of a programmer, network analyst, hardware specialist, or systems administrator, but it is important that the candidate be able to communicate with technical staff and correctly interpret what they say in order to communicate it effectively to non-technical users in reports, procedures, and other documentation.

It is important that the coordinator be organized, detail-oriented, and a competent writer. The candidate should be able to work methodically through complex problems and issues and be experienced in managing vendors and evaluating product offerings. He or she should also be fluent in project management principles and techniques. In addition to these skills, the coordinator will need highly developed qualities of patience, perseverance, and diplomacy.

A common theme emerges in meetings of organizations for disaster recovery coordinators. Regardless of the initial level of enthusiasm and team spirit participants bring to the disaster recovery planning project, a substantial effort will

be required to keep participation levels high. Planners need to cultivate enthusiasm and constantly reinforce the buy-in of plan participants. Unless participants see the plan as their creation, nearly everyone will develop a resentment of the planning process.

DR planning is demanding work. IT operations personnel can easily come to view the coordinator's insistence on routine backups as an unwarranted interruption of their already overcrowded processing schedules. They need to be applauded for the work they are doing to safeguard the corporation's most important asset, information.

Similarly, application developers may be put off by the DR requirement that they pause periodically to document changes made to programs and systems so that work can be reconstructed in the event of disaster. Reinforcing the importance and value of their work—known in the vernacular as stroking their egos—may ensure their continued enthusiastic cooperation.

User departments may develop an intense dislike of the coordinator's constant testing and probing for possible gaps in their preventive and protective measures. The coordinator needs to work with users and ensure that they regard the procedures involved as their own effort, rather than a task that is being imposed on them from outside.

Senior management may even come to disdain spending money on a project that delivers little tangible return on investment. Coordinators can diffuse this trap before it occurs by exploring every possible dual-use or dual-value opportunity for disaster avoidance and recovery components.

The relationship with management works both ways. To supplement the skills that the coordinator brings to the job, the IT or business manager will have to provide the coordinator with authority to make decisions and to quell dissent, visible (and budgetary) support and enthusiasm for the planning effort, and personal support for the coordinator's ego.

No statistics are available to demonstrate the stress level associated with the position of disaster recovery coordinator, but considering the nature of the job—the need to confront the dark side of business survival daily and make the safety and security of fellow employees one's personal concern—the coordinator's stress level must rate somewhere between that of a dentist and a Middle East peace negotiator. The manager needs to recognize this and compensate for it, not only in salary, but by freeing the coordinator from other tasks and giving personal recognition and reinforcement for the valuable work that the coordinator is performing.

The above may convey the impression that fulfilling the role of DR coordinator is a thankless task. Before readers rush to put this book back on the shelf, it should be observed that there are few business roles that are more compelling and challenging than disaster recovery planning. Creating an effective team, working across the exclusive territories established by business units, developing innovative strategies to fit requirements, and playing the ombudsman for corporate safety and continuity comprise a dynamic set of tasks that appeal to one's creativity and provide an enormous sense of accomplishment.

A NOTE ON METHODOLOGY

A cursory examination of the literature will confirm that there are as many methodologies for developing disaster recovery plans as there are plan authors. This book seeks to find common ground by returning to the fundamental methodology of project management.

Fortunately, disaster recovery planning is too young an endeavor to have spawned argumentative schools of adherents to this or that guru's methodology. There are no gurus except, perhaps, those who have experienced and recovered from an actual disaster. Having talked with many of them in research for this book, they are wiser and somewhat modest about their accomplishment. Hardly the guru type.

This is not to say that there are not pretenders. In certain facets of disaster recovery plan development, one is almost certain to run up against a vendor representative, a plan author, or a risk manager who is convinced he or she has all the answers. It would seem that, in the wake of 9/11, everybody from the value added reseller to the local cellular telephone salesman has decided to hang out a DR consulting shingle. The best policy is to listen. They may, after all, have a few worthwhile observations.

In the meantime, there are far more important and basic skills to master. One of the most important is one's ability to think systematically about the planning task. This is no simple feat: One must, after all, superimpose rationality on an event that is inherently chaotic—disaster.

It cannot be overstressed that disaster recovery planning is not something that one can do perfectly the first time. Only by putting the plan on paper and testing it can its errors be realized and corrected. The only effective method for DR planning is trial and error.

There are a few other points to make about the approach of this book to its subject. As previously observed, developing a disaster recovery plan is a project entailing the performance of many discrete tasks and the allocation of fixed resources. The end product of the effort is less a plan document than a recovery capability. The plan is only a roadmap for yet another project: recovery from an actual disaster.

To help the reader understand the objectives and alternative strategies that must be considered in the formulation of the plan, it is sometimes necessary to describe in detail how the plan will be implemented in a disaster recovery project. To aid the reader, a simple diagrammatic distinction has been made between the planning project and the recovery project. When this book describes the plan development project, the accompanying illustrations use the techniques of data flow diagramming. When the recovery project is described, flow charts are used.

Data flow diagrams, or DFDs, seem appropriate to the description of the plan development project since the project generally consists of acquiring, processing, and presenting information.¹⁹ Figure 1-2 provides the context for the disaster recovery planning project. It shows the plethora of organizations—

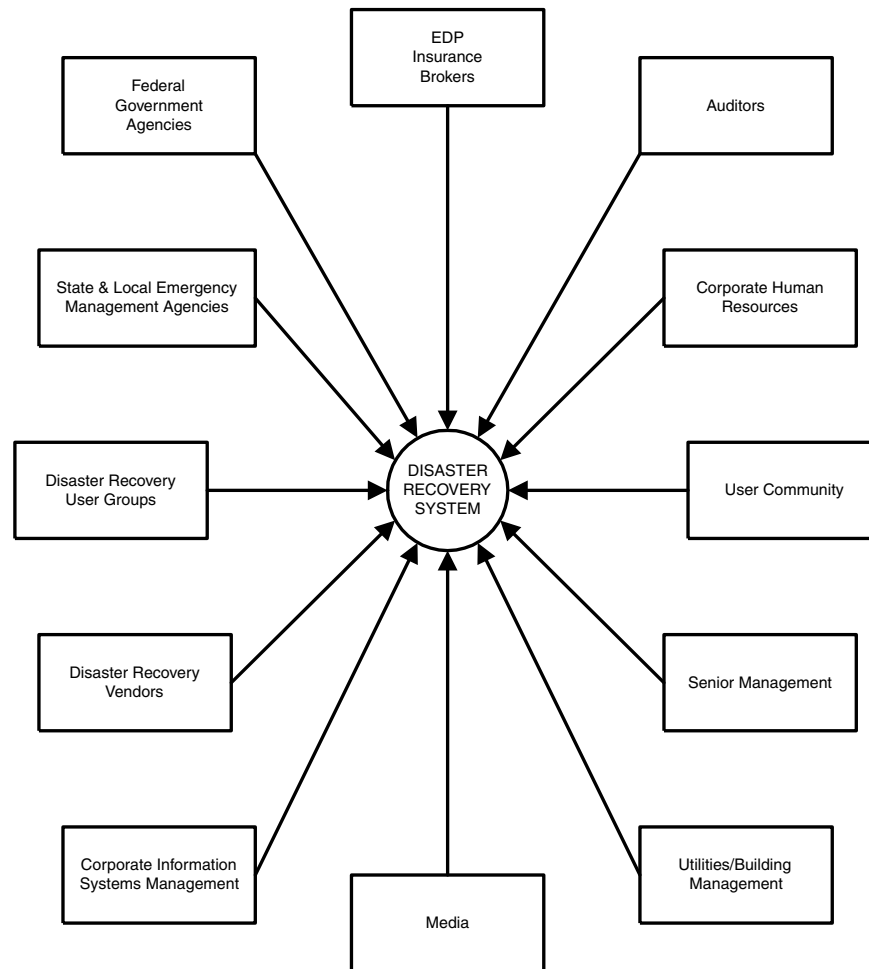


Figure 1-2 The context of disaster recovery planning.

including corporate departments, professional groups, and regulatory agencies—that shape the environment of the planning endeavor and form the reality against which plan adequacy is judged.

From this simple diagram, however, little can be discerned about the components of disaster recovery planning. Thus, in the coming chapters, the reader will find other DFDs that illustrate the major activities involved in the planning project.

For example, Figure 1-3 is a DFD depicting data flows and activities described in Chapter 1. Information resources, such as industry standards, published

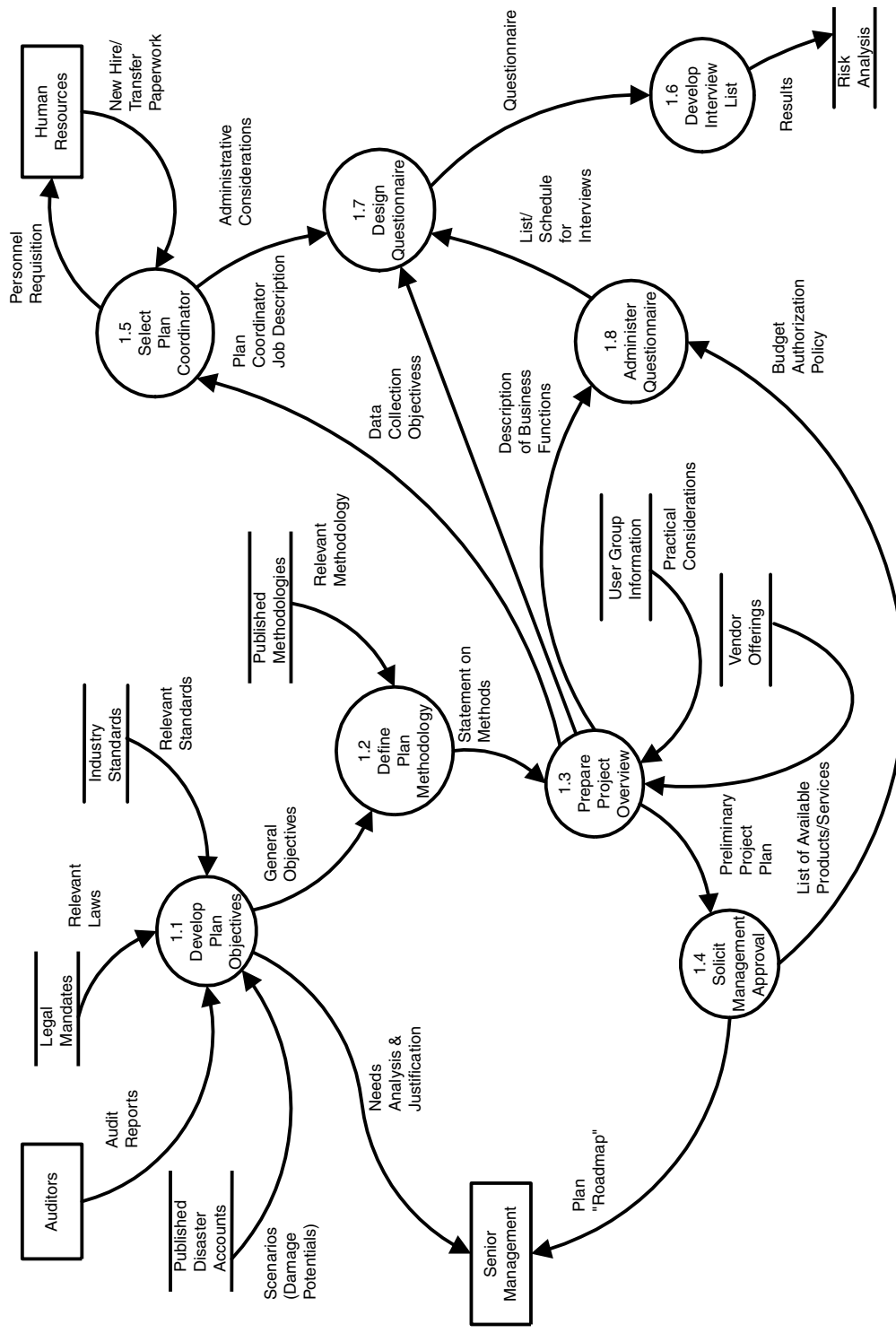


Figure 1-3 Initialization phase data flow diagram.

disaster accounts, and legal mandates, are used to develop a rationale for the plan development project for presentation to senior management. Data from these sources is used to define methods (consultant or in-house development) and to create project outlines. Other inputs and outputs are also presented to account for the numerous tasks involved in the initial start-up phase of disaster recovery planning.

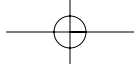
DFDs do not necessarily show precedence or chronological order of tasks. They are flexible, spatial constructs that the reader, it is hoped, will find easy to apply to his or her planning requirements. As such, DFDs are preferable to the linear and rigid structure of a flowchart depicting tasks and milestones in the plan development project.

Elsewhere in this book, the reader will encounter flowcharts that provide examples of master plans for various aspects of the recovery project. These flowcharts attempt to superimpose order and sequence on recovery events. Flowcharts are not intended as models to be rigorously followed, but as guides for creating and organizing one's own implementation plan. A concatenated flowchart is provided at www.drplanning.org, a web site that has been established to serve as a "living appendix" to this book.

It is hoped that this distinction in illustrations will help to clarify any confusion that may arise between the planning project and the implementation project that is its product.

ENDNOTES

1. D. O. Aasgaard et al., "An Evaluation of Data Processing 'Machine Room' Loss and Selected Recovery Strategies," MISRC Working Papers (Minneapolis, MN: University of Minnesota, 1978).
2. Thomas Hoffman, "Denial Stalls Disaster Recovery Plans," *Computerworld*, 2/23/98.
3. Philip Jan Rothstein, Rothstein Associates, Brookfield, CT, comments to the author, 07/99.
4. Gary H. Anthes, "Lotsa Talk, Little Walk," *Computerworld*, 9/21/98.
5. "6th Annual Information Security Survey," conducted in conjunction with *Computerworld*, Ernst & Young LLP, 1998.
6. Jaikumar Vijayan, "Client/Server Disaster Plans Fall Short," *Computerworld*, 11/03/97.
7. Bruce Caldwell, "Homestretch," *Information Week*, 7/19/99.
8. Eddy Goldberg, "DP Nightmare Hits N.Y. Bank," *Computerworld*, 12/02/85.
9. Ibid.
10. Dale Stackhouse and Kenneth T. Ungar, "The Foreign Corrupt Practices Act: Bribery, Corruption, Recordkeeping and More," *The Indiana Lawyer*, 4/21/93.
11. William Perry, "The Auditor, EDP, and the Federal Government," in *Data Processing Management* (New York: Auerbach Publishers, 1979).
12. Ibid.
13. Ibid.
14. Interview with Inspector Roy Williams, St. Petersburg, FL Fire Department, 9 January 1987.



15. Interviews with Maar Haack, EDP Underwriter, The St. Paul Insurance Companies, and Tom Cornwell, CHUBB Insurance Company, December 5–6, 1987.
16. Ibid.
17. Jon Toigo, "Alternatives for Disaster Recovery Plan Development," *Data Security Management* (New York: Auerbach Publishers, 1988).
18. Rothstein, op. cit.
19. Data flow diagram (DFD) standards taken from Tom DeMarco, *Structured Analysis and System Specification* (New York: Yourdon, 1979).

