DOCUMENT RESUME

ED 469 331 HE 035 291

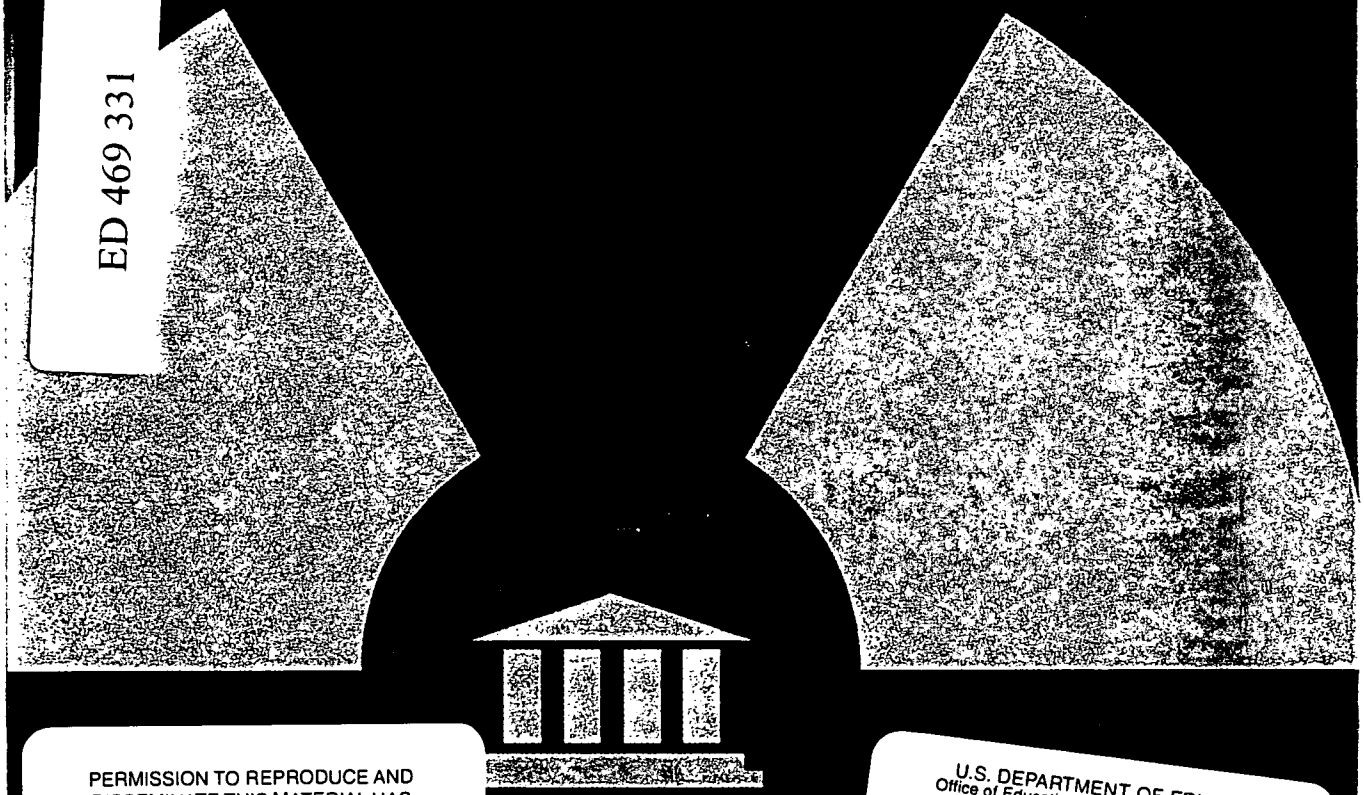
AUTHOR	Qayoumi, Mohammad H.
TITLE	Mission Continuity Planning: Strategically Assessing and Planning for Threats to Operations.
INSTITUTION	National Association of Coll. and Univ. Business Officers, Washington, DC.
ISBN	ISBN-1-56972-022-3
PUB DATE	2002-00-00
NOTE	69p.
AVAILABLE FROM	National Association of College and University Business Officials, P.O. Box 362, Annapolis Junction, MD 20701-0362 ($30, members; $45, nonmembers). Tel: 866-348-6300 (Toll Free); Web site: http://www.nacubo.org.
PUB TYPE	Books (010) -- Guides - Non-Classroom (055)
EDRS PRICE	EDRS Price MF01/PC03 Plus Postage.
DESCRIPTORS	*College Administration; *Educational Facilities Planning; Higher Education; Natural Disasters; *Reliability; Risk; *Risk Management
IDENTIFIERS	*Continuity; *Emergency Preparedness

ABSTRACT

This book covers the principles of risk and risk management and offers a framework for analyzing the significant, often unforeseen threats facing higher education institutions today. It examines the critical elements of a disaster preparedness plan and addresses business continuity and mission continuity planning. The book also provides tools for calculating system reliability and examines facilities-related risks. The book guides institutions in putting plans in place to minimize or eliminate service interruption to the processes that are critical to the organization. The chapters are: (1) "Risk Management"; (2) "Disaster Preparedness"; (3) "Business Continuity Planning"; (4) "Calculating System Reliability"; and (5) "Addressing Facilities-Related Risks." (Contains 26 references.) (SLD)

Mission Continuity Planning

Strategically Assessing and Planning for Threats to Operations



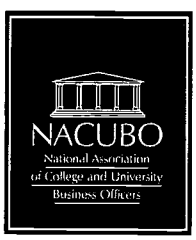
By Mohammad H. Qayoumi

NACUBO
National Association of College and University Business Officers

Mission Continuity Planning

Strategically Assessing and Planning for Threats to Operations

By Mohammad H. Qayoumi



National Association of College and University Business Officers
Washington, DC
www.nacubo.org

Printed in the United States of America

ISBN 1-56972-022-3

TABLE OF CONTENTS

acknowledgments

I want to express gratitude to the reviewers of this book, both for affirming and for challenging my work. This book was considerably strengthened by the comments of Janice Abraham of United Educators, John Dvorak of Massachusetts Institute of Technology, Deborah Fisher of Massachusetts Institute of Technology, Jamie Lewis Keith of Massachusetts Institute of Technology, Sandra Lier of University of Washington, and John "Barry" Walsh of Indiana University.

I am grateful to Michael Carbine, the extraordinary editor with whom I worked, and to Donna Klinger of NACUBO for editorial direction. I also would like to thank my wife, Najia, for her tremendous support as I worked on this book over the holiday season.

Mohammad Qayoumi
California State University, Northridge
June 2002

INTRODUCTION

I recently heard an insurance commercial on the radio proclaiming that "If there were no risk, we could do anything." Moreover, if we lived in a deterministic universe, we need not worry about risk. But given the world we live in, risk is an important factor that comes into play in all but the most trivial decisions. All organizations in our society, including colleges and universities, must take risk into consideration and develop effective strategies for assuring the continuity of their operations so they can achieve the goals in their mission statements. The complexity of today's enterprises necessitates addressing business continuity as a systematic discipline.

Traditionally, business recovery plans dealt primarily with backup and recovery of individual systems in a disjointed fashion. The sole focus was identifying best available technologies as redundant in the most cost-effective manner. For most institutions, business continuity planning was limited to operational issues by individual work units that dealt solely with disaster planning. Today, business continuity is viewed as a strategic issue involving all aspect of the enterprise. In other words, business continuity planning must be addressed as a core competency rather than an isolated and disjointed exercise by individual operational units. Universities have expanded this concept under the title of "mission continuity planning." Mission continuity planning (MCP) is a delicate balance between science and art. It is a science because it requires a systematic discipline, and it is an art because it requires innovation, critical thinking, and creativity. Above all, the mission continuity plan must be tailored to the specific needs and circumstances of the institution.

In today's complex and uncertain operating environment, all organizations are paying attention to the increasing costs generated by downtime and service interruptions. At the same time, the number and severity of potential threats that could cause service disruption have been growing exponentially. Consequently, senior college and university managers have also begun paying close attention to mission continuity planning. Clearly, mission continuity planning is a process that must be embraced and driven from the top down by college and university leaders. Doing this will ensure that the proper level of attention and resources are assigned to this activity so that an effective plan can be created and implemented. The terrorist attacks of

September 11th and subsequent acts of domestic terrorism demonstrated the necessity of having mission continuity plans in place, and were a reason for writing this book.

The intent of this book is to provide college and university administrators with an overview of the basic concepts of mission continuity planning so they will have a better appreciation of their role in developing such plans. The first chapter discusses the concept of risk and its associated principles, and identifies the strategic, financial, legal, and operational risks to which colleges and universities are exposed, including specific activities that can create potential vulnerabilities. Risks are classified, analyzed, and evaluated, and the importance of risk management is discussed. This chapter creates an overall framework by examining the significant threats facing today's colleges and universities.

Chapter 2 addresses the importance of disaster preparedness and the critical elements in a disaster preparedness plan. Different types of disasters, including floods, hurricanes, tornados, earthquakes, tsunamis, fires, and acts of terrorism, are examined. In addition, threats posed by chemical, biological, and radiological agents are identified and the impact of the U.S. Patriot Act of 2001 is discussed. The balance of the chapter addresses the key steps in creating a disaster preparedness strategy, including the development of an emergency response plan, the kinds of units that should be included in developing such a plan, and the role and function of an emergency operation center. The chapter focuses primarily on the operational issues associated with disaster preparedness planning.

Chapter 3 addresses business continuity planning and the critical role that information technologies, including Enterprise Resources Planning (ERP), play in today's organizations and the potential threats facing these systems. The chapter examines the risk of cyber attacks by both hackers and crackers, attacks that can create havoc in college and university operations. The chapter also discusses the important differences between business continuity plans and business interruption insurance, as well as the role of rapid recovery systems. The major aspects of mission continuity planning are identified and addressed.

Chapter 4 constitutes a departure from the first three chapters by addressing the concept of reliability in a quantitative manner. Key reliability metrics – such as mean time between failures (MTBF), mean time to detect (MTTD), mean time to repair (MTTR), and availability – are defined. In addition, several techniques that can be used to analyze reliability and system availability are also discussed. This intent of this chapter is to help the reader grasp the importance and utility of these mathematically complex concepts, and clarify the systemic issues caused by the failure of individual equipment in a network.

The fifth and final chapter addresses facilities-related risks faced by today's college or university. It begins by discussing the importance of electrical power distribution systems, potential risks related to power outages, and steps that can be taken to minimize the frequency and impact of power outages. The basic reliability requirements of power systems in a digital economy versus the capability of existing electrical systems are discussed. The chapter then covers

water distribution systems and flood issues, and potential threats to building heating, ventilation, and air conditioning systems. This issue has grown in importance since the September 11th terrorist attacks and subsequent domestic anthrax incidents; the air intake systems of many buildings are vulnerable to the malicious releases of life-threatening chemical or biological agents. The last chapter also discusses managing hazardous materials in facilities, for which the U.S. Patriot Act of 2001 has imposed new requirements.

A list of references will help readers find additional and more detailed information on the various topics addressed in the book.

CHAPTER ONE
RISK MANAGEMENT

OVERVIEW

Colleges and universities today are complex enterprises that serve a large number of diverse stakeholders. They are a place of congregation for thousands of faculty, students, and professional staff in the pursuit of learning and acquiring new knowledge. Running a university entails addressing a complex web of multiple interdependent processes. Although the level of interdependence among these processes may vary widely, they all contribute to the attainment of the organization's mission. In other words, the failure of one or more of these processes can impede the institution's ability to meet all of its goals and objectives. This leads to the concept of risk, which can be viewed as any event that would negatively impact an organization's ability to meet its stated objective.

There are many potential risk factors that any enterprise, including colleges and universities, face on a one-time and/or ongoing basis. These include (a) threats from natural disasters — such as earthquakes, floods, hurricanes, tsunamis; (b) system malfunctions — such as fire, power interruptions, equipment failures; (c) malicious acts — such as sabotage, computer hacking, fraud, terrorism; and (d) human error — such as operator's carelessness, and lack of adequate knowledge. In addition, threats from various kinds of cyber attacks are becoming a part of risk analysis. Among these are threats from 'crackers' (malicious hackers); non-functioning ERP systems (such systems now run most business processes); and the growing threat from the unauthorized disclosures of sensitive information about students, faculty, and staff. The negative consequences of these factors can be gradual or immediate.

While several steps must be taken to minimize the risk exposure that organizations face in this area, the first and most important is developing a better understanding of the nature of these risks. Although the operations of individual colleges and universities vary, common management principles run across all of these institutions and can be drawn upon to provide a better understanding of the fundamental concepts of risk and risk management.

Risk is defined as the possibility of an adverse result that may occur in the future. Two important concepts associated with risk are: (a) the probability of a negative occurrence, and (b) the adverse impact that may result as the consequence of the event. However, the contem-

porary definition of enterprise risk management has expanded beyond adverse events to include the idea that the proper management of risks can help achieve organizational objectives, and that thoughtful risk taking can be a beneficial activity. Sometimes the probability of the negative occurrence can be easily determined but in most cases, the probability may not be known. In such cases, there is an uncertainty in the level of risk. Risk per-se is not a problem. But the concern associated with risk is the potential for an impact that could be minor or catastrophic.

As mentioned, risks are an ongoing part of life, and since every college or university eventually will confront risk, the role of management is to find ways to manage it. In this context, the potential for risk should be viewed as an opportunity to improve overall system performance. Managers who ignore risk face the probability that a serious incident will occur at some point in the future, and that the incident will negatively impact the organization, and most probably at an inopportune time.

DEFINING RISK AND UNCERTAINTY

In developing a risk assessment model, it is important to know how risk is related to the ability of an enterprise to meet its overall objectives. Therefore, seeking input from senior leadership about their priorities, interests, and concerns is essential in framing the risk assessment. The ranking methodology should be sufficiently comprehensive to apply the risk factors uniformly across various units and subdivisions. To the extent possible, it is important to develop quantitative models that incorporate risk, weighting methodology, and impact factors for a scoring criteria. This will enable you to develop a continuum running from low to high. Because it may be difficult to use a strict quantitative model for many situations, a three-tiered model can be used to group risk factors into low, medium, or high.

Various methods can be found in the literature for assessing risk. One approach suggests a five-step model, namely goal determination, risk identification, risk analysis, control deployment, and ongoing monitoring. These activities are briefly discussed below. Start by reviewing the organization's goals, priorities, and objectives. Based on this review, identify potential exogenous and endogenous elements that pose risks to the organization. Once the risks are identified, analyze the impacts of these risk factors if they are not managed. Then develop a systematic approach to address the risk factors. Finally, audit and monitor the effectiveness of the risk assessment process and establish a schedule to repeat the review.

A different way to define risk is to view it as the combined effects of three factors: threats, vulnerabilities, and impact. Here, threat is defined as probable events that may be caused due to an inherent system weakness. Vulnerability is defined as a system weakness that may be exploited by the threat. Impact is defined as the adverse result as a consequence of the threat. This can be mathematically displayed as the simple multiplication of these three factors:

Risk = Threats X Vulnerabilities X Impacts

By using this simple formula, you can quantify risk by assigning a probability to the three factors. For instance, one approach is to assign a percentage scale to each of the three factors, namely values between zero and 100. This way, the minimum value will be zero and the maximum value for risk will be 1,000,000. For many applications, this level of precision is overkill. A different way to quantify risk into several bands is to divide the above three factors into levels. This way, a low value is assigned a score of 1; a medium value gets a score of 3; and a high level is assigned a score of 9. In this approach, the minimum score is one and the maximum score is 9x9x9 = 729. The model could possibly be simplified further by giving only two values to the above three factors, where one will represent low and two will represent high. This way, the risk level can be divided into four levels, namely 1, 2, 4, and 8, where 1 represents the lowest and 8 represents the highest risk level.

TYPES OF RISK

Institutions must engage in a process to assess their tolerance for risk, and to assess, under broad categories, the range of risks they face. These risks must then be prioritized by impact, importance, and ease of mitigation or avoidance. Key stakeholders who must be involved in this process include trustees, senior leadership, faculty, students, staff, alumni, local community, and federal and state regulators. The kinds of risks that an enterprise face can be numerous. Moreover, it should be noted that a single activity might pose a threat to several institutional interests (e.g. financial, operational, strategic, etc.). When multiple interests are threatened, the risk is often greater, although a significant risk to a single important interest can be equally significant.

In order to better understand the nature of these risks, the first step in the analysis entails breaking the risks into four major categories: strategic, financial, legal, and operational.

Strategic Risk

This encompasses primarily long-term threats that may impact the institution's ability to meet its goals and objectives. Major activities that can lead to strategic risk include:

- failure to take advantages of possibilities;
- demographic changes in the institutional service area;
- long-term enrollment trends;
- competition from other institutions for the same students, research grants, and development dollars;
- institutional image and reputation;
- changes in delivery of teaching and impact of technology;
- the rise of for-profit universities delivering space independent asynchronous learning opportunities that better meet the needs of nontraditional students;
- keeping up with changing technologies;
- unionization of graduate assistants and its impact on research grants and teaching;

- long-term funding prospects from all sources, such as federal and state allocations, support from businesses, foundations, and alumni;
- governance issues; and
- alignment of physical capacity with operational needs.

Financial Risk

Any threat involving the potential loss of tangible assets is a financial risk. The major subcategories of activities that can result in financial risk are:

- market and interest rate risk;
- integrity of financial information;
- accuracy and efficacy of financial information;
- control mechanisms for major business processes;
- inventory systems for capital equipment;
- separation of duties in basic financial processes;
- major financial processes, such as accounts receivable, accounts payable, and cash flow;
- investment and endowment management;
- procurement function and use of procurement card, e-commerce, and other strategies;
- cashiering and other forms of cash transactions, including petty cash;
- managing payroll and check disbursement;
- fraud and misappropriation of financial resources; and
- unrelated business income tax.

Legal Risk

Legal risk is related to compliance with federal laws and regulations as well as with local ordinances. Over the past few decades, a stream of new rules and regulations has continually increased the compliance burden on universities. As a result of these developments, the compliance risk has risen sharply. Some of the major regulations include education codes, employment laws, environmental rules, and IRS rules, to name a few. The risk factors include:

- knowledge of all relevant regulations;
- training and awareness of staff;
- developing plans to audit individual units for compliance;
- developing and implementing a code of conduct for the organization; and
- establishing control mechanisms to ensure compliance.

Operational Risk

Operational risk is often defined as the risk of error or fraud within manual or systems environments. It consists of threats to major functions, such as academic programs, human resources,

sponsored research, facilities management, environmental health and safety, admission and records, information management, athletics, and auxiliary enterprises. These functions are diverse, and each contains its own risk factors. They include:

1. Academic programs

- Faculty review, tenure, and promotion
- Monitoring and control of curriculum
- Academic freedom and free speech issues
- Grading policies and reviews
- Student/faculty ratio and class size
- Relating academic policies

2. Human Resources

- Faculty and staff hiring practices
- Employee relations issues, including discipline and grievance
- Employee performance evaluation
- Hostile work environment, including sexual harassment
- Staff classification matters
- Payroll, leaves of absence, and benefit management
- Employment eligibility and immigration issues
- Workers' compensation

3. Sponsored Research

- Determination of indirect cost and allocation methodology
- Intellectual property issues, including patents, licensing, and commercialization
- Compliance issues relating to GAO and OMB requirements
- Research involving human subjects
- Research on animals and related compliance factors
- Delivering grant outcomes to sponsoring agency
- Reporting research efforts
- Project accounting

4. Facilities Management

- Maintenance of buildings and grounds
- Service interruptions of major utilities, such as electric, heating, cooling, water, and sewers
- Building security
- Facilities accessibility and mandated ADA requirements
- Capital program issues, such as planning, design, and construction
- Real estate issues

5. Environmental Health and Safety

- Workers' safety

- Hazardous materials management
- Radioactive materials management
- Biological agents
- Chain of custody issues
- Awareness training and documentation
- Buildings and grounds safety
- Disaster preparedness and emergency management

6. Admissions and Record

- Enrollment management
- Recruitment plan and tuition discounting
- Financial aid strategy and managing yield
- Admission standards
- Student transfer and articulation agreements
- Confidentiality of student records
- Competition from other campuses for the same applicants

7. Information Management

- Accuracy, accessibility, and confidentiality
- Data integrity and security
- Hardware reliability and obsolescence
- Software licensing
- Communication infrastructure reliability and capacity
- System connectivity and compatibility concerns
- Disaster recovery and business continuity
- Backup and recovery
- Physical security and environmental control
- Control of Web pages and their content
- Equipment maintenance

8. Athletics

- Compliance with NCAA rules
- Facilities concerns
- Recruitment practices
- Community support
- Retention and graduation rate of athletes
- Budget management, revenue collection, and cash handling
- Institutional image

9. Auxiliary Enterprises

- Campus parking and transportation services
- Residence hall and other campus housing

- Child day care service
- Commercial operations
- Food services
- TV and radio stations

10. Other Operation Activities

- Student life activities
- International transactions
- Joint research activities
- Foreign nationals or institutions
- Mixed use funding (e.g. gift, research, endowment)

In addition, another risk category that is very important for academic institutions is reputational risk. An institution's reputation is the asset that generates private funding, attracts quality students, and recruits and retains capable faculty.

RISK CLASSIFICATION

An organization's ability to withstand the negative impact of a risk represents its tolerance. The degree of tolerance may vary widely based on a particular risk. In addition, the tolerance to the same risk factor may vary significantly depending on other conditions. For instance, if the application server for the student registration system fails three days before the beginning of the fall semester, the negative impact is more severe than had it failed sometime in the middle of the semester. Thus, the tolerance factor is one way to measure the criticality of different risks. For critical applications, even short interruptions can have a sizable impact. For instance, if a mainframe computer is subjected to an electrical interruption lasting only a moment or for several hours, the impact may be similar. Another important aspect for consideration is an organization's appetite for risk tolerance. Organizations often can tolerate more risk than they encounter. Sometimes, the inverse is true.

The tolerance continuum can be divided into four functional categories: (1) critical, (2) vital, (3) sensitive, and (4) non-critical.

Critical functions are those where the consequences of failures are most significant. Moreover, it is not easy to develop simple alternative solutions for these functions. In an emergency, the organization must have access to backup equipment or have redundant onsite equipment. An example of a critical function is the central cooling system of an Internet server during the summer months.

Vital functions are similar to critical functions in one aspect: it's difficult to create alternative solutions for these functions should they fail. However, a failure will not have a significant impact if the system is restored within a time period that allows the system to catch up quickly and return to normal operations. An example of a vital function is running a batch process in a computer system. If the computer system fails for up to several hours, the system may be able to catch up without any significant impact.

A sensitive function is one for which alternative solutions can be created, but for which a cost will be incurred during the time it takes for normal service to be restored and the system to catch up. An example of a sensitive function is an automated procurement system. If there is a system failure for a significant period of time, a manual process can be developed and used, although it may be costly and cumbersome. When the system is available again, it may take significant time to catch up and bring everything back to normal.

Finally a non-critical function is one where any major service interruption will not have major negative consequences. Moreover, once service is restored, there will be no need for major catch-up.

RISK ANALYSIS AND EVALUATION

Every activity in an enterprise can generate a positive impact and a potentially negative impact. The positive impact is seen as the opportunity while the negative impact is the risk. Every risk assessment must examine the activities that result in a negative impact and then determine the probability of an occurrence for each identified event. It is important to recognize that the risk assessment is not an end by itself. Rather, it is a method an organization uses to develop related controls that, in turn, will help the organization achieve it business goals. Therefore, the risk mitigation steps should focus on specific business needs. A senior security officer of an electric utility put it this way when he described the information technology risks faced by his firm: "We are not in the business of protecting information. We only protect information insofar as it supports the business needs and requirements of our company" (Toigo, 2000).

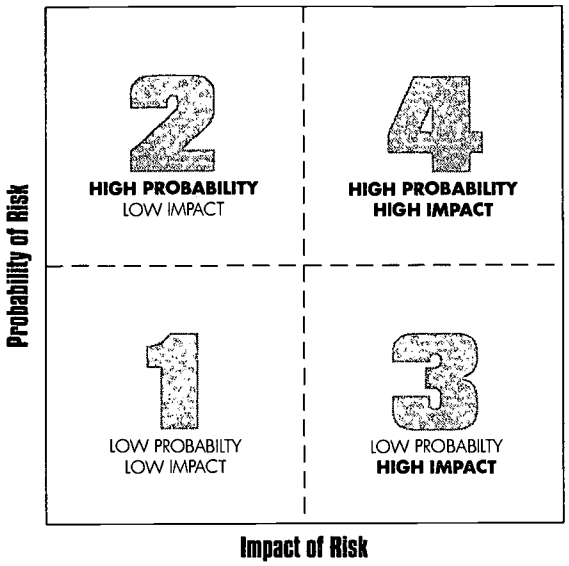
Risk assessments can use a quantitative or qualitative approach. Although many may prefer an approach that attempts to quantify risk, the lack of such analysis does not diminish the value of performing a qualitative assessment. At a minimum, the assessment will provide an opportunity for gaining insights that could be valuable in managing various risk factors.

Risk evaluation and management is not an event. Rather, it is a continuous four-step process involving (1) planning, (2) assessment, (3) action deployment, and (4) monitoring and reporting.

The first step entails establishing objectives linked to the organization's goals.

The second step identifies and quantifies the risk. This involves prioritizing all risk factors and calculating the probability associated with all risks as well as their consequences for everyone in the organization. One way to present risk and its associated impact is shown in the matrix in Figure 1, where the probability of risk is shown on the "Y" axis and the impact of risk is shown on the "X" axis. The risk factors can be divided into four groups: (1) low probability and low impact, (2) high probability with low impact, (3) low probability with high impact, and (4) high probability and high impact. Clearly, risk factors with high probability and high impact must be dealt with first, while factors with low probability and low impact would be addressed last. The strength of this technique results from the fact that you can visually evaluate all risk fac-

FIGURE 1



tors in a rapid manner and group them into low, moderate, and high-risk elements before deciding which should be addressed first.

The third step in the process is addressing the identified risks. There are four basic ways to handle risk: (1) risk assumption, (2) risk control, (3) risk mitigation, or (4) risk avoidance. Risk assumption is appropriate in situations where the probability of the risk and/or its impact is low. In addition, there may not be an economical way to mitigate the risk. In this case, the detrimental consequence of the risk is consciously assumed as a "cost of doing business." Risk control entails taking certain actions to lower the probability of occurrence and/or the impact of the risk. This could be accomplished by a variety of actions, including improving the process to reduce risk, adding redundant paths, incorporating inspection, and installing a monitoring system for early warning purposes.

Risk mitigation involves transforming the process to become more robust and, consequently, to eliminate the probability of a particular risk. This may be accomplished by moving to a different technology and/or redesigning the process. Finally, risk avoidance implies that given the high probability of an occurrence or the negative impact of a particular risk, the process is abandoned. This scenario is appropriate if it makes business sense to forego a particular capability in view of the potential impact. Naturally, risk avoidance is practical only if a process is not deemed to be mission-critical and where the risk exposure associated with the process is unacceptable.

In many situations, none of the above mitigating techniques may be an option for an organization. In these cases, transferring risk to an outside entity at a particular cost is an option. In other words, organizations attempt to protect themselves from risks by purchasing insurance from a third party. This means an enterprise limits its losses to a predetermined level and the insurance carrier assumes the risk.

The fourth and final step in the risk evaluation and management process is monitoring and reporting, which deals with evaluating the effectiveness of the first three steps that have been undertaken as part of the process and making any necessary changes. This involves collecting data on basic metrics, examining risk awareness within the organization, and providing input on how to enhance operations.

A cost-benefit analysis must also be performed in order to determine which risk-management options are viable. An analysis must be undertaken to determine whether the institution is in the business of managing the particular risk or should contract with the necessary expert to assume the risk. It also is necessary to assess the probability of risk that is assumed, its likely impact, and the cost of the negative impact. Afterwards, seek ways that the risk could be minimized or successfully avoided.

ENSURING THE SUCCESS OF YOUR RISK MANAGEMENT PROGRAM

The success of any risk management program will depend heavily upon senior leadership's demonstrated support of and commitment to the program. But other steps must be taken as well to ensure that the program succeeds in achieving its goals. These include:

- fostering a successful risk management culture by integrating risk management policies and procedures into the organization's goals and value system,
- communicating the acceptable level of risk limits to all employees and actively finding ways to involve all key stakeholders in the discussion,
- including risk management as an important part of all employee management activities for every manager who is responsible for mission-critical functions,
- incorporating risk management in employee performance evaluations and creating a reward and recognition system that reinforces desired risk management behavior, and
- creating a cross-functional multidisciplinary team to manage risks in key areas. These areas include financial services, construction management, human resources, insurance, environmental health and safety, etc. Such teams may conduct self-assessment, monitor compliance, increase awareness, and provide input to senior leadership.

REASONS FOR IMPLEMENTING RISK MANAGEMENT

Managing risk does not necessarily mean avoiding actions that create risk. Rather, it requires developing discipline to systematically identify and evaluate risk for the purpose of minimizing the institution's exposure to risk and and/or the potential impact of risk. Managing risk often requires that a mix of experts at an institution be involved in the process, and that a variety of institutional offices have controls in place to manage risk. These include offices with functional-area responsibilities such as environmental health and safety, sponsored programs, design and

construction, human resources, financial services, and information services, as well as those with systemwide responsibility for managing enterprisewide risk, such as legal, internal auditing, compliance, and insurance.

An effective risk management strategy will benefit an institution in many ways. But most importantly, it will help the institution:

- achieve its mission,
- focus on organizational priorities and aligning the use of resources for the institution's primary mission,
- place more emphasis on preventing rather than reacting to events,
- promote a more open environment where managers can discuss potential exposures to risks,
- provide an environment where mistakes are used as learning opportunities rather than a reason for punishment,
- create a stronger emphasis on planning to identify new opportunities,
- foster a culture of accountability where all employees take responsibility for managing risk in their respective operational domains,
- enhance stakeholders' confidence in the organization's ability, and
- empower all employees to seek innovative solutions to address potential risks.

Managing risk is an ongoing journey rather than a destination. This means as we addresses current risk factors, new risks will eventually arise that require attention. Therefore, this is not a task that can be handled on a one time or ad hoc basis. Constant vigilance is the only sure way to effectively manage risk. The success of a risk management strategy depends on the demonstrated support of and commitment from senior leadership. The following chapters in the book address various aspects of risk management in more detail.

CHAPTER TWO

DISASTER PREPAREDNESS

It is a mistake to think of risk analysis as a complex and mysterious process that is difficult to master. In fact, anyone with a basic understanding of statistics who can think systemically possesses the basic skills to perform a risk analysis. Learning a formalized methodology can facilitate the assessment and make the process very efficient.

A strong indicator of an organization's strength is its ability to successfully respond to unforeseen circumstances. Indeed, disasters and other emergencies test the agility of organizations under conditions in which the loss of human life and property may be eminent. Such incidents significantly tax an institution and increase its fragility. Disasters inflict serious damage on almost all enterprises, and in a significant number of cases, they seriously threaten the viability of these enterprises. For instance, research from Gartner suggests that roughly 40 percent of businesses experiencing a disaster go out of business within five years. For universities, the aftermath of a disaster can ripple across the institution: enrollment will drop sharply; gifts, grants, and research activity will slow down; and the institution's overall financial health will suffer. The projected worldwide losses attributed to unplanned downtime were more than $1.6 trillion in the year 2000. As a result, preparing an institution to deal with potential and likely disasters is an important component in ensuring the sustainability of an institution over the long term.

While no level of preparedness can totally eliminate the risk for all possible eventualities, any degree of preparedness will decrease the devastating potential of natural or human-made disasters. Executives must not only be familiar with the opportunities afforded by new preparedness technologies, but also have a better understanding of the new set of risks and vulnerabilities that their organizations are confronted with. Lack of adequate preparation can seriously endanger an organization's ability to survive potential threats over time. If the probability of the occurrence of any pending accident or disaster is more than zero, the accident or disaster will occur given enough time.

TYPES OF DISASTERS

Disasters can be divided into two main types. The first encompasses disasters that happen suddenly and without notice, such as earthquakes, fires, or acts of terrorism. In such cases, recov-

ery teams begin their search and rescue efforts and take necessary steps to contain the damage. The second type includes phased disasters, such as floods, hurricanes, typhoons, tornados, and tsunamis, where there can be an early warning of eminent danger. In such cases, an emergency can be declared before the incident occurs so people can take advantage of available time to prepare for the potential disaster in advance of its occurrence. A vulnerability assessment should be completed before determining the appropriate plan of action.

Since weather-related emergencies typically can be predicted several days in advance, an effective use of this time in preparing for the emergency can significantly minimize the loss of human life and physical damage. To this end, following local weather reports becomes an important risk management activity. This information can be obtained from radio and television weather channels, the National Oceanic and Atmospheric Agency (NOAA) Web site (http://www.noaa.gov), and many other weather-related Web sites.

The following section identifies eight kinds of disasters that can affect an institution and appropriate responses that can help minimize their impact: (1) floods, (2) hurricanes, (3) tornadoes, (4) earthquakes, (5) tsunamis, (6) fires, (7) bomb threats, and (8) acts of terror.

Floods

The campus facilities office should research local flood plains and water levels reached during previous floods and make this information part of the record. The information should be included in the emergency response manual used by all members of the campus' emergency response team. If facilities are located below a flood plain, consider developing a plan for protecting building occupants, closing down operations in an orderly fashion, and isolating and shutting off utilities in case of an emergency. It is important to emphasize that no person should enter a flooded area in a vehicle. Water may penetrate the engine and electrical system and immobilize the car, trapping its occupants and raising the possibility that they may drown. Water currents in a flood are usually far stronger than they appear. While it may be tempting for individuals to try crossing a flooded area by foot, currents as small as a foot in depth can be strong enough to overcome any who try.

A response plan should include evacuation procedures and identification of safe routes that can be used to leave (and avoid) potential flood zones. Consider stocking a supply of sandbags where they can be easily seen, and/or making prior arrangements for adequate numbers of sandbags to be delivered on demand. Record the locations of utility shut-off valves and switches, and develop procedures for shutting them off safely prior to an emergency. Develop procedures for removing and/or protecting sensitive and expensive equipment, supplies, records, chemicals, and other items to higher ground before a flood. Follow weather reports and projected flood levels, and implement your plan well before the event occurs. Carefully crafted response plans will help an organization respond to an emergency in a systematic manner.

Hurricanes and Tropical Cyclones

Hurricanes or tropical cyclones are severe storms that impact the Atlantic coast, Gulf coast, Pacific coast, Hawaii, and Caribbean. These storms are associated with sustained winds of above 74 miles per hour, although they can reach as high as 160 miles per hour. In other parts of the world, hurricanes are called typhoons. The hurricane season starts in the beginning of June and continues through the end of November. Hurricanes can bring 6 to 12 inches of torrential rain and generate ocean waves of up to 25 feet high. They can also spawn tornados, which is discussed later in this section. In many cases, severe rainfall may precede the hurricane and continue long after the hurricane itself dissipates.

Hurricanes can be extremely destructive. Strong winds impose a sizable force on structures as they try to drag or uplift them; this weakens units and can destroy their contents. Trees are uprooted and rapid flooding occurs due to quick storm surges. Heavy waves can batter shorelines, propel loose objects, and destroy structures in their path. Hurricanes generate numerous secondary effects that can be damaging as well, such as tornados, power outages, water supply contamination, and the flooding of sewage treatment facilities.

Hurricanes are classified into five categories based on wind speed using the Saffir-Simpson scale as shown below:

Hurricane Categories	Wind Speeds in Miles per Hour
Category One	74 – 95 mph
Category Two	96 – 110 mph
Category Three	111 – 130 mph
Category Four	131 – 155 mph
Category Five	Over 156 mph

These classifications help emergency response planners estimate the potential destructive force of a particular hurricane and take appropriate action. The National Weather Service (NWS) tracks hurricane formations as they develop in the ocean, monitoring the strength, rate of gaining strength, and direction of motion. The NWS also calculates the geographical areas that may be affected by the hurricane. Because they are slow moving storms, hurricanes can be tracked and their approximate landfall location and potential for damage can be known several days in advance. Therefore, the evacuation of all but essential emergency staff can begin days ahead of landfall.

The response to a hurricane is divided into three phases. The first is the awareness phase starting 60 to 72 hours before landfall, when wind forces may reach 30 to 60 mph. The second phase, called the standby phase, begins 48 to 60 hours before landfall, during which time a "tropical storm" will be underway. The third and final phase, called the response phase, starts

48 hours before landfall. By this time, the NWS will have issued hurricane watches and warnings. A hurricane watch means that a hurricane is possible within the 24 to 36 hours; a warning means that a hurricane will hit the shoreline within the next 24 hours.

In preparing an effective hurricane response, examine data from prior incidences and their impact on the campus. Procedures must be in place for evacuating the facilities well in advance of the incident. Needless to say, the longer an evacuation is delayed, the more difficult it will be to successfully move people to safe areas given resulting traffic volume and impact of deteriorating weather conditions on traffic flow. Identify essential staff who must remain on campus during the emergency to complete protective tasks. Check all related emergency equipment such as standby generators and fuel for operating the units; emergency portable lighting; portable sump pumps; battery packs; and the like. Finally, secure all doors and windows and brace them with sheets of plywood.

Tornados

Tornados are fierce and strong whirling winds usually associated with a strong thunderstorm. They consist of a funnel-shaped cloud that moves at speeds of 10 to 50 mph. Tornados can be very destructive because their wind speeds range from 100 to 500 mph, although only 2 percent of tornados reach wind speeds of more than 300 mph. Tornados normally cover a width of 900 to 1,500 feet and may travel up to 50 miles across. Tornado season in the continental U.S. runs from March to August, with the largest number of incidents occurring between April and June. Tornados occur in roughly half of the continental U.S., with most occurring in the Midwestern and Southeastern states.

Regions at high risk for tornados normally have a cadre of trained spotters who can inform the community quickly of potential danger. By collecting information from various spotters, the NWS decides whether to declare an area under tornado watch or upgrade the watch to a tornado warning. As soon as conditions are favorable for the formation of a tornado, the NWS declares a tornado watch; the watch is upgraded to a tornado warning once a funnel is spotted. Tornado preparedness should include identifying shelters where people can take refuge. Only areas that can withstand the forces exerted by a tornado, preferably those located on a subterranean level, should be declared as shelters. Adequate staff must be available to shut off utilities to buildings damaged by tornados.

Search and rescue procedures should be a priority after a tornado has passed and the area is declared safe by the weather service. This information usually is communicated through local and campus law enforcement agencies as well as area radio and television stations. Buildings that are damaged by a tornado should be searched to make sure no one is trapped or injured. Emergency staff should evaluate the structural safety of the affected buildings. When buildings are deemed safe, access can be opened to others. If the structure is found to be unsafe, arrangements for its repair or demolition should be made. Large amount of debris and rubble

can be dispersed over a wide area during a tornado, so a sizeable clean-up effort may be necessary. Finally, remember that timely dissemination of information to everyone who could be affected is critical in order to minimize injury and prevent the loss of life.

Earthquakes

Unlike many other natural disasters, earthquakes happen abruptly. The sudden ground movements during an earthquake release tremendous amounts of energy that result in significant damage to buildings, dams, bridges, highways, and other structures. Moreover, the abrupt ground movements can liquefy land that is otherwise solid, causing major structural failures. If an earthquake happens during the rainy season, the potential for structural damage is much worse. Other damage caused by earthquakes include landslides, rock falls, ground ruptures and tsunamis (if the earthquake occurs under an ocean). Earthquakes also trigger numerous secondary events such as fires, floods, utility outages, dam failures, and the release of hazardous materials.

Many areas in the United States are vulnerable to earthquakes, although they are typically associated primarily with California and other western states. In fact, 39 states have varying degrees of seismic hazard. The severity of earthquakes is measured using the Richter scale, which employs a logarithmic scale ranging from 1 to 9. This means the difference in strength between any two subsequent levels is an order of magnitude. For example, 6 on the Richter scale is 10-times stronger that 5. Generally speaking, if an earthquake measures less than 3 on the Richter scale, it is barely felt. When an earthquake's magnitude registers above 4, the probability of damage increases. During the past 36 years, 16 major earthquakes ranging from 5.5 to 8.6 on the Richter scale have struck the United States.

Based on these statistics, it is not surprising that earthquake preparedness is a priority for most Californians, although the earthquake centered in upstate New York on April 20, 2002, measuring 5.1 on the Richter scale, demonstrated all too well that earthquakes are not limited to the West Coast.

MAJOR EARTHQUAKES IN RECENT YEARS

Locations	Year	Magnitude
Alaska	1964	8.6
Portland	1993	5.5
Seattle	2000	5.5
Northern California	1980	5.9
	1984	6.1
	1989	7.1
	1992	5.7
Southern California	1971	6.5
	1979	6.7
	1983	6.5
	1986	6.0
	1987	6.0
	1991	5.8
	1992	6.0
	1992	6.5
	1994	6.7

The first step in earthquake preparedness is surveying all buildings and making sure that gas cylinders, bookshelves, and other similar items that could fall are seismically braced and tightened to the wall, floor, or a building column. Whenever possible, install seismic shutoff valves for natural gas lines to reduce the likelihood of fires due to ruptured lines. The plan should identify where essential staff and volunteers are to report after an earthquake. It should list the locations of all main utility shutoff valves and switches that can be used to isolate sections of the campus or individual buildings. It must also list all facilities containing hazardous chemical, biological, or radioactive materials.

Qualified structural engineers should survey all buildings after an earthquake. Access to buildings should be limited to emergency staff until the engineers declare the buildings safe. The reason for this is that a major earthquake typically is followed by several aftershocks. While a building may look safe to the untrained eye, it may have been weakened to a point where it could collapse during an aftershock. Moreover, there is a good chance that some of the asbestos-containing materials in the building will have been disturbed after major tremors and consequently become friable. It is important to identify these buildings and take air samples. This will ensure that the asbestos fiber counts in these buildings are not above the safe threshold level before these buildings are reopened for occupancy.

Search and rescue procedures should be launched as soon as possible after a building has partially or totally collapsed. Rescue teams should also have access to data about hazardous materials in the building.

As mentioned, earthquakes usually occur suddenly and without warning. This increases the importance of effective earthquake preparedness training for the campus and its community. As part of the overall training initiative, periodic refresher training courses that include the enactment of possible scenarios should be conducted.

Tsunamis

Tsunamis (coastal tidal waves) are usually generated by undersea earthquakes, landslides, or meteorites or underwater volcanic eruptions that have taken place hundreds of miles from the coastline. They are more common along the Pacific than the Atlantic coast, and are especially likely to occur in the coastal areas of Alaska and the upper Northwest. When they occur, tsunamis can impact areas miles away from the shoreline. Areas that are less than 50 feet above sea level are more vulnerable. In a tsunami, winds in the open ocean can reach more than 400 mph, and tidal waves can be as high as 1,000 feet, cresting every 5 to 90 minutes.

In areas vulnerable to tsunamis, it is important to have a record of information about prior incidents and their impact on the area. This will serve as a guide in developing a response plan for future emergencies. The Tsunami Warning Centers in the Pacific region of the U.S. monitors potential signs of a threat and communicates warnings to the affected areas via local radio and television stations. Some of the warning signs of an impending tsunami include ground tremors

and rumblings, sudden changes in shoreline waters, and small waves that grow to significant heights when they hit the coastline. The evacuation plans for a tsunami are similar to these used for a flood. When a tsunami is forecasted, secure all equipment, shut off utilities, and evacuate people to higher ground away from the coastline.

Fires

Smoke inhalation rather than the fire itself causes many injuries and fatalities during a fire. A building's alarm system should be triggered the moment a fire is detected in order to evacuate everyone to safety. On most campuses, the fire alarm system is connected to the university police and/or the local fire department. It is important to quickly determine the area being affected, the extent of the fire (and smoke), and the equipment involved. Because time is of great importance in a fire, it is critical that systems are in place that enable fire-fighting crews to respond to the fire as quickly as possible. This underscores the importance of connecting the central fire alarm system to the campus police and local fire department. In addition, it is always good practice to ensure that fire-fighting equipment can easily reach all areas of the campus. This means ensuring that all access roads are sufficiently wide to permit access by fire-fighting equipment, and that no barriers are ever placed on these roads.

Fires can be divided into four categories:

Class A: Involving ordinary combustible materials such as wood, paper, and rubbish.

Class B: Involving flammable liquids that create a vapor-air mix. These include many oil-based substances such as gasoline, grease, paint thinners, paints, and mineral oils.

Class C: Occurring near operating electrical equipment. In fighting such fires, non-conducting extinguishing substances such as carbon dioxide must be used.

Class D: Involving combustible metals such as magnesium, sodium, and titanium.

Each campus must have a good working relationship with the local fire marshal. The local fire departments also should have a copy of the campus fire alarm system indicating the locations of the fire alarm systems as well as a document showing the location of all hazardous chemical, biological, and radiological substances.

Bomb Threats

While the campus police are the prime responders to bomb threats and will direct the institution's overall response, a bomb threat can be called in to any person or any office on campus. In such situations, it is important to remain calm and ask the caller about the location of the bomb, the time the bomb is set to explode, the shape of the bomb, the reason why the bomb has been planted, and its magnitude. Also ask the caller for his or her name and address, and the reason why the particular location for the bomb was chosen. Pay close attention to the caller's voice, any background noise, the type of language used by the caller, and whether the

voice sounds familiar. Any of this information will be of value to the campus police as they take appropriate action. When a call is received, contact the campus police immediately and follow their directions. Refrain from using cell phones, microphones, or portable radios, since the radio frequencies waves transmitted by such devices can activate a bomb's triggering mechanism if it is within 1,000 feet of the phone or radio.

Acts of Terror

Prior to September 11th, the risk of a terrorist attack against a university seemed remote and far-fetched. But the events of September 11th and the subsequent incidents of anthrax contamination have convinced campus executives to incorporate acts of terrorism into their disaster preparedness plans. These plans focus on the malicious release of chemical, biological, or radioactive agents. One primary area of concern is the introduction of such agents through the central heating, ventilation, and air conditioning system (see chapter 5 for a detailed discussion of this threat and recommended responses). Threats from chemical, biological, and radiological agents are discussed below.

CHEMICAL AGENTS. Chemical agents can cause a variety of reactions ranging from mild headaches to serious injuries, incapacitation, or death. The impact of a chemical agent is felt quickly and exposure to a chemical agent requires immediate remedial action. Such agents can be spread by aerosolized devices, opening or breaking containers, and other covert actions. Chemical agents can cause nausea, disorientation, breathing problems, and other serious life-threatening reactions. The effects of a chemical agent will be limited to a highly localized area, and will be felt within the first few minutes to a half an hour of release. The presence of unexplained odors, droplets, oily films, abandoned spray devices, or unusual metal debris should be considered indicators of such an attack.

BIOLOGICAL AGENTS. People who are exposed to biological agents may not experience symptoms for several hours or up to several weeks after exposure. This makes the detection of a biological attack more complex and difficult. In most cases, local health care providers will be the first to detect exposure to biological pathogens such as anthrax or smallpox. By this time, those exposed may have infected others with whom they have come into contact. The presence of suspicious devices or packages, coupled with the occurrence of a pattern of diseases or illnesses that are inconsistent with the region or area, indicates that a biological attack has occurred.

RADIOLOGICAL AGENTS. Exposure to radiological agents may not be apparent to its victims unless a detection device is used. The presence of unexplained fuel

canisters with nuclear placards or of nuclear equipment in areas where they are not normally used or stored may indicate that people have been exposed to nuclear or radiological agents.

There are three likely scenarios for an intentional dissemination of radiological agents. The first scenario consists of an explosion that results in a nuclear yield. This may occur if weapon-grade, or close to weapon-grade, radioactive isotopes of a nuclear fuel such as plutonium or uranium are combined in an explosion in which a nuclear chain reaction is simulated. The second scenario involves the use of a non-nuclear explosive device to spread radiological agents. This can occur if a detonating device is surrounded with radioactive material. Upon activation of the explosives, the radioactive materials will be spread over a large area. Experts call this a "dirty bomb." The third scenario entails spreading a radiological agent without the use of a non-explosive device, such as a crop duster.

In case of a suspected radiological incident, campus law enforcement should secure the area as quickly as possible. A radiological incident requires immediate support from other agencies, including the Federal Bureau of Investigation, U.S. Department of Justice, and state and local law enforcement agencies as needed.

USA PATRIOT ACT OF 2001

President Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, commonly called the USA Patriot Act, into law on October 26, 2001. It consists of nine sections addressing domestic security:

- Title I: Enhancing Domestic Security Against Terrorism
- Title II: Enhanced Surveillance Procedures
- Title III: Financial Infrastructure
- Title IV: Protecting the Borders
- Title V: Removing Obstacles to Investigating Terrorism
- Title VI: Providing for Victims of Terrorism, Public Safety Officers, and Their Families
- Title VII: Increased Information Sharing for Critical Infrastructure Protection
- Title VIII: Strengthening the Criminal Laws Against Terrorism
- Title IX: Improved Intelligence

The act gave sweeping powers to Federal Bureau of Investigation and other law enforcement agencies in combating terrorism. Colleges and universities are most impacted by the law's provisions on the stockpiling of biological agents. Also, the act defines "restricted persons" who are prohibited form handling such substances. The law prohibits campuses from stockpiling biological agents, microorganisms, and toxins in unnecessary and excess quantities. Moreover, it prohibits the restricted persons from possessing, receiving, transporting, transforming, or ship-

ping these substances. The prohibition and criminal sanctions for violating the act apply to individuals.

According to the act, a "restricted person" is anyone who has been or is:

- indicted or convicted of a crime that is punishable by more than one year of imprisonment;
- a fugitive from justice;
- an illegal alien in the U.S.;
- a legal alien in the U.S. — not including permanent resident — who is a national of Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria;
- an unlawful user of any controlled substances such as illegal drugs or a drug used illegally;
- adjudicated as mentally defective or has been committed by a mental institution; and/or
- dishonorably discharged from U.S. armed forces.

It is important for university researchers, principle investigators, and laboratory directors to become familiar with the act and its relevant provisions. Although the criminal penalties for violations apply to individuals rather than institutions, any violations can jeopardize the institution's reputation. Such risks can be minimized if the university ensures that faculty and staff potentially affected by the law understand its prohibitions. Moreover, policy decisions must be made concerning appropriate actions to be taken if and when an individual can no longer pursue his or her work because of the act. Finally, hiring and appointment letters for these positions should contains condition positions specified by the Patriot Act stating the individual's legal ability to work with the necessary materials.

ELEMENTS IN THE DISASTER PREPAREDNESS PLAN

A disaster preparedness or emergency response plan is used by an institution to coordinate its resources to protect life and property immediately after a significant accident or disaster. The plan must define the command structure as well as the roles and responsibilities of key emergency response staff. It should spell out how the plan will be activated and by whom.

The organizational structure outlined in the disaster recovery plan should be simple and top-down in nature, involving a few key players who can make decisions promptly. It should differ from the organizational chart used for the institution's normal operation, since the chaos and confusion created by most disasters can render highly detailed, step-by-step response plans useless within moments of the incident. Because timely decisions are critical, a response plan should use a holistic and systemic approach to the emergency rather than one requiring decision by committee. Normal decision-making on a college or university campus typically entails periods of deliberation, multiple inputs, and shared consensus. This is inappropriate for emergencies, when decisions must be made rapidly and decisively.

An effective emergency response consists of five elements: (1) initial notification, (2) immediate assessment of conditions, (3) activation of the emergency plan, (4) protective actions to minimize damage, and (5) required follow-up activities. Because help from external agencies is needed in many emergency situations, the university's plan should be coordinated with local and regional fire departments, HAZMAT teams, and other local emergency response entities. Remember that while these agencies will be helpful if a disaster is confined to campus, they will be preoccupied with helping other affected areas if the disaster is widespread (due to earthquakes or floods, etc.). The university cannot count on their support during the first hours (or days) after a widespread disaster.

The key elements of a disaster response plan include:

- overall statement of purpose;
- criteria for declaring an emergency and putting the plan into action;
- organizational chart for emergency response and designated chain of command;
- communication plan, including a designated media spokesperson;
- names and telephone numbers of critical staff;
- default assignments for critical staff; and
- basic supplies and equipment.

KEY STEPS IN DEVELOPING A DISASTER PREPAREDNESS PLAN

Clearly defining roles and responsibilities among different disaster response departments will ensure that a disaster preparedness plan will operate smoothly and be effective. This entails identifying key university stakeholders, such as faculty, students, staff, alumni, student families, local neighbors, and state and local agencies. An effective response plan and communication system that addresses the need of all stakeholders is crucial. Contact information and coordinated on-call systems are critical components of the plan.

The first step in developing a disaster preparedness plan is to perform a risk analysis and determine which specific hazards should be addressed. A list of typical hazards includes events such as earthquakes, hurricanes, tornados, power failures, terrorism, and fires. Keep in mind that such incidents typically do not occur in isolation; one incident may trigger other types of hazards. For instance, a hurricane may spawn a tornado, cause power outages, create strong winds, and produce flooding. Similarly, an earthquake may generate fires, release hazardous materials, and cause water dams upstream of the campus to fail.

The second step is to create a profile of likely hazards and their possible consequences. This will include such items as frequency of the hazard, possible magnitude, duration, and seasonal patterns. Historical data is an excellent guide in predicting these factors. Other sources of information include Federal Emergency Management Administration (FEMA), the National Weather Service (NWS), U.S. Geological Survey (USGS), and the Federal Insurance

Administration (FIA). In addition, an inventory of hazardous chemical, biological, and radioactive materials is important for responding in emergencies.

The third step involves prioritizing the risks identified during the second step, using this information as a general framework for developing the campus' emergency response plan for specific hazards.

The fourth and final step entails testing the plan and identifying areas for improvement. As gaps become apparent, modify the plan to address specific concerns.

USING A POLICY GROUP AND AN OPERATIONS GROUP

The organizational structure of the plan is a key element in determining its effectiveness. One common organizational approach is to create and use two distinct and separate response units: (1) a policy group and (2) an operations group.

The policy group consists of campus leadership, such as the president or chancellor, provost, vice president of business and finance, vice president for student affairs, chief information officer, chief university spokesperson, legal counsel, and others identified by the president as needed for specific emergencies. This group is responsible for deciding when to activate the plan, determining all policies and procedures to be followed during the emergency, and handling all media interactions during the emergency.

The operations group carries out the tactical and operational tasks under the direction of the policy group. On many campuses, the director of public safety heads this group. Other key members include, but are not limited to, the director of the physical plant, the director of human resources, the director of purchasing, the director of environmental, health, and safety, and the director of financial services. In order to carry out all of its tasks, the group's efforts are augmented by several field department units. These include student health center, information technology, residential life, and counseling services. These areas should be required to develop their own department-based emergency plans that are coordinated with the campus-wide plan.

The major tasks of the operations group include implementing the directions and priorities of the policy group, gathering and communicating field information to the policy group, securing the resources needed to support the operation, and keeping track of all costs related to the emergency. The efforts of this group are divided among four major units:

Operations Unit

This unit is responsible for activities such as law enforcement, traffic control, search and rescue, building assessment, hazardous material handling, and medical and counseling services.

Finance Unit

This unit records and keeps track of finances, campus staff, and volunteers actively involved in field and other associated activities.

Logistical Unit

This unit is responsible for securing equipment and procuring supplies, and attending to shelter, utilities, and communication.

Planning Unit

The planning unit analyzes field conditions and documents damage, assesses the impact of the disaster on academic areas, and serves as liaison with the faculty.

One of the challenges in developing an emergency response plan is identifying team members for leadership positions. Some of the criteria used for selecting employees when filling normal positions, such as punctuality, may not be relevant for emergency conditions. Emergencies require a high degree of structure and clear roles and responsibilities. Responders must be able to think quickly in real time and adapt to quickly changing situations. Therefore, managers who are linear thinkers and who may perform well under normal circumstances may not be good choices for an emergency response team. Employees who have been with the institution for many years may be good candidates, since they may know more about the organization and may command the respect of novices. But they also may be deeply entrenched in the existing institutional practices and unaware of or unable to readily accept new and more innovative approaches.

Another important consideration when selecting members for the team is the distance of a team member's residence from the campus. This can become a critical factor if an emergency occurs after normal working hours. During the 1994 Northridge earthquake, for example, several key team members could not get to the severely impacted campus of California State University, Northridge, since many freeway overpasses were damaged and several roads were impassable. Similar difficulties were experienced during Elena, the 1985 Florida hurricane. In many cases, the issue is not only distance but also accessibility.

THE ROLE OF THE EMERGENCY OPERATIONS CENTER (EOC)

Institutions should create an Emergency Operations Center (EOC) that can be activated during emergencies. The EOC can be used to store all necessary equipment and supplies well ahead of an emergency. The EOC is activated when the campus president or chancellor declares an emergency, and it serves as the main command center until conditions have been stabilized and the EOC is deactivated. The EOC should be located in a building that is structurally sound and is likely to survive a disaster intact.

In selecting the location for an EOC, is it imperative to match the building with various kinds of prevalent disasters for the local area. For example, an EOC for a California campus, where earthquakes are of major concern, should be located in a single-story building above the 100-year flood plain and away from tall buildings. In contrast, an EOC for a campus in the Midwest, where tornados are of major concern, would be in the basement of a building locat-

ed above the 100-year plain and built as a concrete bunker. This EOC should have the structural strength to withstand winds of up to 500 miles per hour. In addition, if the EOC is located at subterranean level, it reduces the probability of any damage sustained by the tornado.

The EOC should have an easy means of ingress and egress, and should be equipped with its own stand-alone emergency power units. These units should be powered by gasoline or diesel fuel; the natural gas supply could be interrupted in an emergency. The EOC should contain all essential emergency communication equipment and preferably have its own network server. In addition, there should be adequate storage space for basic supplies, first-aid kits, campus maps, utility plans, and other essential items. In addition, a kitchen located either in the EOC or in a nearby building is helpful, since the center may remain active for days prior to and after a disaster and EOC staff and other essential personnel must be fed and cared for.

ACTIVATING THE EMERGENCY RESPONSE PLAN

The campus chief executive officer (president or chancellor) is responsible for activating the emergency response plan. If the chief executive officer cannot be reached, the provost or the CFO may activate the EOC. Because rapid decisions must be made during the initial phase of any emergency, the college or university must identify in advance several individuals with a predetermined hierarchy for declaring the emergency and activating the EOC. Should that person be unavailable, the next highest-ranking (and physically present) member of the cabinet should be authorized to activate the plan.

Soon after an emergency is declared, the head of the operations group or the highest-ranking team member should activate the Emergency Operation Center. The policy and operations groups should gather in the EOC. The operations unit dispatcher immediately begins contacting other members of the EOC by telephone, pager, or e-mail (if functioning), and periodically reports to the director of the operations group on the availability and arrival time of team members. If communication lines are down, the director of operations may call upon the news media to notify the public that an emergency plan has been activated. This becomes the signal for EOC members who are off campus to report to campus as soon as possible. The director of operations then designates individuals for the operation, finance, logistical, and planning units.

EOC OPERATIONS

The operation of the EOC is governed by the priorities set by the policy group. Generally speaking, the basic priorities are the physical safety of individuals, followed by securing and preserving physical assets such as buildings and infrastructure, and restoring academic programs. While the character and nature of individual disasters may determine the order of priority for initiating a specific response, the following illustrates an appropriate order of priority for initiating responses for various types of buildings.

1. Facilities occupied by many individuals, such as residence halls, hospitals, classroom buildings, occupied stadiums, or other special event venues
2. Facilities that house student health centers, hazardous materials, and critical supplies such as food, and buildings that could be used as potential shelters if needed
3. Facilities that house major campus systems, such as information and communication centers, central utility plants, and energy systems
4. Facilities that contain classrooms, labs, and other academic spaces
5. Facilities that house administrative functions and other uses not mentioned

An important factor in responding to an emergency situation is managing the flow of information. Under an Incident Command System, the information path follows the organizational structure of the plan. This means that information collected by field department units is transmitted to the policy group by the operations group. Similarly, any directions issued by the policy group to field departments is communicated by the operations group. Because EOC members are responsible for performing multiple tasks, there is a high probability that they will overlook some of these tasks during an emergency. Given this, checklists should be developed as part of the plan. Copies of these checklists should be included in the booklets distributed to all EOC members, because some members may assume and perform the duties and responsibilities of other center members.

During an actual emergency, EOC team members are expected to collect and analyze a large amount of information and to make decisions quickly. In many cases, members will be forced to make decisions with incomplete information. They need to remain focused on organizational priorities as conditions change. Therefore, it is critical that senior leaders be able to cope with ambiguity, and that they possess temperaments that allow them to consider innovative approaches and solutions that have not been thought of previously. Only leaders who have the resilience to withstand a high-intensity, fast-paced decision-making environment can successfully meet these challenges.

Once conditions have stabilized and normal operations resumed, the emergency plan should be deactivated. However, some follow-up activities will continue, such as identifying alternate spaces for affected academic and support programs, and determining the extent of losses and identifying cost recovery issues.

Losses caused by many disasters are of such magnitude that financial and logistical help is needed from federal and state agencies. Given this, key team members should be trained on interacting with the Federal Emergency Management Administration (FEMA).

ATTENDING TO THE NEEDS OF STAFF DURING AND AFTER AN EMERGENCY

Even an organization with an effective disaster recovery plan sometimes fails to address employee needs during and after an emergency. When an organization successfully survives a disaster,

leaders and senior managers will feel a strong sense of satisfaction and accomplishment, and may presume that all staff share a high level of satisfaction as well. This may reduce the ability of managers to be sensitive to the needs of their staff in the aftermath of a disaster.

Managers must be aware of and attend to the emotional needs and anxieties of staff after a disaster has occurred. Communicate to employees that management cares about them and that their feelings of anxiety and fear are natural and understandable. The importance and value of employee assistance programs (EAP) in times of crisis cannot be overemphasized. Most universities offer such services through in-house professionals or outside firms. Use multiple communications channels to remind employees about the services offered by the EAP.

The American Psychological Association has identified the following warning signs of fear and anxiety or post-traumatic stress (MARSH, 2001). It is important that managers be cognizant of the signs of post-traumatic stress among their employees:

1. Recurring nightmare and preoccupation with the event
2. Shift in appetite
3. Difficulty in falling asleep
4. Experiencing fear and anxiety if exposed to situations that may remind the individual of the event
5. Experiencing sadness, depression, and lack of energy
6. Being on edge and too alert
7. Inability to make decisions or focus on routine and daily activities
8. Feeling withdrawn and disconnected to others
9. Failure to remember specifics of the event and avoiding things that may remind the individual of the event

TESTING AND MAINTENANCE

Ongoing training must be a crucial part of an emergency response strategy. No matter how well designed a disaster plan may be, it will be useless if members of the emergency response team have forgotten its elements and their individual roles. This emphasizes the importance of holding regularly scheduled refresher courses for existing staff. In addition, new employees must become familiar with the plan.

Another important aspect of disaster preparedness is conducting periodic tests of the plan's performance. Many universities attempt to fully or partially activate their plan once a year to identify areas that need to be modified or improved. Periodic disaster simulations must contain an assessment component to measure important factors such as speed of activation and ease of coordination among various response teams so corrective actions can be taken to improve the plan. This also calls for a source of ongoing funding for the plan to ensure that it will work if and when it is activated.

SUMMARY

In summary, six major steps are involved in creating a disaster preparedness plan:

1. Identify a small team of individuals to serve as the working group to develop the recovery plan. Team members should have expertise in law enforcement, physical plant, environmental health and safety, computer and communication systems, internal auditing, and financial management. The team may report to campus senior leadership through the vice president for business or administration.
2. Review campus mission-critical processes and examine worst-case scenarios in the event of a major disaster. In addition, the team should investigate how quickly these processes could be restored during an emergency.
3. Identify the kinds of impact disruptions can cause and the actions necessary to develop backup and work-around systems so the campus can function at the minimum acceptable level. This may also include developing agreements with vendors and/or other agencies that can provide part or all services during the recovery period.
4. Seek ways to improve organizational tolerances within such process failures. This may include redesigning the process to reduce or eliminate its vulnerability.
5. Determine key staff required for such emergencies and their general areas of responsibilities.
6. Document the findings and periodically test to ensure their validity and/or make appropriate changes.

Finally, the following questions can be used as guidelines to evaluate the organization's level of disaster preparedness:

1. Is an evacuation plan available, and are all employees familiar with the plan?
2. Is the plan periodically tested and is staff feedback used to make enhancements?
3. Do all employees know their assigned role in a disaster, including where to assemble?
4. Are there procedures in place addressing whom to notify during an emergency? In answering this question, spot-check to see if the emergency off-hour telephone contact list includes cellular phone numbers, pagers, and e-mail addresses for key staff.
5. Is there a procedure to systematically update the above information in a timely manner?
6. Are training sessions held on the disaster preparedness plan, including periodic rehearsals? Are insights learned during the rehearsals used to improve and refine the plan?
7. Are local emergency response groups, such as fire departments, HAZMAT teams, and local utilities familiar with the campus layout? Do they know the locations of the main switching stations, main water valves, chemical storage areas, and the like?

CHAPTER THREE

BUSINESS CONTINUITY PLANNING

Before discussing business continuity planning in more detail, it is important to understand the main difference between a disaster preparedness plan and business continuity planning. The primary difference between a disaster preparedness plan and a business continuity plan is that the former is concerned with tactical solutions while the latter deals with strategic issues.

A disaster preparedness plan basically addresses the period immediately following the disaster. The emphasis at this point is to bring conditions under control, minimize damage, and resume critical functions at the minimum acceptable level.

A business continuity plan, on the other hand, deals with how critical functions can be restored to their normal performance level so recovery can occur. It concerns all resource questions involved in facilitating and sustaining long-term recovery. In addition, disaster preparedness planning mainly addresses operations, while business continuity planning addresses a broader range of issues, especially getting a campus up and moving again as an ongoing concern. Business continuity planning is a business rather than a technical issue. It deals with how one keeps an operation running after it has sustained damage as a result of a disaster. More specifically, it addresses such issues as how the organization can receive supplies, manufacture its products, deliver its services, and meet the needs of its customers by resuming the flow of goods and services.

Business continuity planning was originally used for computer centers and information technology systems. The role and the need of business continuity plans have significantly increased for a variety of reasons. In the past several years, many organizations have extended the use of business continuity planning to other critical systems in the enterprise. Some have expanded the concept to mission continuity planning.

INFORMATION TECHNOLOGY AND BUSINESS CONTINUITY PLANNING

The networked enterprise is one of the most dominant forces shaping today's economy. It has fundamentally transformed the major paradigms with which most managers are familiar and comfortable. It is also fundamentally changing the ways in which an enterprise

interacts with its customers, suppliers, partners, and other stakeholders. The proliferation of e-commerce is moving at an increasingly rapid pace because of its sales potential and the savings it promises.

The failure to protect the integrity of an organization's information technologies can be catastrophic. Organizations are becoming increasingly dependent on "just-in-time" systems, meaning that any disruption will affect the entire process. At the same time, the ability to manually provide adequate services is decreasing. Consequently, the gap between the cost of service disruptions and the ability to use manual systems is widening. Given this, organizational leaders are asking questions not only about their ability to respond quickly to business disruptions, but also about how the risks they face can be managed in such a way that they can continue to meet the needs of current and future customers. The result is the need for a holistic approach to risk management, with an emphasis on prevention. This is where a comprehensive mission continuity plan comes into play. Despite the importance of mission continuity planning, a study by KPMG Consulting suggests that while over 60 percent of corporations have enterprise-wide disaster recovery plans, more than 70 percent have not been able to meet all of their recovery objectives (Alonso, 2002).

The growing use of enterprise resource planning, customer relationship management, and e-commerce has greatly increased the need for closer collaboration among an organization's partners. The complexity of mission continuity planning for both physical and cyber assets is also rising. As a result, executives must pay close attention to both if they want to ensure the survival of their enterprise. This requires an overall change in the way organizations address risk: from meeting a predetermined recovery time during an emergency to focusing on how to ensure the continued operation of information service systems at all times. In other words, the emphasis has shifted from responding to a single catastrophic event to managing the total impact of service interruptions.

The terrorist attacks of September 11th have fundamentally changed aspects of risk in general and, more importantly, for information technology. Even before this tragedy, IT professionals believed that as the level of connectivity increased, so would the vulnerability of a particular asset. In a survey of more than 450 executives and IT directors, conducted by one of the major consulting firms, over 75 percent had experienced unplanned service interruptions. In addition, they reported a wide gap between expected recovery-time versus the actual time needed by many information centers.

Like other business enterprises, colleges and universities rely on major enterprise-wide integrated computer application systems. These may include enterprise resource management and other major systems, such as customer relationship management, to which many employees, suppliers, partners, and other higher education institutions as well as state and federal agencies must have access. These systems process thousands of transactions per second, typically in a distributed hardware environment. These systems not only execute a large number of

transactions in seconds, but they also serve as the eyes and ears of the enterprise by collecting, analyzing, and storing terabytes of data and converting them into vital information critical to the successful operation of the organization.

Prior to the use of enterprise resource planning applications, large computer applications ran on a single platform on a mainframe connected to a limited number of dumb terminals and a few other input/output (I/O) devices. This meant that the mainframe systems were usually operating in a stand-alone fashion. As a result, data security and reliability issues were simple and straightforward. With the advent of enterprise resource planning, most applications now run on a three-tiered architecture. This means that the presentation software, the application, and the database reside on different hardware, and that the three layers are connected by high-speed links to many other computer systems within and outside the organization. Service interruptions are more damaging to the organization in this environment. The tolerance for system outages is extremely low because mission-critical applications are an integral part of most enterprise resource plans, and security and reliability matters are far more complex now than they were in the days of mainframe computing.

UNDERSTANDING THE RISK OF CYBER ATTACKS

Deliberate sabotage, hackers, crackers, computer viruses, human error, power surges or outages, hardware failures, network downtime, fires, and floods may disrupt computer systems. A survey of computer crime and security issues conducted by the Computer Security Institute (CSI/FBI) in 2001 found that 70 percent of 538 respondents said that their Internet site was subject to computer attacks, up from 59 percent for the year 2000. Ninety one percent reported that their employees abused their Internet privileges.

While the main types of cyber-crimes involve viruses, denial-of-service, hackers, security breaches, internal attacks, and privacy violations, FBI statistics show that roughly three- quarters of all threats to computer systems come from former and/or disgruntled employees. For this reason, an effective information security system that can prevent internal attacks reduces the bulk of an organization's potential vulnerability.

Based on current estimates, there are 65,000 known computer viruses, and between 300 and 600 new computer viruses are introduced each month. *Internet Week* reported that in 1999, over 6,800 person years were spent in North America alone addressing virus and DoS (Denial of Service) attacks. The cost of computer virus attacks in North America for the year was estimated at $1.6 trillion (Vulpitta, 2002).

One way to get a better understanding of how vulnerable critical services are to cyber attacks is to investigate the interdependencies among telecommunication, electric power, and financial services. Telecommunication and financial systems cannot function without electric power. And distributed financial systems cannot function without telecommunication services. The controls of most utility electrical distribution systems are provided remotely; power systems

would fail without computers. Finally, an attack on a financial system will create havoc and seriously damage the functional ability of an institution.

Although a large number of organizations have basic information security procedures in place, almost half say they fail to investigate information security breaches to determine the root cause of their vulnerability. Many organizations believe that mission continuity planning for information technology is the responsibility of the IT department rather than an integral and critical part of the organization's larger strategy. That is why senior executives in many organizations are not actively involved in information security and its role in achieving the organization's overall mission.

Despite the importance of information systems, a significant number of staff are unaware of policies addressing information security. In fact, many staff are unaware of training programs that address this issue. Although almost three-quarters of all cyber attacks come from an organization's own employees, many organizations still believe they are more vulnerable to external attacks.

Until recently, most cyber attacks involved amateur hackers of high school and college age. Most gained access to computer systems via "back doors" that were often left open to allow authorized vendors to gain system access. Unfortunately, this allows hackers to enter as well, and when they do, they can gain access to the system undetected and begin to control it. Therefore, keeping a computer system's "back door" open or failing to install patches or use adequate firewalls and virus protection programs are analogous to keeping an institution's doors and vaults unlocked and open to the public. Most computer system vulnerabilities are the result of weak operating systems when patches are not applied.

A recent study by the FBI cites a sobering statistic: roughly 90 percent of all criminals in the U.S. are computer literate. This implies that cyber attacks will escalate even further. Moreover, as the sophistication of these computer-literate criminals increases, so will the frequency and the complexity of cyber attacks. This means that we can expect to see the proliferation of more sophisticated computer viruses and worms and other forms of DoS attacks. For instance, the number of pending computer attack cases being handled by the FBI climbed from 126 in 1996 to 1,154 in 1999. Some expect DoS attacks as well as sophisticated viruses and worms to continue to increase at a rapid pace. The number of attempts to deface electronic information sites will rise, and more attempts will be made to spread disinformation and propaganda. Finally, unauthorized intrusions into critical infrastructure systems may result in utility service interruptions and/or data corruption.

TAKING STEPS TO PROTECT COMPUTER SYSTEMS AND NETWORKS

The following 12 steps can be used as a guide to protecting computer systems and networks from these attacks. While taking these steps won't totally eliminate the possibility of cyber attacks, they will provide reasonable assurance that the damages from such attacks will be minimized.

1. Review the policies and procedures relating to employees' and vendors' access to all computer systems and networks.
2. Define and identify every user groups' access to the system, and review the business justification for the access. This involves reviewing the access levels of all employees.
3. Develop mechanisms to enforce the policies and practices already in place.
4. Make sure that the computer systems maintain a record of all user logins. In addition, the system should retain a backup copy of these records, preferably in separate hardware.
5. Create an adequate separation of duties among all system operators, programmers, and network administrators.
6. Establish a systematic process to periodically review the latest technology in computer security, and determine whether they are appropriate for the operations. Sometimes, installing security patches provided by manufacturers can effectively protect against almost all known security breaches.
7. Employ a system that forces users to change their passwords periodically. Moreover, passwords should be a minimum of eight characters, and the system should store several prior passwords and not accept them again if a person tries to reuse the old password as a new one.
8. Create a procedure that will systematically review updates on the sources of the latest cyber attack. These updates can be obtained from the FBI's National Infrastructure Protection Center (www.nicp.gov), the InfraGuard forum (www.infraguard.net), and Carnegie Mellon University's CERT Coordination Center (www.cert.org).
9. Establish procedures to perform data backup of all systems on a frequent basis. In addition, create provisions for off-site storage of all critical data in a secure location.
10. Make sure that computer systems are adequately protected against electrical problems such as power outages and surges. This includes installing backup systems as discussed in more detail in chapter 5.
11. Institute security audits using unbiased and competent personnel, i.e. the internal auditor, or third party, and implement all reasonable recommendations from these audits.
12. Review termination procedures and take appropriate steps when employees are reassigned or separated from the institution to ensure that their access to the system is revoked.

CREATING A BUSINESS CONTINUITY PLAN

Business interruption is defined as the loss of productivity, output, and/or profits caused by any disruption of normal operations. Losses may include physical damage as well as additional

expenses incurred while operations are being restored. Most business interruption policies address direct losses but fail to include indirect expenses such as unabsorbed overhead, unproductive labor, or employee payroll. As a result, business interruption insurance does not provide a financial guarantee, nor does it cover all losses (see the section that follows for a discussion of business interruption insurance as well as business recovery services). This underscores the need for a strong, effective business continuity plan.

The first step in creating a business continuity plan is performing a risk assessment. The second step is to develop an emergency response plan. The third step is creating a communication plan to disseminate critical information within and outside the institution. The fourth and final step is ensuring that an effective crisis management plan is in place to get the organization back on the road to recovery and normalcy as quickly as possible.

In developing a business continuity planning team, make sure to include individuals with expertise in database administration, computer hardware, application software, systems engineering, networking, and telecommunication, disaster recovery, business continuity, and process management. In addition, secure representatives from key application user groups and any other major internal and external customers, suppliers, and users.

The first task the team will face when developing the business continuity plan is performing the risk assessment (see chapter 1 for a detailed discussion of this topic). This can be done by asking the following questions:

1. What are the organization's most critical processes? These processes may include student registration, student records, payroll, accounts payable, accounts receivable, and general ledger, to name a few.
2. Which applications are part of the campus enterprise resource plan and which are running independently on legacy systems? Which applications are accessible via the Internet?
3. What risks are assumed if any of the above applications fail? What are the consequences of these failures?
4. What kind of service disruptions can the organization tolerate before they begin to have a detrimental affect on the organization?
5. What kinds of work-around or other procedures are in place in case of a failure?
6. Are any procedures in place to periodically test these work-around processes?
7. Are there processes for which no backup procedures are available? If gaps are identified, develop backup procedures for these processes.

An effective business recovery plan entails more than having a fully redundant system for the mission-critical environment. The plan must (a) address alternate facilities and communication equipment, (b) include a comprehensive business impact analysis, and (c) have a fully developed business continuity plan. The business impact analysis will systematically calculate the cost of downtime for every mission-critical system. Based on the downtime cost analysis, it

can become obvious that the cost of down time for critical systems may vary widely. The impact analysis can help determine the cost-value relationship for these systems. Consequently, the institution can focus its resources based on overall organizational priority. In other words, resources may be allocated to mission-critical systems that have the highest priority and the costs can be justified based on the values that will be attained in improving business continuity.

BUSINESS RECOVERY SERVICES VS. BUSINESS INTERRUPTION INSURANCE

The costs involved in acquiring a fully redundant system may be prohibitive. A more cost-effective approach may be to contract with a business recovery center. Many industries have used business recovery services to reduce their exposure to the risk of business interruptions. There are some similarities between the use of a business recovery service and acquiring business interruption insurance. Both try to protect the institution from unpredictable events and associated costs, and both use a shared-risk model. The underlying principle of business interruption insurance is that because the risk of interruption is low (albeit costly), the premiums paid by a large number of participants in the pool will be sufficient to cover the costs incurred by those who suffer a loss.

Many senior executives do not clearly understand the factors that impact decisions about business interruption insurance and allocating resources across risk categories. Nor do they typically relate risk-management expenditures to value gained. One reason for this is that many senior executives have not systematically evaluated the alternatives available to them for reducing their exposure to risk. Effective risk management requires better insight concerning the existence of major threats and the steps that must be taken to assess and, subsequently, reduce the risk. This involves knowing how much risk the enterprise can tolerate, and what should be done to address the balance of the risk it faces. This also means determining which risk levels can be self-insured and which levels of deductibles should be chosen. Finally, it means determining whether the organization can afford the premiums at the desired level of deductibles.

One of the results of the September 11th terrorist attacks is increased business interruption insurance premiums. The insurance market had tightened significantly because of the stock market losses of 2000, but insurance premiums skyrocketed after the attacks. This is another reason for expending more effort on business continuity planning. In fact, some insurance companies are offering lower premiums to organizations with business continuity plans in place.

A business recovery service offers shared resources to its subscribers at a reasonable cost, assuming that several subscribers will not experience interruptions at the same time. Given this, the same hardware could be subscribed to by many at a much lower cost than would be entailed in providing a dedicated redundant system.

There is a fundamental difference, however, between acquiring business interruption insurance and working with a recovery service. In dealing with an insurance company, the insti-

tution's relationship with the insurer will be passive and reactive except for paying the premiums and, possibly, adopting some of the carrier's recommendations. In contrast, the institution's relationship with a recovery service will be proactive in the sense that the institution will be expected to work actively to eliminate or minimize down time. This entails performing dry runs and using the service's technical advice in system configuration.

A second and perhaps the most significant difference is that insurance normally covers only the direct financial costs generated by an accident. In many cases, insurance will fall short of covering indirect costs such as customers' good will, organizational image, and market share loss. In many cases, these costs may be larger than direct costs and may seriously jeopardize the survivability of an enterprise. The business recovery service, in contrast, will seek ways to eliminate or significantly reduce interruption so these losses will not be realized.

RAPID RECOVERY SYSTEMS

As an organization's dependence on real-time computing increases, the pressure to reduce recovery time to ensure access to a current database is an ongoing challenge. Now more than ever, businesses are examining the feasibility of installing rapid recovery systems for their critical information systems. A number of rapid recovery techniques have been developed to address this need. They include:

1. *Electronic Journaling*. This involves a transfer of log information from the database management system to a remote site.
2. *Disk Mirroring*. As updates on a disk are completed after each transaction, a disk in a remote location is modified. This ensures that the remote disk contains the latest changes made to the production disk, making the remote disk a true mirror image of the original.
3. *Database Mirroring*. This arrangement is similar to disk mirroring, except that as the primary database is updated, the change in the remote database occurs at the same time.
4. *Standby Operating System*. A mirror image of the primary operating system is kept on disk, and a copy could be used promptly in case of a disruption.
5. *Hot Standby*. In this arrangement, a dedicated full or partial copy of the system is ready and available for almost instant use. This may contain a duplicate of the primary system hardware and software. A copy of the unique operations that must be activated in the event of an emergency should also be kept offsite.

MISSION CONTINUITY PLANNING

As mentioned, many organizations have expanded the concept of business continuity planning to all functions that are key to accomplishing their mission. Mission continuity planning is a collection of procedures that define how an organization can resume operations in the event of a dis-

ruption in its ability to provide services to customers. The philosophy behind a mission continuity plan is minimizing or eliminating service interruption to the critical processes that represent the backbone of the enterprise. Developing an effective mission continuity plan can be costly and sometimes difficult to justify when resources are strained. But the costs associated with inaction could jeopardize an organization's survival. The major reasons for developing a plan include:

1. *Meeting Regulatory Requirements.* Some industries, including financial institutions and medical facilities, may be required to have a working mission continuity plan. They must also take reasonable measures to resume operations in a relatively short period of time.
2. *Reducing Insurance Costs.* The existence of a functional mission continuity plan can reduce an enterprise's annual insurance premium by from 5 to 40 percent.
3. *Maintaining a Competitive Advantage.* In the current business environment, many institutions depend on just-in-time delivery systems. Today, many organizations operate as a tightly interconnected system in which a slowdown or stoppage in any part will affect the entire network. This illustrates how organizations are closely linked with their suppliers and customers. Any interruption in the supply chain affects customers and partners more immediately than it did in the past. Because many companies expect their suppliers to have a bona fide business continuity plan, suppliers with such plans can showcase them as a competitive advantage when they compete for business.
4. *Protecting the Organization's Image.* While service interruptions can be costly from a financial standpoint, they can also generate negative media coverage. This can result in the loss of existing as well as potential customers. On the other hand, an institution will gain the public's confidence if it can quickly resume operations after a disaster or prevent any interruptions in service during the disaster from occurring in the first place.
5. *Ensuring the Organization's Survival.* As mentioned earlier, organizations failing to address possible business interruptions have a 40 percent chance of going out of business within two years after experiencing a disaster. Therefore, an effective mission continuity plan can significantly enhance the survivability of an enterprise in the event of a disaster.

DEVELOPING A MISSION CONTINUITY PLAN

The following 11 steps can be used to develop a mission continuity plan:

1. *Set organizational goals and identify realistic objectives.* This involves examining the levels of service interruption the organization can tolerate, and determining the cost of such interruptions. This exercise will help identify the most critical processes and the functional areas on which the organization must focus. During this step,

determine potential risks and threats, and identify what can be done to make the critical processes more robust in order to minimize or eliminate possible threats. Remember that preventive measures will help reduce the overall risk exposure and threat of a possible accident. Risk analysis, covered in detail in chapter 1, involves examining the duration of the interruption, associated financial costs, possible fines or penalties, customer loss, and other factors. Appropriate preventive actions may involve acquiring redundant equipment, setting up alternate operation sites, creating backup electric power sources, and taking other steps to reduce risk. Prevention and mitigation issues can be grouped into three major areas:

- *Preventing identical or similar failures in the same system.* This is the most helpful situation, where knowledge gained from the failure is used not only to perform necessary repairs but also to mitigate, to the extent possible, the probability of a similar failure in the future.
- *Preventing a similar failure in other similar systems.* This entails a situation where, by analogy, one may be able to extend the insights gained in one set of circumstances to eliminate or minimize the probability of failure in other systems with similar characteristics. But remember that it may not be possible to find all failure modes to which the system could be vulnerable.
- *Preventing a failure that has not yet occurred but that, with the proper combination of prerequisites, could occur.* This approach is used to analyze complex systems where the old control conditions may be either obsolete or irrelevant. The lack of prior experience with a similar situation makes the task more challenging and may require a more formal analysis using simulation or other reliability engineering techniques.

2. *Analyze the business impact of the unmitigated risks and their primary and secondary consequences.* For instance, if the student registration system crashes, what impact would this have on classes, enrollment, tuitions and fees collections, and financial aid disbursement? Or, what length-of-failure time frame will negatively impact the organization's ability to fulfill its legal requirements? As part of the analysis, the impact of every critical function and the recovery time should be determined. Establish a recovery time objective (RTO) for every critical function. One method is to classify an RTO for these functions according to the following:
   - AAA Class: These include functions for which down time is not allowed. To accommodate the requirement, a fully redundant hot site of an alternate system in a different physical location may be required. Hot site refers to a redundant backup system that is running in parallel with the main system but normally in a different geographical location. As a result, those using a hot site system will not experience any failure in either of the systems. In contrast, a cold site is a back-

up system that is on standby but not continually operating. The cold site activates when there is a failure in the main system. The switchover entails a temporary loss of service.

- AA Class: This consists of functions that should be recovered within four hours. However, this may require the installation of hardware onsite or in an alternate location. It should be noted that installing hardware and software within four hours is difficult.
- A Class: These functions must be recovered within the same day; however, they do not require set-up hardware.
- B Class: Functions that should recover within 24 hours.
- C Class: Functions that should recover within 24 to 72 hours.
- D Class: Functions that can take more than 72 hours of down time prior to recovery.

In developing RTOs for various critical functions, the interdependencies that exist among them should be kept in mind.

3. *Assign key individuals responsibility for those functional areas for which critical processes were identified,* such as human resources, public safety, facilities operations, financial services, internal audit, and information technologies.
4. *Conduct a business impact analysis.* Look to an in-house risk manager or insurance carrier for assistance.
5. *For every critical process, assign appropriate individuals who can develop a business recovery plan addressing a major service interruption.* This plan would include the cost, time, backup equipment, and any work-arounds needed to resume full operations. Develop agreements to borrow staff from other divisions and from sister institutions. This may be done on a mutual exchange basis. Also, in developing backup suppliers, remember that local suppliers may not be able to help during a region-wide disaster, so consider using national suppliers. The recovery plans may involve one or more of the following strategies:
   - Transfer of functions to an alternate operation within the same organization.
   - Transfer of functions to a different geographical site within the same organization.
   - Making arrangements with a sister institution to serve as each other's backup facility during an emergency.
   - Contracting with a dedicated site that provides backup service.
6. *Identify the minimum requirements needed to return to full operation.* This entails determining which documents, supplies, staff, and other vital resources must be stored offsite. Unless the backup location is a mirrored site, determine the frequency of updating backup records. Based on the agreed-upon frequency, develop a schedule to update back-up records. Other policy issues to be addressed

include identifying who can retrieve backup data, which data should be included, and how long it will take to retrieve the data.

7. *Integrate the individual recovery plans into a draft mission continuity plan,* and resolve any conflicts or inconsistencies among individual recovery plans.
8. *Identify a central location for the mission recovery plan.*
9. *Develop a cost estimate for implementing the draft mission continuity plan recommendations,* and present the plan to institutional leadership.
10. *Upon plan adaptation, conduct training sessions, establish a testing schedule, periodically audit the plan, and make appropriate improvements.* One effective training technique is the scenario walk-through. Cross train staff in several functional areas; it is difficult to know who may be available during an emergency. A more flexible and versatile staff will enhance the chance for a quicker recovery.
11. *Identify a mission continuity planning coordinator to periodically update the plan.* Remember that the plan should be treated as a living document, which means it should always be updated to meet the current needs of the organization.

The need for effective mission continuity planning is becoming more important as colleges and universities increasingly view themselves as members of a competitive industry rather than the model for a monopolistic cottage industry. This requires a radical change in the traditional approaches to allocating resources for mission continuity activities. There is a natural tendency in many organizations to allocate resources to wishful activities rather than to activities critical to the organization's continued existence and success. Neglecting the very real threats and vulnerabilities facing today's colleges and universities will jeopardize the survival of many of these institutions. The vital importance of mission continuity planning must be acknowledged, and the organization's commitment must be demonstrated by the allocation of resources necessary to carrying out mission continuity efforts.

To the best of this author's knowledge, no college or university includes in its mission statement the explicit goal of continuing to exist over a long period of time, although its leaders always implicitly note this goal. If this assertion is correct, then mission continuity planning must be a top responsibility for senior college and university executives. In the words of President Franklin D. Roosevelt, "There are many ways of going forward, but only one way of standing still." The choice is ours!

CHAPTER FOUR

CALCULATING SYSTEM RELIABILITY

DEFINING SYSTEM RELIABILITY

Given the level of complexity of most processes in an enterprise, it is not possible to evaluate the reliability of systems in an ad hoc manner. Rather, it is necessary to approach the issue of reliability from a quantitative standpoint. Reliability can be defined in several ways. The simplest definition is the probability of a product or a process to perform its intended function under specified conditions when desired by the user. Today, reliability studies have migrated from general concepts to a quantitative discipline. Factors that affect reliability include process design, cost factors, environmental conditions, and human factors. There are several ways to enhance the reliability of a process. But before discussing reliability enhancement, it is important to consider the nature of reliability itself.

RELIABILITY METRICS

The reliability of system can be quantitatively measured in relation to system failures. In other words, reliability is equal to one minus the failure rate. Therefore, if one has the value of one of the two parameters, namely reliability or failure rate, the second can be calculated by subtracting the first from one. One approach is to operate the product or run the process continuously until failure. If this process is repeated many times, the data can be plotted for equal time intervals. For most products, the plot will resemble a "bathtub curve," implying that the curve can be broken into three parts.

The first part of the curve is called the burn-in or infant mortality period. Here, the failure rate will be at a high level; however, it will continuously drop. The high failure rate may be due to bad design, poor manufacturing, misuse, or misapplication. This implies that if the system is debugged, such failures will not occur in the future. This is the reason why there may be a delay between the time a new product or new software is released and the time when it is sufficiently robust for most applications.

The second part of the curve entails the product's normal operating period. During this time, the failure rate is constant and is primarily a function of design limitations. Most failures

in this area are due to random causes. Any significant reduction in the failure rate requires a redesign of the product or the process.

The third and final part of the curve is the wear-out period, implying that the failure is due mainly to old age. Here the failure rate continuously increases. To achieve any significant drop in failure rate, critical parts of the system that show signs of fatigue must be replaced.

In most cases, one is interested in the product's normal operating period. It therefore makes sense to focus the balance of the discussion on the constant rate of failure. Here, the constant failure rate implies that the distribution of time between failures will follow an exponential curve. The mean time between failures (MTBF) is the total test period divided by the number of failures, or the inverse of the failure rate. In other words, the higher the failure rate, the lower the MTBF. For instance, if the failure rate is 5 percent per month, MTBF will be 1/0.05 = 20 months. The probability of no failure (or survival) at any particular time can be determined by the exponential of minus time divided by MTBF as shown below:

$$R = \text{Exp } -(\text{time}/\text{MTBF}) = e^{-(\text{time}/\text{MTBF})}$$

To illustrate this with an example, assume that the MTBF for a computer server is 1000 hours and that a particular batch process will take 10 hours to complete. To calculate the probability that the process will complete successfully without any server failure, apply the formula using an MTBF of 1,000 hours and process time of 10 hours as shown below:

$$R = \text{Exp } -(10/1000) = e^{-(10/1000)} = e^{-0.01} = 0.99 = 99\ \%$$

This means there is a 99 percent chance that the process will run successfully without any server failure. Looking at this example another way, the probability of failure is 1 percent.

Although the MTBF concept is simple, it is easy to misunderstand its meaning. First, MTBF is the probabilistic average rate of failure and not a deterministic number. Since MTBF is constant, it is assumed that after every failure, the system is repaired fully and put into operation almost instantly. Second, the probability that a product can operate without any failure for a period equal to or more than the MTBF is 37 percent, and not 50 percent as one would intuitively believe. This is because MTBF represents the average time between two failures and not the probability of whether a product can operate at any given time. The above answer can also be illustrated mathematically, since $R = \text{Exp } -(1/1) = e^{-1} = 0.37$.

Finally, because the exponential relationship between the probability of success (R) and MTBF is exponential, an increase in MTBF does not enhance the reliability by the same proportion. For instance, if the MTBF is five years, the probability of success (R) at one year is 82 percent. If MTBF is doubled to 10 years, R will only increase to 90 percent, or an increase of less than 10 percent. Moreover, if MTBF is again doubled to 20 years, then (R) increases to 95

percent, or an additional increase of less than 5 percent. This implies that any successive large increase of MTBF enhances system reliability by a very small percentage.

ANALYZING SYSTEM RELIABILITY

In most actual applications, a system consists of many individual parts that are connected to constitute the entire system. If one know the reliability of individual components, it is possible to calculate overall system reliability. This can be accomplished by briefly reviewing how to calculate the reliability of individual components if they are connected in a series or in parallel, as shown below.

Series Systems

A series system consists of two or more individual parts or activities where the reliability of the system depends on every individual element functioning as planned. The total system reliability is equal to the product of individual reliabilities. For instance, if a system has three parts and the reliability of individual parts are:

R1 = 95 %
R2 = 90 %
R3 = 85 %

The system reliability is equal to R1 x R2 x R3 = 0.95 x .09 x0 .85 = 0.73 = 73 %

As this illustrates, overall system reliability is lower than the reliability of the lowest part. This shows that the reliability of one part is very low regardless of the high reliability of other components. For instance, if a three-part system has a reliability of 0.95, 0.95, and 0.2 percent, the overall reliability is 0.18 percent. This proves the saying that a chain is only as strong as its weakest link.

Parallel Systems

A parallel system implies that there are two or more paths to complete a process. This means that if all parallel parts operate and one fails, the system will continue to operate. For instance, if a system has three parallel parts, where the reliability of individual parts are:

R1 = 95 %
R2 = 90 %
R3 = 85 %

Calculating the overall system unreliability and subtracting it from 1 determines the overall system reliability.

$$U1 = 1 - R1 = 1 - 0.95 = 0.05$$
$$U2 = 1 - R2 = 1 - 0.9 = 0.1$$
$$U3 = 1 - R3 = 1 - .85 = 0.2$$
$$U = U1 \times U2 \times U3 = 0.05 \times 0.1 \times 0.2 = 0.001$$
$$R = 1 - U = 1 - .001 = 0.999 = 99.9\ \%$$

The overall reliability of a system is more than the highest individual part. No matter how many parts are in parallel, the overall reliability of the system will always be lower than 100 percent. Parallel systems are used in evaluating the role of redundancies in systems.

In most cases, actual systems are rarely either a series or a parallel system. In fact, they are usually a combination of the two, so the analysis requires utilizing both the series and parallel systems.

SYSTEM AVAILABILITY

System availability refers to the fraction of time that a system is ready for use. In order to better understand the concept, let us determine the logical scenario of actual system in the continuum of time. Assume that if a system started operating successfully, it will continue operating successfully over time until it fails. Once it fails, there is an average time required to detect the cause of the failure; and, subsequent to that, another block of time is required to complete the necessary repairs. Then the system will be available for use. The average time between any two failures is the MTBF (mean time between failures). Similarly, the average time it takes to determine the cause of the failure and the parts that need to be repaired is called Mean Time to Detect (MTTD). The average time for the repair is called the Mean Time to Repair (MTTR). System availability is mathematically defined as:

$$A = (MTBF)/(MTBF + MTTD + MTTR)$$

Based on the above concepts, one must increase MTBF and reduce MTTD and MTTR in order to increase system availability. There are several ways to increase MTBF, including choosing a robust system or improving design, incorporating good diagnostics to monitor system conditions, and performing adequate preventive maintenance. Similarly, having the right diagnostic tools and technically competent staff to pinpoint the root cause of the failure so repairs can commence immediately can reduce MTTD. Finally, having access to replacement parts and technical staff needed to quickly perform the required repairs reduces MTTR.

CHAPTER FIVE

ADDRESSING FACILITIES-RELATED RISKS

Physical facilities play a critical role in the ability of colleges and universities to accomplish their mission. That is why it is important to examine some of the main risks associated with these systems, especially those involving electrical distribution, water distribution, and HVAC (heating, ventilation, and air conditioning). Traditionally, design engineers, building code officials, and construction inspectors view structural integrity as the main facilities risk. That is why great care is required in facilities design and construction.

The first step in addressing facilities-related risk is assessing the institution's requirements for openness and tolerance for security. While this is another way to assess risk tolerance, it focuses on physical freedom as opposed to security. The second step in the process is assessing physical conditions and systems, redundancy of systems given a particular level of security. Options need to be developed to meet security needs and solve issues of vulnerability versus accessibility.

Addressing physical security means taking several issues into consideration, including (1) perimeter security (control of access to the campus by vendors, visitors, the public, security of land and hard scapes); (2) physical security (strength and security of building materials and locations, taking into account different threats); (3) physical access (to buildings, utilities service areas, laboratories, offices, etc., and related security approaches such as locks, alarms, and cameras); (4) medical systems; (5) evacuation plans; (6) emergency communications systems; and (7) training to respond to emergencies (for all members of the university community and for emergency responders in the community).

This chapter examines the main risks and reliability issues relating to a campus' infrastructure and its physical facilities. While several security factors will be discussed, the chapter focuses on the risks associated with three main utility systems: electrical distribution, water distribution, and HVAC (heating, ventilation, and air conditioning). In addition, the management of hazardous materials in buildings is examined.

STRATEGIES FOR PROTECTING CAMPUS INFRASTRUCTURES AND FACILITIES

Addressing building security in a university setting is a more challenging task than it is in other

types of settings. The key reason is that universities by their nature are high-access places. Campus master planners have tried to design facilities that are open and inviting for anyone on an almost unlimited basis. This is particularly true when school is in session. The issue today is how to provide adequate security while maintaining a high level of access.

In developing strategies for protecting campus infrastructure and facilities, the first step is to learn about the existing conditions by performing the required inspections and tests to obtain a better understanding of and insight into potential risks. This may involve calling upon in-house expertise as well as seeking help from consultants in the areas of security, fire protection, structural engineering, information technology, and mechanical and electrical engineering. The goal is to obtain input for developing the risk prevention management plan. The second step in the process is to identify mechanisms that can monitor the critical parts of the campus infrastructure and other major facilities to detect potential problems.

When examining the safety and security of campus facilities, pay close attention to: (a) critical buildings and infrastructures, such as utility distribution systems (power grids, water supplies and distribution, telecommunication centers, and utility tunnels), (b) major areas where people congregate (stadiums, concert halls, and other assembly areas), and (c) critical buildings (computer centers, major research facilities, university records, and archives).

ELECTRICAL DISTRIBUTION SYSTEMS

Current electrical distribution systems on almost all campuses are at risk of failures that can seriously interrupt the operation of the university. For instance, should an interruption occur in the power transmission lines between the utility and the campus, in most cases there are no other paths available for delivering power to the campus. This means that for many institutions, all electrical power is delivered to the campus by one cable, and any physical damages along that delivery path can potentially interrupt electrical service to campus facilities. This, in turn, interrupts the operations of the institution. As a result, proactive steps must be taken to ensure the continual flow of electrical power to the campus.

The reliability of electrical distribution systems for a campus depends upon two factors: the utility source and the in-house distribution system. For a large number of small and medium sized campuses, power from the local utility arrives through one cable, and any failures on that line results in service disruption. In order to improve reliability, two pairs of separate cable feeders should connect the campus with the local utility. This dual system is called a double-ended power station. During normal conditions, each feeder cable would provide electricity to roughly one-half of the facility. However, if one of the two cables was damaged for any reason, there is adequate switching to manually or automatically shift all loads to the remaining line, thus reducing the power loss to a momentary interruption. Both feeder cables should not be installed in the same cable duct bank. To the degree practical, make sure there is sufficient physical separation between the two feeders so both would not be affected in case of failure or a fire.

A triple-ended station can be used if an institution desires a higher level of reliability than a double-ended station. Because of the higher cost of this arrangement, a triple-ended station is only used for health care and research facilities to afford greater reliability and protection. With a triple-ended station, the facility has three separate feeders, with two feeder cables coming from one utility substation and the third from a different utility substation. Under normal conditions, each feeder serves roughly one third of the facility. If one or two feeder cables fail, there is adequate switching system capability to disconnect the affected cable(s) and cross-feed all critical loads from the working feeder. A triple-ended substation provides additional levels of reliability even if one of the local utility substations is affected, since service to the facility is not interrupted.

The most common and least expensive way to distribute electricity within the campus facility is the radial system. In this arrangement, the main campus substation is viewed as the center of a circle, with single cables connecting individual buildings to the substation. If the cable fails, power is interrupted. To improve the reliability of an in-house distribution system, a looped arrangement is used. This system is found primarily at medium to large-sized facilities. On these campuses, the primary electric service for several buildings is connected in the form of a daisy chain, in which both ends of the loop terminate at the main substations. This provides two power paths for buildings. If any cable section between any two buildings is damaged, power to all buildings could be restored quickly with proper switching. To further enhance system reliability, more complex distribution arrangements, such as primary-selective, secondary-selective, and network systems, are also used.

THE IMPACT OF ELECTRICAL DEREGULATION

Deregulation of the power industry has created limited choices for some customers while increasing the potential risk exposure for most customers. In the traditional (regulated) model, electric utilities were vertical monopolies responsible for meeting the power needs of all customers. The utility was responsible for projecting future electric needs of its service area and raising the funds needed to build generating capacity as well as the transmission and distribution infrastructure. In this model, state public utilities commissions regulated the price of electricity, and price fluctuations were relatively modest.

With the advent of deregulation, the level of the risks being assumed by institutions is significantly higher. The risk of major price fluctuations increases tremendously, and three factors contribute to a reduction in the overall reliability of uninterrupted service.

First, when utilities were required to maintain adequate capacity to serve all projected loads, the utilities not only built sufficient capacity for peak load conditions but also maintained extra capacity (commonly known as reserve margin) in case of emergencies. The National Electric Reliability Council (NERC) recommends that utilities have minimum reserve margins of approximately 15 percent. In the 1970s, the average reserve margin in the U.S.

was around 30 percent. Although that did not reflect a cost-effective system, it did ensure a more reliable source of power for customers.

With the rise of independent power producers and the uncertainty associated with deregulation, many utilities have postponed building new generation plants. As a result, the average reserve margin nationally is now less than 10 percent. Since reserve margins are not uniformly distributed across all geographical areas, states in some regions such as the Southwest and New England have experienced capacity shortfalls that led to sizable price fluctuations and power shortages. Rolling blackouts have occurred in California, Nevada, Arizona, New York, and several other states. Similarly, several areas around Chicago faced price hikes with power purchases at the wholesale level during the summers of 1998 and 1999.

To illustrate the magnitude of these price fluctuations, consider that during the past few years, electricity was being bought and sold at somewhere between $25 and $50 per megawatt-hour at the wholesale level, depending on specific region of the country. This translates into 2.5 to 5 cents per kilowatt-hour. When the transmission, distribution, and other costs were added, the price-at-retail figure would be between 6 and 11 cents per kilowatt-hour. In 2000, the peak price in California rose above $3,000 per megawatt-hour. In fact, in July 1998, the price in the Chicago area at one point reached $7,000 per megawatt-hour, or 140 times the normal price.

Second, the current shortage of adequate transmission lines creates a price and reliably risk factor. Even if there is adequate generation capacity, there are no adequate means to transport the power to consumers. The underlying reason for the current lack of transmission lines is due to the fact that while companies building electric generation sites can recover their investment within four years, it takes 28.5 years to recover a transmission line investment. Given the absence of regulatory pressures and the lack of financial incentives, and because it costs an average of $100,000 per mile to build new transmission lines, very little new transmission capacity has been added. In 1990, for instance, about 12,500 miles of new transmission lines were being added annually. By the end of the decade, however, that number dropped to less than 5,000 miles per year.

Third, the age of many electric generation units and distribution systems is creating substantial risk. As a former U.S. Energy Department secretary has noted, "America is a superpower, but it's got the grid of a Third World nation." In sum, deregulation has increased the risk factor for power systems and has negatively affected their reliability.

DEPENDENCE ON THE DIGITAL ECONOMY

Another consideration is the risk that the growing dependence of the Internet and related electronic technology creates for the nation's power supply. In 1999, the amount of information available on the Internet was roughly 350,000 terabytes per month. By 2003, that figure will reach over 15 million terabytes per month. Today, the Internet, related servers, routers, and

switches are estimated to consume about 10 percent of the electricity in the U.S. Some experts say this figure could reach between 40 and 50 percent by the next decade. This implies that the existence of a reliable electric power supply is critical to the successful operation of any institution, including a university campus.

Another risk is related to the fact that power grids in many parts of the country lack adequate interconnections to provide sufficient levels of redundancy for alternate paths. And even if alternate paths are available, the systems lack the capability to modulate the flow of power among various transmission lines. This is analogous to water flow on parallel pipes without valves to siphon water from a fully loaded pipe to a pipe that is not fully loaded. Today, new electronic devices are being developed to provide such capability and enable the utilities to smoothly switch power among various sources in the event of natural disasters, sabotage, or terrorist attack. However, it will be years before these devices will be installed.

Further, and at a more fundamental level, current electric power distribution systems are designed and built primarily to serve loads required by lighting systems and electric motors. These loads normally require a reliability of 99.9 percent or "three nines." This means they can withstand an interruption of roughly 8 hours per year. Although such disruptions may be acceptable for refrigerators, fans, and other appliances, it does not meet the reliability requirements of a computer server. Most critical electronic equipment, such as computer servers and the Internet, require reliability rates of between "five nine" (99.999%) to "seven nine" (99.99999%). These figures mean that power disruptions would range between 3 seconds to 5 minutes per year, well beyond the capability of most current power systems. Power outages cost a significant amount of money. For instance, the cost of the August 10, 1996, power loss in California was calculated at almost $1 billion. Based on a 1995 study by the Electric Power Research Institute (EPRI), the annual cost of power interruptions in the U.S. is $30 billion. It is projected that the current annual cost is closer to $100 billion.

REDUCING THE RISK OF POWER INTERRUPTIONS

The following two options can be used to reduce the risk of power interruptions and the costs associated with such interruptions.

The first option is to install an Uninterruptible Power Supply (UPS) for critical equipment. With a UPS, the load is powered under normal conditions by the electric utility. When there is a loss of power, the UPS automatically switches from the utility power to its battery system, and no loss of electricity is experienced. This is only a short-term solution that will allow computer systems to safely shut down. However, if there is an emergency generator that can charge the battery system, the operation can continue for as long as desired.

A second option is to install on-site power generation equipment connected to the electrical grid as a distributed generation system. Distributed generation systems (DGS) are a new approach to improving the reliability of power systems for mission critical loads. In traditional

power systems, large electric utility plants generate all electricity and the power is transmitted across long distances using distribution systems to load centers and individual customers. This means that power always flows in one direction: from the utility to its customers. Service interruptions will occur when there are failures at the utility's generating site, or transmission lines.

New technology makes it possible to generate modest quantities of electricity using small units located on the campus. These units are connected individually or through a micro-grid to the electric utility system. One increasingly popular technology is the microturbine. This small generation unit comes in sizes ranging from 30 kilowatts to 75 kilowatts and can work in tandem with the utility power. With proper control circuitry, the microturbine can be isolated from the utility system when power from the utility is lost, and the microturbine will continue to serve critical loads without interruption. Currently, these units can be installed at a cost of about $600 per kilowatt.

WATER DISTRIBUTION AND FLOODING ISSUES

Colleges and universities typically are at risk for damage resulting from two sources of flooding: (a) flooding due to natural causes (large rainfalls, etc.) and (b) leaks and failures in current water supply equipment.

In the first kind of flooding (due to natural causes such as abnormally large rainfalls), water will follow gravity's pull from a higher location to the lowest possible point. If a college campus is situated below the 100-year flood plain, history eventually will itself and that location will be subjected to flooding. As a result, it is important to know the 100-year flood record when planning a new development. Planners and developers can use this information when reviewing site surveys and contours so they can avoid building structures that could be affected by floods. When land costs and other site limitations dictate that structures must be built in flood plain areas, make sure that these structures do not house critical functions and/or programs that use expensive equipment that would be difficult to move and costly to replace.

In many cases, even if a facility is located above a flood plain, there is still the possibility that parts of a facility or infrastructure, such as subterranean floors, utility duct banks, and/or tunnels, could flood. Campus surveys and records of prior flooding problems can be used to identify at-risk locations. Once these locations have been identified, take the following two steps to reduce future risk.

First, make sure a good and well-maintained drainage system is in place to remove water from such areas as quickly as possible. This may require installing submersible pumps powered by an emergency power system. These pumps work automatically using two limit switches. The pump is activated when the water level increases beyond the first limit switch. The pump stops when the water level drops below the second (lower) limit switch. Such equipment is normally connected to an emergency power system, since they are considered part of the facility's critical equipment.

Second, make sure there is a water level detection system in place that can warn campus maintenance staff if water accumulates beyond a certain predetermined level. This detection system usually involves a third limit-switch located on the submersible pump at a higher elevation than the other two switches, but well below the level at which water damage would result during flooding. The high water-level alarm would sound either when the pump fails due to a lack of power or other mechanical or electrical problem, or if the drainage system becomes blocked. In addition, the alarm may sound when water is rising at a rate faster than the pump can handle. At this point, the alarm means that an additional temporary pump is needed to prevent flooding.

The second source of flooding is due to leaks in and sudden failures of the campus' existing water system. This creates the risk of localized flooding in critical areas of the campus, including the (a) potable water distribution system for the campus, (b) chilled water system (for central cooling applications), (c) water sprinkler system (for fire suppression), and (d) condensate return systems (for central heating applications). These systems are normally pressurized, meaning that any sudden pipe burst would result in a large quantity of water being dumped in a localized area during a very small period of time. In addition, there are several gravity flow systems, such as sewer and storm drainage systems as well as drainage pipes from spot coolers and unit air conditioners, that pose flood risks, although flooding would not take place at the same rate of speed as it would from leaks or failures in pressurized systems.

Ensuring good design is an effective way to minimize flood damage from water distributions systems. For example, the impact of floods can be minimized when mechanical engineers consciously plan the routings of water distribution systems away from mission critical areas during the planning stage of a new facility. Additional precautionary steps must be taken when water distribution systems cannot be segregated. One preventive approach is to use waterproofing materials to minimize water intrusion into sensitive equipment and areas. A second approach is to build a secondary containment area for sensitive equipment. This can prevent or at least slow the water intrusion rate. A third technique is to install a series of detection sensors connected to a central monitoring system. These sensors could include measures that combine (a) limit switches to measure water levels, (b) pressure sensors in water lines to monitor sudden pressure drops due to pipe ruptures, and (c) moisture sensing devices to monitor humidity level in cable trays or electronic cabinets.

HEATING, VENTILATION, AND AIR CONDITIONING (HVAC)

Most large buildings have mechanical ventilation systems that bring fresh air into the building for all interior spaces. Based on the outside temperature, the fresh air is heated or cooled before being delivered to the space. To reduce energy costs for office buildings and classrooms during hot and cold days, a large percentage of the air is recirculated and the balance is com-

posed of fresh air. In most cases, the amount of fresh air introduced is roughly 15 to 20 cubic feet per minute per person. In many laboratory facilities and hospitals, no air is recirculated and the building is constantly supplied with 100 percent fresh air to avoid cross contaminations among laboratories and decrease the risk of patient infection.

The fact that buildings are continuously being supplied with outside air creates the possibility that airborne hazards could be introduced into a building either by accident or maliciously. During the past two decades, there have been several incidents of noxious chemicals, hazardous fumes, and foul odors in buildings that have resulted in evacuations, illnesses, injuries, and disruptions in normal building operations. Several articles in professional journals and the popular press have addressed the "sick building" syndrome and what can be done to ameliorate such conditions. The terrorist attacks of September 11th and subsequent anthrax contaminations have prompted facilities managers and university administrators to evaluate the vulnerability of their buildings for such risks.

Some chemicals are noticeable, meaning that gaseous traces could be perceived by humans quite rapidly in the form of smell, respiratory problems, skin irritation, and other signs and symptoms, before they cause serious harm. However, many chemicals cannot be detected before they cause serious health-related problems. Biological agents are mostly imperceptible, and few if any detection devices can identify their presence in a real-time manner. If a highly concentrated chemical is released inside a building, the effect of the chemical will persist for a longer period than had the chemical been released outside, since buildings receive only a limited amount of fresh air to dilute the chemical quickly. If a high percentage of the air is recirculated, the hazardous fumes effect will remain for an even longer period of time. This means that if a hazardous chemical or biological substance is introduced in a building, the effect may remain for a considerable period.

A building is also vulnerable to external releases of chemicals and biological substances based on the number and locations of fresh air intake openings. A smaller amount can enter through cracks and joints, leaky windows, and other means. However, if any airborne hazard is introduced in an air intake system, it will be rapidly transported to all areas of the building. Therefore, it is imperative to evaluate those measures that have been put in place to minimize that potential for the introduction of chemicals and other hazards through the air intakes.

Fresh air intakes are set at ground level in many facilities. These buildings are more susceptible to foul play and malicious acts. As a result, campus security should patrol these areas and watch for any unusual activity. In the case of critical facilities, the installation of surveillance cameras is recommended. Air intakes should be screened on an outward sloping angle so foreign materials would roll off and outward and could not easily be introduced into the air system. For new construction, air intakes should be elevated to make them less accessible to unauthorized individuals.

Another area where hazardous materials could be introduced into the air distribution system is the mechanical room. For this reason, ensure that all mechanical rooms are locked and that access to these spaces is limited to authorized staff.

Three additional building areas vulnerable to the release of hazardous materials and worthy of special attention are the entrance lobby, mailroom, and receiving area. These are places where an outsider could deliberately introduce hazardous substances. As a result, these spaces should be on separate air handling systems that are isolated from the rest of the building. In addition, the entry points of a building should be under negative air pressure. In this way, any hazardous substance introduced in that area will be contained and will not impact the rest of the facility.

MANAGING HAZARDOUS MATERIALS IN FACILITIES

Federal and state governments over the past 30 years have promulgated a plethora of rules and regulations addressing the handling, labeling, and disposing of chemicals and radioactive materials. University campuses contain literally tens of thousands of these substances. In addition to the risks created by the presence of these hazardous substances, there are also serious legal and monetary risks involved when colleges and universities fail to comply with the rules and regulations concerning their management. These risks include fines and penalties as well as civil and/or criminal prosecutions. An examination of actions taken by the Environmental Protection Agency (EPA) over the past 10 years shows a steady increase in the number of penalties levied against colleges and universities. The number of criminal penalties has grown at an even faster rate as universities risk losing research funding from federal, state, and other sources if they violate these rules and regulations. In addition, they face restrictions on their academic freedom and can be subjected to adverse publicity. These factors contribute to the degrading of the university's reputation.

Colleges and universities have three options for addressing the management of hazardous materials:

- *Ignore Environmental Laws:* In this scenario, the organization and its management team in all probability will eventually face civil and/or criminal penalties. Clearly, this option is not sustainable in the long run. The continued failure to comply with federal, state, and other rules and regulations increases the probability of accidents that may damage the environment and jeopardize the safety of campus students, faculty, and staff.
- *Phase Out Chemical Usage:* This may mean eliminating almost all lab research activities in the natural sciences and several fields in engineering. This decision would not only threaten a university's academic freedom, but also would severely impact the quality of these programs.
- *Develop a Conformance Strategy:* This means developing a systematic process that

is preventive, detective, and corrective in nature, and aimed at achieving compliance with all environmental laws. This action lays the foundation for an environmental management plan that addresses the environmental aspects of an enterprise. It also enables the organization to control the impact of its activities. This is the best way for colleges and universities to manage hazardous materials.

ENVIRONMENTAL MANAGEMENT SYSTEM (EMS)

An environmental management system addresses the risks associated with chemicals under normal and emergency conditions. At its core is the environmental policy of the organization. The environmental policy should be established and supported by senior leadership. It should be relevant to the nature, scale, and potential environmental impacts of all activities of the university covered by environmental, legislative, and regulatory requirements. The policy must provide a framework for setting environmental objectives and achievable targets. It should commit the institution to continual improvement and reflect the institution's values concerning environmental management. Finally, the policy must be communicated to all employees.

Four basic components support the environmental policy: (1) planning, (2) implementation and operation, (3) auditing and corrective action, and (4) management review.

Planning

Planning involves developing a model that helps faculty and staff deal with hazardous chemicals and identify early on the potential environmental issues inherent in teaching courses and research projects that involve hazardous materials. This includes identifying gaps between legal requirements and environmental aspects of related activities, and developing targets and objectives that will constitute the basis for the environmental management program.

Implementation and Operation

The implementation and operation phase entails two distinct but interrelated activities. The first activity involves a three-step process. First, review all physical processes that may potentially impact the environment. Examples of such processes are grounds management, vehicle repair and maintenance, painting, power generation, and custodial services. Second, identify the inputs and outputs of these processes. Typical inputs for such processes are coal, fuel, paint, and hazardous chemicals. Typical outputs include solid waste, hazardous waste, air polluting emissions, and waste water. Create a database containing all chemical substances with their appropriate Materials Safety Data Sheets (MSDS). Third, evaluate these outputs and identify those with a negative impact. Then, review all legal and other regulatory issues concerning those outputs carrying the risk of significant environmental impact.

The second activity is undertaken after the first has been completed, and involves identifying the desired environmental competency elements for faculty, students, and staff con-

cerning processes with negative environmental impact. Then, develop a training program to educate all individuals who handle chemicals. In addition, create procedures to control all environmental activities and communicate these procedures to those who handle these substances.

Auditing and Corrective Actions

In this stage of the process, compare the measures and targets established during the planning stage to determine whether the actual conditions are in conformance with prior projections. If targets are not being met, devise action plans to ameliorate the condition. In addition, identify action items to prevent non-conformance in the future. Finally, record all findings for future reference.

Management Review

The overall effectiveness of an environmental management system should be assessed on a periodic basis. Make any changes required to align the program with the environmental policies of the enterprise.

CONDUCING AN IMPACT EVALUATION

After reviewing all processes and determining their environmental impacts, evaluate the extent and consequences of each impact. This involves determining the scale and severity of the impact, the probability of occurrence, and the duration of the impact. In addition, the evaluation should address business considerations such as potential regulatory impacts, costs associated with and difficulty of changing the impact, consequences involved in changing the process, and the possible impact on public image. Recognize that although negative environmental impacts generally receive more attention, some processes might have positive impacts, and both should be noted. The next step is segregating the impacts into two groups: minor and significant. The goal here is to help focus efforts on the "significant few rather than trivial many." Any impact that carries a regulatory compliance dimension is classified as significant. Finally, concentrate on mitigating the risk of significant impacts as quickly as possible.

BENEFITS OF AN ENVIRONMENTAL MANAGEMENT SYSTEM

An Emergency Management System (EMS) creates a framework for addressing environmental issues in a systematic manner. The value of an EMS is even more important now, given the USA Patriot Act. In addition, an EMS will help colleges and universities:

- reduce environmental regulatory and compliance costs;
- reduce environmental liabilities, potential fines, and citations from compliance agencies;
- reduce waste generation and protect the environment;

- enhance the institution's public image;
- help the institution accomplish its mission; and,
- enable managers to fulfill their roles and responsibilities.

NEW TECHNOLOGIES FOR BUILDING SAFETY

Many new technologies currently available or under development are designed to continually monitor utility distribution systems and provide valuable monitoring information on a real-time basis. Some researchers are working on developing technologies that will incorporate redundancies for systems in high-rise buildings.

One idea under consideration is the development of additional means of egress besides the stairwell. Here, researchers are investigating the feasibility of incorporating vertical chutes built from reinforced concrete and coated with heat resistant material to be used for emergency evacuation. Another research project is investigating the feasibility of embedding a large number of wireless sensors in the physical structure of large buildings. Theses sensors would serve as *de facto* smart bricks. If part of the building were damaged during an emergency, the remaining sensors would provide valuable data on the condition of the remaining structure, indicating, for example, whether the building is safe to re-enter or if the structural damage has placed the building in eminent danger.

SUMMARY

As you can see from the topics covered in this chapter, the risk to facilities is becoming a major area of concern for colleges and universities on several fronts. The first set of concerns deals with the need for more dependent infrastructures, such as more reliable power systems as opposed to the current capability of these systems. The second major area is having comprehensive management practices in dealing with hazardous materials and what to do in case of an emergency. The third major area is new security challenges that campuses face since the September 11th attacks. Some new monitoring technologies can assist us in reducing the campus exposure levels. The important factor to recognize is that no amount of new technology can substitute for sound management practices to actively identify these risks, determine their impacts, and take the necessary steps to address these issues. Lack of adequate care will prove to be a very costly option in the long run.

REFERENCES

Alonso, Felipe. "Managing Business Continuity," E-Business Advisor, http://Advisor.com/Aricles.nsf/aid/SMITT566.

Andrews, J.D. and Moss, T.R. *Reliability and Risk Assessment,* Longman Scientific & Technical, Essex, UK, 1993.

Association of Higher Education Facilities Officers. *Emergency Preparedness,* Alexandria, VA: APPA, 1992.

Bignell, Victor and Fortune, Joyce. *Understanding System Failures.* Dover, NH: Manchester University Press, 1984.

Bjelke, Sten. "The Nature of Business Risk," *IT Audit,* Vol. #2 December 1, 1999, http://www.theiia.org/itaudit/index.cfm?fuseaction=print&fid=236.

California State University Northridge, *Campus EMERGENCY Management Plan,* Northridge, CA, Revised September 1998.

Charles E. Schumer Presentation to New York City Summit, September 22, 2000, http://www.cio.gov/Audit_Summit/09-22-00/Schumer.htm.

Clark, Robert N. "Risk-Based Departmental Audits," *College & University Auditor,* December 2001, pages 12-15.

Critical Infrastructure Assurance Office, "White Paper on Critical Infrastructure Protection," May 1998, http://www.ciao.gov/CIAO_Document_Library/paper598.htm.

Dames & Moore, "The Northridge Earthquake January 17, 1994," A Special Report by Dames and Moore, Los Angeles, 1994.

Defense Systems Management College, *Systems Engineering Fundamentals,* Fort Belvoir, VA: DSMC Press, October 1999.

Foster, Harold D. *Disaster Planning.* New York: Springer-Verlag, 1980.

General Accounting Office, *Executive Guide: Information Security Management,* GAO/AIMD-98-68, May 1998.

General Accounting Office, *Information Security Risk Assessment: Practices of Leading Organizations,* GAO/AIMD-00-33, November 1999.

Hewlett Packard Services, "Why Business Recovery?" http://www.hp.com/hps/brs/learn_why.htm.

MARSH, "Helping Employees Cope With Disaster," *The New Reality of Risk,* Vol. 1, Issue 6, October 26, 2001.

McGraw, Karen and Harbison, Karen. *User-Centered Requirements: The Scenario-Based Engineering Process,* Mahwah, NJ: Lawrence Erlbaum Associates Publishers, 1997.

Monaco, Frank. "IT Disaster Recovery Near the World Trade Center," *EDUCAUSE Quarterly,* Number 4, 2001, pages 4-7.

Qayoumi, Mohammed. *Electrical Distribution Maintenance,* Alexandria, VA : APPA, 1989.

Ross, Nicole. "Are You Covered?" *Contingency Planning & Management,* November 2001, pages 22-25, http://www.contingencyplanning.com/article_index.cfm?article=407.

Toigo, Jon W. *Disaster Recovery Planning.* Upper Saddler River, NJ: Prentice Hall, 2000.

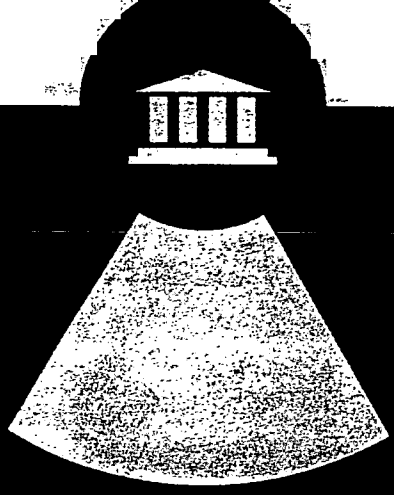
USA Patriot Act of 2001, Library of Congress, http://thomas.loc.gov/cgi-bin/query/z?c107:h.r.2975:.

USA Patriot Act Self Assessment Questionnaire, Department of Environment Health and Safety, MIT, http://web.mit.edu/afs/athena.mit.edu/org/e/environment/programs/pdf/Questionnaire.pdf.

Van Grop, John and Westbrock, Bill. "Powering the New Digital Economy: How Enterprise Energy Management Systems Help Maximize Power Reliability," Power Management Ltd., August 29, 2001.

Vulpitta, Richard T. *On-Site Emergency Response Planning Guide.* National Safety Council, 2002.

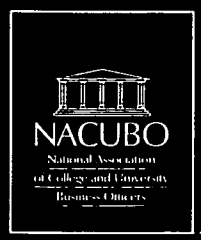
Zonis, Beth. "Business Continuity for Critical Enterprise Applications," *Contingency Planning & Management,* November 2001, pages 26-29, http://www.contingencyplanning.com/article_index.cfm?article=408.



About the Author

MOHAMMAD H. "MO" QAYOUMI is vice president for administration and finance and chief financial officer at California State University, Northridge. He is also a tenured professor at the Department of Manufacturing Engineering and Engineering Management. He has a bachelor's degree from American University of Beirut in electrical engineering, MS degree in nuclear engineering, MS degree in computer engineering, Ph.D. in electrical engineering, and an MBA in finance from University of Cincinnati. He is a licensed professional engineer and a certified management accountant.

Mo has over 25 years of industrial and higher education experience. He has published more than 65 articles, seven books, and several chapters in various books and has made presentations at many conferences across the U. S. and internationally on various topics in the areas of quality, energy, and systems theory. Mo is a senior member of the Institute of Electrical and Electronic Engineers (IEEE). He also served as a Malcolm Baldrige National Quality Award examiner from 1998 to 2001 and as a senior examiner for Missouri Quality Award Program from 1997 to 2000. Mo currently serves as the chair of the California State University Risk Management Authority (CSURMA).



Published by NACUBO, 2002
National Association of College and University Business Officers
2501 M Street, NW
Washington, DC 20037-1308

NC3026

U.S. Department of Education
Office of Educational Research and Improvement (OERI)
National Library of Education (NLE)
Educational Resources Information Center (ERIC)

NOTICE

Reproduction Basis

X	This document is covered by a signed "Reproduction Release (Blanket)" form (on file within the ERIC system), encompassing all or classes of documents from its source organization and, therefore, does not require a "Specific Document" Release form.
	This document is Federally-funded, or carries its own permission to reproduce, or is otherwise in the public domain and, therefore, may be reproduced by ERIC without a signed Reproduction Release form (either "Specific Document" or "Blanket").