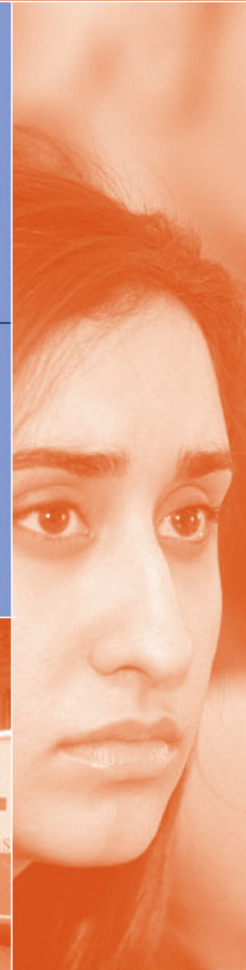


EMERGENCY PLANNING

DISASTER AND CRISIS
RESPONSE SYSTEMS FOR
JEWISH ORGANIZATIONS



DISCLAIMER & LICENSE

© 2003-2005 United Jewish Communities.

This publication is intended to help institutions become aware of basic emergency planning considerations. It is not intended to provide comprehensive, institution-specific advice on any aspect of emergency planning nor is it meant to replace the advice of a professional in the appropriate field (e.g., emergency planning, law, building safety). Some of the topics discussed in this publication are subject to federal, state/provincial and/or local codes and regulations. This publication does not provide a universal guide for regulatory compliance. The material is being provided for educational and informational purposes only, without representation, guarantee or warranty of any kind, and it should not be construed as professional advice. United Jewish Communities, the Jewish Community Relations Council of New York, Anti-Defamation League, John Jay College of Criminal Justice and the authors are not responsible for any injury, loss or damages to persons or property arising from the use or misuse of this information.

This publication is not in the public domain. The use of this publication is limited to licensees as set forth herein. Licensees may use, reproduce or distribute this publication within their organization, but no licensee shall put, display, link or make available this publication or any of its contents on any internet web site. Licensees shall not distribute this publication or any portion thereof without this disclaimer and license agreement. Licensees shall not modify, publish, transmit, transfer, sell, create derivative works from, display or in any way exploit any of the contents, in whole or in part, except as otherwise expressly permitted.

*

The authors welcome all comments and suggestions. If you have any, please call David M. Pollock at (212) 983-4800, ext. 132 or E-mail them to pollockd@jcrcny.org.

MANY OF THE PHOTOGRAPHS USED ON THE COVER COURTESY OF THE FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA), U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C. 20472.

CONTENTS

Preface.....	5
Introduction	7
Don't Be Overwhelmed	11

THE BASICS

Hazard and Risk Analysis.....	14
Plotting Scenarios	19
Response Teams	24
Implementing Your Emergency Plan.....	40

PROTECTION STRATEGIES

Evacuation Tactics	51
Sheltering-in-Place & Lockdowns.....	65
Duck, Cover & Hold	72
Hurricanes and Tornadoes	77
Suspicious Objects, Bombs and Bomb Threats	81
Bomb Incident Strategy.....	84
Security Planning	93

MANAGERIAL AND ADMINISTRATIVE CONSIDERATIONS

Managing Risk and Liability.....	98
Insurance Considerations	102
Creating and Implementing Policies and Procedures.....	107
Mutual Aid and Assistance.....	111

APPENDICES

Hazard Analysis Worksheets	117
Emergency Communication Tactics	139
Power Outage Tips.....	144
Supplies and “Go Kits”	147
Special Events	156
Persons with Disabilities.....	161
Staff and Clientele During and After Crises	163
Preparing Your Building for Airborne Chemical, Biological or Radiological Attacks	166
Dealing with the Media During Crises	171
Data and Document Preservation.....	174
Guidelines for Hiring a Security Contractor	179
Criteria for Security Contractor Selection Checklist.....	189
Emergency Procedures for Sabbath and Religious Holidays.....	190
Houses of Worship & High Holidays	191
Glossary of Terms	195
Authors.....	200

PREFACE

History teaches us that disasters and crises occur and the history of our people tells us that we are capable of overcoming them. The Jewish community faces the same hazards that challenge our neighbors, such as fires, storms or floods. The sobering realities of terrorism both at home and abroad mandate that we remain ever vigilant and take the prudent steps to protect our Jewish institutions. There are many hazards – both natural and man-made. No matter what steps we have already taken to prepare and respond, we can always do better.

Hurricanes Katrina and Rita taught us a new dynamic – disasters can have a regional impact on our agencies, houses of worship and schools. Mutual cooperation among organizations has been both necessary and beneficial. For the most part these relationships developed on an *ad hoc* basis. If we plan we probably can do even better.

This work is not just about extreme catastrophic situations. There are so many other types of events that can and will arise that it just makes good sense for all Jewish organizations to plan ahead. This manual will give you significant guidance and recommendations to prepare for a great many of these possibilities. It also covers how to engage in cost-effective emergency management and how to mitigate losses to the organization while continuing to provide safety to your employees and service to your communities.

United Jewish Communities (UJC) sought experts in the fields of crime, disaster, crisis and emergency response to bring you this framework and template upon which to build concrete plans for the avoidance of and response to extraordinary—and not so extraordinary—circumstances. The issues presented in this manual are to be taken seriously, and the solutions are to be laid out methodically and carefully.

The real key to making this planning effort both successful and manageable is to make it yours. Think of this manual as your community’s personal “Emergency Planning Toolkit.” Each institutions’s facilities, assumptions, staff and resources are different. Many of your solutions will be different as well. This manual is designed to help you anticipate possible situations and risks, break them into their various components, and develop strategies and tactics for your “response teams.”

Remember: These situations are far easier to handle and overcome when contingencies have been thought through under less stressful circumstances and possible responses have already been put in place.

United Jewish Communities and the Conference of Presidents of Major Jewish Organizations have recently established the Secure Community Network (SCN). Conceived

and launched to address the need for better coordination and the dissemination of timely and accurate information about security concerns, SCN is an important first step toward a more secure, connected Jewish community. To learn more about SCN go to their website, [http:// www.scnus.org](http://www.scnus.org).

This manual was a cooperative effort. We wish to express our deepest appreciation to all of the members of the UJC Emergency Committee for their energy, support and funding of this effort, with a special acknowledgment to Barry R. Swartz, UJC Senior Vice President, who guided this effort along with Jonathan Lichter, Rabbi Eric Lankin and Karen Feingold. Tremendous thanks go to the leadership of the Jewish Community Relations Council of New York: Ezra G. Levin, President, Sally Goodgold, Chair, JCRC Commission on Jewish Security and Michael S. Miller, Executive Vice President and especially to David Pollock, who was the project manager and principal author of the manual; Marcia R. Eisenberg and Jennifer Glick. The faculty and staff of the John Jay College of Criminal Justice: particularly Gerald W. Lynch, President Emeritus, Jeremy Travis, President, Lawrence Kobilinsky, Associate Provost, Professors Norman Groner and Bob Loudon provided us with critical support, guidance and direction. We also thank the ADL for their expertise and contributions.

Richard Katz of the JFMC Facilities Corp, Martin J. Hertz of Morrison Cohen Singer & Weinstein, LLP; Dana Friedman of Dragonfly Technologies, Gerard McCarty of the National Preparedness Division of FEMA, Region II, Claire B. Rubin of Claire B. Rubin & Associates and George Washington University Institute for Crisis, Disaster and Risk Management, Howard Feinberg and Lauri Kravetz Cohen of UJC Consulting and Bert J. Goldberg of the Association of Jewish Family & Children's Agencies read the manuscript and made invaluable comments and suggestions. Their input was both welcome and helped to improve this work. Any errors are solely the responsibility of the authors.

UJC is certain that you will find this guide to be an extremely useful set of tools. While it comes to you in large part because our world is getting more dangerous, let us hope and pray that better times are ahead. This is one of many ways that we can do our part to ensure the safety and security of our own communities. To be sure, *kol yisrael arevim ze baze*h—this is our responsibility to one another.

Robert Goldberg, Chair, Board of Trustees, UJC

Carol Smokler, Chair, Emergency Preparedness Committee, UJC

Howard M. Rieger, President and CEO, UJC

INTRODUCTION

Hurricanes Katrina and Rita and the horrors of September 11th tragedies and disasters of historic proportions. Today, when the need for emergency planning is discussed too many worry about similar major, catastrophic occurrences. True, terrorism remains a looming issue and many experts expect it to get worse before it gets better. But by focusing on such mega-events it's easy to become paralyzed.

Yet man-made disasters are far less likely than natural ones. Tornadoes, blackouts, fires and even water-main breaks occur on a regular basis. So do micro-events such as layoffs, a sexual harassment charge or the death of a beloved teacher. Any one of these can have a detrimental impact on your organization. Consider:

- How does an agency placing home care attendants provide coverage for its at-risk clients during a blizzard?
- If a staff member is accused of abusing a minor, what should be your agency's next step?
- A senior citizen housing complex is in the path of a hurricane. How and where do you move the residents?
- If buses bringing campers home are involved in a highway accident and children are sent to the emergency room, how does the camp respond to the authorities, the campers and their parents?
- After construction workers start a catastrophic fire destroying a landmark synagogue does the congregation have insurance sufficient to rebuild? Where do they meet in the meantime?

Each of these examples is taken from reality. Each involves an emergency, disaster or crisis. Lives can be lost or people injured. Depending on how the affected organization handles the situation, its reputation can be tarnished or enhanced. And an effective response to each of these micro-events can be a major component of mega-event planning. Emergencies, disasters or crises can, and will, happen, but many negative consequences can be mitigated.

One consideration is expense. Disasters caused by natural hazards have become increasingly costly. From 1989 to 1993, the average annual loss from natural disasters was \$3.3 billion nationally. Over the next four years, that average increased to \$13 billion annually. More importantly, since 1975 over 6,000 people have been killed and over 50,000 people injured in natural hazard events. Emergency systems can, and do, save lives.

QUICK TIP

Don't become paralyzed. Emergencies, disasters or crises can, and will, happen, but many negative consequences can be mitigated.

Why don't we do more planning?

Noah learned: When you hear the thunder, it's too late to build an ark. Jewish history teaches us that when we're pessimistic we usually won't be disappointed. We should be anticipating disaster.

By their very nature, not-for-profit organizations are stretched to the limit. It's hard enough for executives and boards to get to the critical items on their daily to-do lists. It's only natural to think that emergencies will never happen to us or that we can handle whatever is thrown our way. Though not as inevitable as death and taxes, crises will strike. But, our world has changed. If nothing else, it's become a more dangerous place.

Having formal, well-thought-out emergency plans will facilitate an organization's reaction to and recovery from adversity. Planning can help to identify leadership and provide guidance. Emergency systems include a training component. Emergency systems can help to minimize the loss of life and injury and reduce property loss. Emergency systems can help to erect disruption defenses so that an organization can return to its mission and serve its clients as quickly as possible.

QUICK TIP

The phases of emergency planning: Preparedness/mitigation, response and recovery. All focus on safety, stability and the continuity of mission-critical services.

Mapping the plan

Through the emergency planning process, planners should focus on 1) the safety and well-being of employees and clientele, 2) their agency's financial stability and 3) their ability to provide mission-critical services.

The many tasks and functions of emergency management may be summarized as a cycle. Organizations prepare for emergencies and disasters, respond to them when they occur, help people and institutions recover from them and mitigate their potential effects to reduce the risk of future loss.

Preparedness ensures people are ready for a disaster and respond to it effectively. Preparedness requires analyzing what you'll do if essential services break down, developing a plan for contingencies and practicing the plan. The key component of preparedness-planning is life-safety concerns. Another is redundancy. Insurance, covering both replacement and business continuity can ultimately help with recovery.

Response begins as soon as a disaster is detected or threatens. It involves search and rescue; mass care, medical services, access control, and bringing damaged services and systems back on line.

Recovery, or rebuilding after a major disaster, can take years. In communities, services, infrastructure (utilities, communication and transportation systems), facilities, operations, and the lives and livelihoods of many thousands of people may be affected by a disaster. Even if your organization continues to function in the shadow of disaster, its reputation could suffer and take years to recover.

Viewed broadly, the goal of all *mitigation* efforts is *risk reduction*. The emphasis on sustained actions to reduce long-term risk differentiates mitigation from preparedness and response tasks, which are required to survive a disaster safely. Mitigation is an essential component of emergency management. Effective mitigation actions can decrease the impact, the requirements and the expense of a hazard event.

Your emergency planning process will create emergency systems that touch on the entire disaster cycle. You will have to identify the emergency leadership teams, put communication system and backups into place, determine policies and procedures for a wide range of disasters, schedule rehearsals for various scenarios and evaluate what you have done in order to improve your plans.

Organizational leaders will have to set priorities and devote resources to ways to address all of these issues simultaneously. The process is not an easy one. To be effective you must convince people to “buy in.” In differing ways everyone—from the board chair to the custodial staff—is involved.

QUICK TIP

Create emergency systems with leadership teams, communication systems, supplies and backups for a wide range of possible disasters.

How to use this manual

This manual may seem overwhelming, but it’s not. No one expects you to sit down and read the whole thing at once.

“*The Basics*” section will provide the basic tools and background for developing your emergency plan. First, anticipate what might happen through hazard analysis. This is the process of assessing which risks could conceivably have an impact on your organization. Once the possible risks are identified, the process helps the emergency planners to match available resources to the risks. Next, figure out how hazards can affect your organization by plotting scenarios—narratives describing plausible, worst case situations. By asking “what is the plausible worst-case scenario?” The team can develop a wide range of responses to disasters and crises. Finally, drills and exercises will help you perfect your emergency responses. With these basic skills and tools planners can build their prevention, preparedness, response and recovery systems.

“Protection strategies” will help you react to life-threatening emergencies. Simply put, in dangerous situations people have to be moved out of danger or sheltered from danger in some way. Evacuations move people from a dangerous location to one of comparative safety. Sheltering-in-place and lockdowns are used when the greater danger is external. Duck, cover and hold is an interim tactic for earthquakes. Together, these are the basic protection strategies.

The goal of the *managerial and administration* section is to help you to put in place the basic organizational structure to help to mitigate emergencies. Many such issues, such as managing risk, insurance or personnel policies, are not simply operational and should be developed in consultation with your Board.

Finally, the *Appendix* contains information for very specific situations.

Neither a borrower nor a lender be

Your sister organization might have a very good emergency plan, but it may not be applicable to your situation. Buildings and staffs are different. Their plan is not likely to work for you, even if you fiddle with it.

While elements of the processes are similar (e.g., many of the components of risk analysis), each organization should go through the process itself. Only then will the logic behind the plan be clear. In an emergency you will be able to “roll with the punches” and adapt the plan as needed. You will know your resources and your capabilities.

Changing the culture

It often seems that our world changed. Major hurricanes and warnings from Homeland Security reinforce the idea that emergencies, disasters or crises can strike anyone, anytime and anywhere. This manual will assist in the preparation of an emergency system to guide you when immediate action is necessary.

And remember. It’s not just the mega-events. You should be planning for the dozens of micro-events that can seriously challenge your agency, your mission and services to your clients. If you have those covered you will have gone a long way toward planning for appropriate responses for even the mega-events.

QUICK TIP

Protection strategies:

Moving people out of danger, e.g., evacuations, or shielding them from danger, e.g., sheltering-in-place.

DON'T BE OVERWHELMED

Few organizations have the luxury of having full-time emergency planning staffs. Emergency planning stretches the resources of any endeavor. To make matters worse, you're a nonprofit, stretched thin and battered by the challenges of fund raising, declining revenues and other complexities of the environment. Emergency planning is not an easy process. Whether your agency is large or small, you must start somewhere. As usual, you should focus on high priority issues.

You will learn that our key priority is "life safety." First, concentrate on steps that can save lives. We will tell you how to build "response teams." Fortunately, you probably already have the initial framework of a response team in place—your fire/safety warden, deputy wardens and searchers. Those people should know what to do in case of fire. They can also be prepared to spring into action in the event of other emergencies. Your fire drill team can be the foundation of your response team.

This fire drill structure is in place because your local authorities mandate fire drills. Fires are one of the most common hazards, but what other hazards will you likely experience? Those in Alberta probably can forget about hurricane preparations while residents of Miami shouldn't spend much time planning for blizzards.

Most of the [hazard analysis](#) (P. 14) component of your emergency planning process should be available from your local government emergency management office. You don't have to reinvent the wheel. Identify the most likely hazards and develop variations of your basic response team appropriate to those hazards.

Early in your planning process you should customize your response team so that it can effectively deal with the various [protection strategies](#) (P. 50) like evacuation, lockdowns and sheltering-in-place.

Once you've identified hazards and put your basic response team in place, define your mission-critical issues. For example, if you deliver food to the frail elderly, you can't simply shut down during a blizzard or a blackout. Some, if not all, of your clients rely on you for their meals. You must have a way of preparing and distributing the food. Such issues define the second tier of priorities (after life-safety).

BASIC STEPS

1. *Identify life-safety priorities.*
2. *Compile a list of hazards.*
3. *Build your response teams to deal with protection and other strategies.*
4. *Identify and plan to carry out mission-critical functions.*
5. *Refine and review.*

While you are engaged in these activities you can try to look at the [managerial/administrative](#) (P. 97) aspects of planning. Most of these are not so esoteric, rather they are sound business practice. Can you get a member of your board to work on an insurance review and another to draft an employee handbook? Your accountant should recommend appropriate financial controls. Can your office manager gather and copy critical corporate documents for off-site storage? None of these tasks are themselves overwhelming.

As you put these steps together you should test your plans through drills and exercises and make the necessary revisions and refinements.

The bottom line is that anything that you do to protect your staff, your clients and your institution is important. If you can minimize injury and loss of life by planning, every second spent on planning will have been worthwhile.

The authors have tried to make your life easier. Almost every page has a tip or basic concept highlighted so that you quickly find the issues you need to read about. This manual has internal hyperlinks to other chapters and external ones to sources rich with further information.

Good luck and keep safe!

THE BASICS

“The Basics” section will provide the basic tools and background for developing your emergency plan. First, anticipate what might happen through hazard analysis. This is the process of assessing which risks could conceivably have an impact on your organization. Once the possible risks are identified, the process helps the emergency planners to match available resources to the risks. Next, figure out how hazards can affect your organization by plotting scenarios—narratives describing plausible, worst case situations. By asking “what is the plausible worst-case scenario?” The team can develop a wide range of responses to disaster and crisis. Finally, drills and exercises will help you perfect your emergency responses. With these basic skills and tools planners can build their prevention, preparedness, response and recovery systems.

HAZARD AND RISK ANALYSIS

What is a hazard?

Things happen, often with the potential for danger or damage. Some hazards are generic and inherent to the operation of virtually all organizations: severe weather, the possibility that a visitor will slip on a wet floor, that an employee will embezzle the agency's funds or that a former employee will allege violation of his civil rights. Other hazards are unique to your organization—the possibility of animal bites, drowning, vehicular crashes or copyright infringements.

HELPFUL TIP

You're not alone. Contact your local emergency management office or police to find which hazards they consider, then proceed from there.

What is a risk?

Simply speaking, a risk is any uncertainty about a future event that threatens your organization's ability to accomplish its mission. A risk is simply the possibility that a hazard can occur, your organization's vulnerability to that risk and its impact on your organization.

How does the puzzle fit together?

Midwesterners don't spend a lot of time worrying about tsunamis, but they are usually concerned about the possibility of tornados. Californians devote significant resources to earthquake preparedness. Piecing together hazard and risk is a critical component of the emergency planning and preparedness process.

Getting help

This manual isn't your only resource. The emergency planners at your local or state emergency planning office can help.¹ They know the natural hazards affecting your region and other broad-based dangers. They should be one of your first stops. Web sites such as <http://www.cbsnews.com/digitaldan/disaster/disasters.shtml> list links to a wide variety of disaster-related information.

¹ For contact information on state offices try the FEMA web site: <http://training.fema.gov/EMIWeb/IS/is1951st.asp>

What is risk management?

Risk management provides strategies, techniques, and an approach to recognizing and confronting any threat faced by an organization in fulfilling its mission. Risk management may be as uncomplicated as asking and answering three basic questions:

- What can go wrong?
- What will we do (both to prevent the harm from occurring and in the aftermath of an “incident”)?
- If something happens, how will we pay for it?

Large organizations may have a risk management department responsible for answering the three basic questions. In addition, the department may manage litigation, coordinate safety programs and undertake the complex analyses required to set monetary reserves for future claims. In small, community-based nonprofits, the risk management function is more likely to focus on issues such as:

- Screening volunteers to protect children from harm;
- Checking motor vehicle records for all staff and volunteers who are driving on the nonprofit’s behalf;
- Developing board orientation and training materials;
- Coordinating the development and consistent use of employment practices; and
- Negotiating the availability of bank credit and purchasing property and liability insurance.

HELPFUL TIP

While everyone experiences dangers, hazards and risks organizations can learn to manage them.

Developing a Risk Management Program

Establish the purpose of the risk management program.

The first step is to determine your organization’s purpose for creating a risk management program. The program’s purpose may be to reduce the cost of insurance or to reduce the number of program-related injuries to staff members. By determining its intention before initiating risk management planning, your agency can evaluate the results to determine its effectiveness. Typically, the executive director of a nonprofit, with the board of directors, sets the tone for the risk management program.

Assign responsibility for the risk management plan

The second step is to designate an individual or team responsible for developing and implementing your organization's risk management program. While the team is principally responsible for the risk management plan, a successful program requires the integration of risk management within all levels of your organization. Operations staff and board members should assist the risk management committee in identifying risks and developing suitable loss control and intervention strategies.

Insurance and Risk Management

For most nonprofits, insurance is a valuable risk financing tool. Few agencies have the reserves or funds necessary for complete self-insurance of their exposures. Purchasing insurance, however, is not synonymous with risk management. In the nonprofit sector, practicing risk management is living the commitment to prevent harm. In addition, risk management addresses many risks that are not insurable—such as the potential loss of tax exempt status, public goodwill and continuing donor support.²

QUICK TIP

Insurance covers the financial aspects of many risks, but others are not insurable. Those, too, must be managed.

The Role of the Risk Management Team

The risk management committee oversees the execution of the five-step risk management process:

Acknowledge and identify hazards.

The operation of every nonprofit involves some degree of risk or uncertainty about future events. The first step in managing those risks is to identify them. No matter how improbable a hazard may seem, if you can envision it happening in your organization, you should list it during the first stage of the risk management process.

Evaluate and prioritize risk.

Through risk analysis the team assesses the probability of each hazard becoming reality and estimates its possible effect and cost to the agency.

² For more information about developing a risk management program in a nonprofit organization, see *Mission Accomplished: A Practical Guide to Risk Management for Nonprofits*, published by the Nonprofit Risk Management Center, 1999.

Hazard Types

Hazards come in many forms. For the purposes of this manual we identify eight risk categories (see [Hazard Analysis Worksheets](#) (P. 117) in the Appendix):

1. Terrorism
2. Natural hazards
3. Financial operations
4. Legal
5. Misconduct by employees, clients or volunteers
6. Activities and services
7. Property loss
8. Technology

An organization should consult with local emergency management officials, look at its past accidents and near misses and check with similar nonprofits in developing probability and cost estimates. FEMA has a local map utility available at <http://www.esri.com/hazards/>. The utility shows a wide variety of historic hazards for your area. Also consider the possible public reaction to an adverse event. Priority areas of concern will include those risks that are most likely to occur and are expensive when they do happen—such as an accident or water-related injury at a community pool. Lower priority risks are those that seldom occur and are not likely to cost as much when they do happen—such as a slip in the agency’s well-maintained offices.

QUICK TIP

Risk strategies: avoidance, minimization, retention and sharing

Risk Management Strategies

Decide how to manage your risks using risk management strategies. Your next task is to develop a written plan. The plan outlines how the agency will manage its major risks. The plan describes the suggested strategy or combination of strategies that the nonprofit will employ. The four basic strategies for controlling risk are:³

Avoidance

Choosing not to offer or ceasing to provide a service or conduct an activity considered too risky. If *non-essential* programs are too risky it is best to terminate them. It is virtually impossible for an organization to be the target of a child abuse charge if it offers no services to children. However, elementary schools with a core-mission of educating children don’t have a choice.

³ Practical examples of risk management strategies can be found in the [Managing Risk and Liability](#) (P. 98) section of this manual.

Minimization

Also known as risk reduction. Changing the activity so that the chance of harm occurring and impact of potential damage are within acceptable limits. Implementing sound policies and procedures (See [Creating and Implementing Policies and Procedures](#), P. 107) tend to reduce exposure to risk. So do emergency plans.

Retention

Accept all or a portion of the risk and prepare for the consequences.

Sharing

Consider sharing the risk with another organization. Examples of risk sharing include mutual aid agreements with other nonprofits, purchasing insurance and sharing responsibility for a risk with another service provider through a contractual arrangement.

Note: In traditional risk management texts, the purchase of insurance and use of contractual arrangements to allocate risk are categorized as methods of “risk transfer.” This term is misleading, however, as it is virtually impossible for a nonprofit to fully transfer risk. For example, when a nonprofit purchases a general liability policy, the insurance carrier agrees to defend and pay for losses incurred by the nonprofit for certain causes of loss. The insured nonprofit, however, retains risk for the loss of its reputation in the community and reductions in the pool of volunteers available to serve the organization. No currently available contract of insurance will restore a damaged reputation or replenish a pool of capable and enthusiastic volunteers.

PLOTING SCENARIOS

Most managers naturally handle minor emergencies well. Major emergencies require planning and preparations. By focusing on plausible worst-case scenarios, the emergency planning team can prepare for most similar situations that are “not so bad.”

Every building faces the hazard of fire. There are also security issues. The first basic tool, hazard analysis, identifies the fact that your organization, the East Cupcake Jewish Center, faces both. With that in mind, you wish to apply the available tools, strategies and tactics to prepare for an emergency. An example of a scenario for your planning and preparation follows:

Scenario

It’s quite busy at the East Cupcake Jewish Center on a bright, cold winter morning. Inside, the “Me and Mommy” classes are singing gleefully, 110 three,-four-and-five year olds are in the pre-school, the swimming pool is full and the senior program is having a luncheon for 125 to discuss the latest best seller.

A delivery man enters the lobby door and approaches the guard desk. He says that he has a package for the executive director, Myron Smith. The guard instructs the delivery man to leave the package, signs for it and the delivery man leaves. Thirty seconds later the package explodes. It was an incendiary device. Within a minute the curtains are in flames and the lobby is filled with smoke. Several people are injured. The automatic alarms sound.

You are Myron Smith, the executive director of the center. Upon hearing the alarm you run out of your office, hearing shouts of, “Myron, Myron, what should we do?”

What orders do you give? What should you have done to try to prevent this? What kind of emergency preparations have you made? What should you do now?

QUICK TIP

By focusing on plausible worst-case scenarios, the emergency planning team can prepare for most similar situations that are “not so bad.”

Discussion

What makes this a worst-case scenario?

1. In general, lobby fires are the worst from a life-safety vantage—the principal means of egress is blocked.

2. When there is an explosion, panic follows. It might be hard to carry out the best-laid plans.

In any emergency scenario there are four components: prevention, planning, response and recovery. While most fires are minor, to a certain extent they all require the same steps. A lobby fire is, by its very nature, worse because it blocks one of the exit routes. Matters are complicated by the wide variety of clientele. This “worst-case scenario” might not exactly fit every building, but it allows us to explore each of the four phases of emergency planning. Let’s examine each:

Prevention

Myron Smith should have looked at different kinds of prevention:

1. *Security tactics.* Can you keep the bomb away from critical areas?
The first problem presented by the situation above is, how did the messenger enter the lobby unchallenged? One of the basic tactics of “perimeter security” strategy (see the [Security Planning](#) chapter, P. 93) is to identify strangers before they enter a building.
2. *Security policy.* Can you keep the bomb away from critical areas?
In an ideal situation the incendiary device should never have been allowed in the lobby. Can you develop and implement policies and procedures for handling mail and packages that will help to safeguard your agency? Do the mail and packages (including messenger deliveries) come through the main lobby? How is the mail screened? Is the staff trained to recognize suspicious packages? How did Myron Smith’s name appear on the package? Is it on the bulletin board outside, in advertisements in local papers or on the web site?
3. *Fire prevention.* Can you stop a large fire from developing? An explosion is bad enough, but must a fire ensue? Because the lobby is a critical area, it should be regularly surveyed with fire safety in mind. Are the curtains non-combustible or fire-retardant? Are there boxes of pamphlets lying around? Does the East Cupcake Jewish Center have a trained fire safety instructor? Does the East Cupcake Fire Department offer classes in fire safety? Is a person assigned, on a daily basis, to tour the facility to check that evacuation routes are clear and that signs and emergency lighting are in working order? Are there fire drills and are they taken seriously? Are the fire drills varied so that occupants are forced to use alternate routes? Have the security consultants locked doors necessary for quick evacuation?
4. *Compartmentation and suppression.* Can you limit the spread of a

QUICK TIP

Identify the emergency leadership teams, put communication system and backups into place, determine policies and procedures for a wide range of disasters.

fire? Are the fire doors shut? Are there sprinklers in the lobby?
When an alarm is pulled does the building HVAC shut down?

5. *Basic fire safety education.* Do people know about “stop, drop and roll”?
6. *Staff training.* Does each member of the staff know his/her role in the event of a fire? Does the appropriate hierarchy exist for an effective emergency response (see [Response Teams](#), P. 24)?
7. *Drills.* Have regular users of the facilities experienced evacuation drills? Have you made provisions for occasional users?

Response to a security violation

1. *Staff training.* Are staff trained to recognize a potential intruder? Are they trained to recognize a potential bomb? Are staff members trained to call 911 immediately? Are staff members trained about the information they need to provide to authorities?

Response to an explosion

1. *Fire suppression.* Is there a fire extinguisher readily available? Does the East Cupcake Jewish Center have a policy covering such situations (e.g., try to extinguish a contained trash can fire, anything else should require evacuation of the affected area)? Should someone try to fight the fire or should everyone evacuate immediately? Have staff members been trained to safely fight the small fires while awaiting the firefighters?
2. *Building evacuation.* In an emergency most people will try to exit through the door they entered. In East Cupcake, the lobby door is blocked by fire. Are alternate exits clearly marked on posted building plans? Have people been taught about alternate exits during their evacuation drills? Are the exits well-marked and the exit signs and emergency lighting in working order? Is the evacuation team well-trained to assist as needed?
3. *Phased evacuation.* In any fire it is appropriate to move people out of danger by evacuating the affected areas. The people most at-risk should be of the highest priority. The East Cupcake Jewish Center Fire Safety Plan should identify and plan for alternative tactics, e.g., how should people be restricted from entering a danger zone, when should the entire building be evacuated, when is a phased evacuation of certain sections preferable and who makes the decisions?

QUICK TIP

Analyze each element of your scenario and think about prevention/mitigation, response and recovery.

4. *Special Populations, toddlers & pre-schoolers.* Toddlers usually have to be carried by caretakers or placed in special strollers. Evacuation planning should start with the assumption that toddlers and pre-schooler classrooms must be located on a low floor. Small children walk slowly and their evacuation might slow others. Your tactical planning should reflect the realities. Planners should experiment with various alternatives, e.g., keeping the pre-schoolers on the right or left side of the stairs so that others can pass them.
5. *Special Populations, swimmers.* How do the swimmers evacuate from the pool in their bathing suits out to 25 °F weather? Do the swimming pool and gym have extra protection (e.g., disposable thermal-reflective blankets) available for such an eventuality?
6. *Special Populations, disabled.* While many seniors can serve as part of the evacuation team, others (see the [Persons with Disabilities](#) chapter, P. 159) might need special support during emergencies.
7. *Areas of Refuge.* Where should the evacuees go? Has Myron Smith completed a [memorandum of understanding](#), (P. 111) with the school one block away so that the staff can bring people there? Are there staff people there to see if everyone evacuated safely? Do they have the appropriate client/student lists? Do they have parent lists so that the staff can call and assure worried parents that everyone is OK? Which staff members should make such sensitive phone calls? Do they have access to phones to do so?

Recovery

Some of the issues relating to recovery include:

1. *Insurance.* Was the building adequately insured? Was this an act of terrorism and excluded from standard policies? Should they have purchased business continuity insurance?
2. *Reconstruction.* To what extent was the building damaged? How long will construction last? Can parts of the building be used?
3. *Service gaps.* Will your clients seek their services elsewhere?
4. *Trust.* Will clients ever feel safe at the East Cupcake Jewish Center? Do parents think that the staff took care of their children?

Depending on the answers to these questions, Myron Smith and his staff could be busy getting back to business. Or maybe his next move should be to circulate his resume.

OUTCOMES

Leaders are often judged by the way they respond to emergencies. If they do well their reputations can be enhanced. When too many things go wrong they should start circulating their resumes.

Other possible fire scenarios

The above is an example of how you might apply a scenario to your own situation. Scenarios may or may not apply to any particular facility. For example, your building may not have a lobby that is used as the primary entrance to the building, in which case the above example may not apply.

Read the following list carefully, and check each of the scenarios that seems to apply to the particular facilities for which you are devising your plan. After the scenarios are selected, we will guide you through the process of selecting appropriate strategies and tactics for your plan.

- Large arson fire at a location adjacent or inside of one stairwell when the building is fully occupied.
- Large, rapidly-developing fire at night in a dormitory facility.
- Smoldering electrical fire in a concealed space when the building is fully occupied (the location of the fire is not immediately evident).
- Large fire during off-hours when there are few people in the building.
- Large fire in a school during lunch or assembly.
- Large, rapidly-developing fire at the entrance, foyer or lobby as a result of religious or secular observance displays being ignited (e.g., Menorah) when building is fully occupied.
- Smoldering electrical fire in a concealed space, when the building is closed during off-hours with only a few people in the building (the location of the fire is not immediately evident).
- Cooking fire in an unattended pot on a stove in a kitchen.
- Fire starts when a person discards a cigarette in common space where it ignites combustible materials.
- Fire ignited when person falls asleep smoking a cigarette and the cigarette falls between cushions. Person wakes and leaves. Noticeable fire starts an hour later.

QUICK TIP

Try to think of variations of your disaster scenarios and test whether your emergency plans cover them.

RESPONSE TEAMS

A Day Like Any Other Day⁴

Jo Ann Schmokenberg is the popular head of school of the East Cupcake Hebrew Day School, a school of 230 children located in the Little Cupcake Hills. She's done much in her five years at the helm to change the teaching style there at East Cupcake because she believes all students learn best when they are actively involved in the process. She's been so busy thinking about fund raising and dual curricula, however, that she hasn't paid much attention to emergency preparedness planning at her school site or the response training available to her from a variety of sources.

When the earthquake hits that Thursday morning in October, Jo Schmo (the term of endearment used by her teachers) ducks under a table and waits out the shaking, all the while trying to remember where she put the disaster response checklists the state education department sent out a couple months ago. She wishes she could recall what hers said. A light fixture crashing down on the table shocks her into a chilling realization: this is IT and she has to do something.

After the shaking stops, she calls for the secretary in the next room. Jo begins to pick her way there, carefully trying to avoid the broken glass all over the floor. In the main office she finds the secretary being ministered to by a volunteer parent who was preparing to lead the afternoon field trip. Blood is streaming from the secretary's scalp, and she's too shaky to answer Jo Schmo's plaintive question, "Who do we call?" The parent says, "I haven't had a chance to try the phone yet." Jo starts toward the nurse's office next door. She's slowed by the debris on the floor and she can't see very well in the hallway because the lights are all out.

As she is struggling with the locked (or is it jammed?) door to the nurse's office, wishing she had a tire iron, a student appears in the gloom saying he's been sent by the third-grade teacher to find out whether they should all evacuate. "Is anybody hurt in your room?" she asks him. "I don't know," he replies. She mutters "evacuate" reflectively under her breath, wondering about the whereabouts of the custodian. "Is there lots of damage in your room?" she asks. "I don't know," he responds. "I'll be right there," she says, "but first I have to get the first aid kit out of here."

*. . . . this is IT
and she has to do
something.*

⁴ Adapted from *School Emergency Response: Using SEMS at Districts and Sites*, California Governor's Office of Emergency Services, June 3, 1998.

At the sound of a voice behind her, she turns to see a fourth-grade teacher approaching: “Jo, we gotta call the ambulance, well, two or three of them, because there’s a bunch of kids hurt in my classroom and in Julie’s. I just left my kids with her to look for first aid stuff. I tried to get to the storage shed on the playground, but there are trees down and a power pole. I looked for Karl, I called for him, but there was no answer. Was he here this morning? Did you notice? Listen! Sirens, maybe on Mountain Boulevard.”

An adrenaline rush propels Jo Schmo back into the main office to use the phone. The secretary is already dialing it, sitting on the floor with a Pampers wrapped around her head. “We need to call an ambulance,” announces Jo, “and then, I suppose, the district office.” “I’m calling my husband,” says the secretary, “I want him to come and get me.” Jo grabs the phone out of her hands and punches in 911; it’s busy.

At this moment the part-time librarian comes into the office, her eyes bigger than usual and her voice quavering, “I wasn’t sure what I was supposed to do; the library is a mess and I . . .” Jo Schmo interrupts her, “We’ve got to get an ambulance; we’ve got injured kids. The phone is busy. I can’t get into the nurse’s office for the first aid kit. Is she here today? I don’t know how many kids are injured. I don’t know if all the teachers are OK. I don’t know if we should evacuate, there are electric lines down on the playground. Have you smelled any gas? Have you seen Karl? Can you run down to the fire station and tell them we need help?”

“Use the radio they gave us,” pipes up the secretary from the floor, “It’s in your office.” Jo Schmo walks gingerly back into her office, crunching glass shards with each step, and begins looking for the radio.

Questions:

- What’s the most important thing for Jo Schmo to do?
- What does Jo Schmo need to know?
- What things need to be done, and who can do them?
- What equipment or supplies are needed? Who can get them?
- Can the employees leave the school and go home?

Planning for emergency responses

Could Jo Schmo have been more prepared? Would it make a difference? Could her staff be trained for emergency responses and assigned specific functions? Could the school have the right equipment in place? What strategies and tactics should Jo have thought about? What emergency procedures should be in place?

The key priority of all emergency planning is the protection of life and safety. Protection strategies are critical and certain functions are common to all emergencies. During dangerous situations there are a finite number of choices. Should you move people from the area of danger into a relatively safe area (e.g., evacuate) or is the safest place inside your building until the danger lessens or passes?

Using the commonalities among emergencies

In dangerous situations there are clear commonalities. In each emergency situation someone must make decisions about which protection strategy is preferable, and the strategy must be communicated and carried out in a clear and effective manner. The key concept is that you can identify the common strategies and tactics (e.g., evacuations or sheltering-in-place) and assign responsibilities and functions to existing staff people. Thus, your response teams can be ready and in place. Organizing response teams is a critical initial step in the planning process. Employees should be identified and trained because inevitably, they will be the first responders.

Jo Schmo knows about fire drills—she’s required to have them by law. As the head of school she is the designated “Fire/Safety Warden.” That used to be called just the fire warden but the real job is bigger. She also has a deputy warden and searchers. The Fire/Safety Warden must assess the situation, give orders and supervise the drill or, if necessary, the fire evacuation.

All too often fire drills don’t go far enough. What else should be done in case of an emergency? Where would Jo Schmo bring the kindergartners if there’s a fire and it’s 15 degrees outside? How does she notify parents?

What Jo Schmo doesn’t know is that these same fire drills give her the basis for a broader emergency response system. Most emergency agencies have

QUICK TIP

No matter what, your staff will be your first responders. A trained, organized and equipped staff can greatly can both reduce the loss of life and property in the workplace and ensure an enhanced recovery.

⁵For more information about ICS, see the FEMA Independent Study Courses at <http://training.fema.gov/>. Much of this section is adapted from those materials.

built their responses around the Incident Command System—better known as ICS⁵, which can readily be applied to the nonprofit world.

What is ICS?

The Incident Command System in use today is an outgrowth of California's FIREScope program developed in the 1970's to improve management of large wildfires. It was designed to provide a commonly accepted management structure that would result in better decisions and more effective use of available resources. It specifically recognized the need to coordinate responders among various levels of government (e.g., multiple municipalities or city, county, state and federal authorities) and among emergency responders (e.g., fire, police, buildings).

In most disasters, nonprofit organizations will have to work with other agencies, e.g., police, fire or emergency management. The organization's response will have to be melding into the broader response. ICS provides a system to do so.

The Incident Command System (ICS) is the model tool for the command, control and response to any emergency situation. It provides a management structure and system applicable to small-scale daily operational emergencies as well as major mobilizations. ICS provides command center and operational staff with a standardized operational structure and common terminology.

QUICK TIP

In an emergency confusion or hesitation could cost lives. People have to know their roles and be trained to carry them out.

Why should a nonprofit organization learn about ICS?

Who is in charge? Are there too many people reporting to one supervisor? Is there a lack of coordinated planning for your organization? Sound familiar? The problems confronting firefighters in California are similar to the ones facing nonprofits. Confusion or duplication of effort can be an everyday problem in many organizations. However, in an emergency, resources are scarce and any hesitation could cost lives.

Another advantage of implementing an ICS-based emergency structure is the signal that you give to emergency responders. If you are using a system analogous to theirs they will consider you to be more professional and your ICS system will readily fit into the broader emergency network. Moreover, your response team easily fits with the overall emergency response efforts.

Some state statutes require that schools and other institutions include ICS as part of their emergency plan.

ICS is modular

Thousands of people can respond to a wildfire emergency. Typically, nonprofits are different. They are relatively small organizations.⁶ ICS may seem both convoluted and a major drain on resources.

In reality, ICS is efficient because it is a modular system. These modules are not specific to particular types of emergencies; rather they are functions that are often needed regardless of the type of emergency. Using these modules as a planning and operational tool helps organizations to identify emergency tasks and the resources necessary to do them. Any emergency has “core” needs, i.e., all emergency responses need a “commander” and a clear chain of command. Others conditions mandate specialized needs such as the evacuation of a building or a “lockdown,” while some crises are legal in nature. Modules can be developed to assign personnel and resources to handle the various types of emergencies. As an incident becomes larger, the core functions will overwhelm the abilities of the commander who will become unable to understand and coordinate all the core functions. In response, the “commander” activates the modules necessary for a particular situation. Each module has a person responsible for its operations.

Under the stress of an emergency, incident commanders naturally tend to focus their attention on the most immediate problems, and might ignore issues that can escalate to the critical point if left unattended. Therefore, other persons need to attend to these functions and bring them to the incident commander’s attention when important decisions must be made.

In addition to commanding the incident, a typical set of modules in ICS include the following:

- Management
- Planning
- Operations & Logistics
- Finance/Administration

Can one size fit all?

A central assumption of ICS is that a single emergency response system can

RESPONSE TEAM PRIORITIES

- *Life safety*
- *Incident stabilization*
- *Property conservation*
- *Business continuity*

⁶ In the United States the average nonprofit organization has 109 full and part-time employees (43% of the Independent Sector organizations are healthcare related). The New Nonprofit Almanac in Brief—2001, Independent Sector.

be tailored to all kinds of hazards and cover any incident. Notice that the core functions of ICS are often needed regardless of the type of emergency. While each organization and each emergency is unique, the ICS system is flexible and provides the framework for the widest possible varieties of response. An organization only needs to activate the ICS modules needed for the particular emergency. Because ICS assumes that an organization will use existing staff, it is cost effective. The basic ideas can even be applied to non-emergency situations such as special events, i.e., someone must clearly be in charge, there have to be reliable methods of communication and there should be appropriate resources to address the situation at hand.

Priorities of ICS

There are four basic priorities of any ICS structure:

Life Safety. The first and foremost goal of any emergency response is to protect staff and clientele and/or to get them away from and keep them out of harm's way (as much as possible). Depending on the emergency, life-safety strategies might involve evacuation, sheltering-in-place, lockdown, duck, cover and hold or other life-safety options.

Incident Stabilization—Although it's not always possible, one should aim at trying to contain an incident and not allow it to escalate beyond the current level. There are many types of examples. Obvious type of incident stabilization is to train certain employees to fight small (e.g., garbage can) fires or to close fireproof doors. Such action will prevent a fire from spreading further. Another category of incident stabilization could involve an employee who is charged with an action that might be criminal. If an organization adequately investigates and takes appropriate disciplinary action the problem could be contained. If not the problem can grow.

Property Conservation—During an evacuation are critical systems shut down? Is there a plan to remove key religious objects (e.g., Torah scrolls) if possible?

Business Continuity—What do you need to do to enable your organization to get back to business with minimal “downtime”? Have you investigated alternative sites? What supplies do you need to operate under emergency conditions? Is your data backed up?

Major Components

There are five major components of any ICS:

QUICK TIP

The Incident Commander has overall authority for an incident or event. That doesn't mean that s/he has to do, or can do everything.

1. Incident Command
2. Planning
3. Operations
4. Logistics
5. Administration & Budget

Incident Command

The *Incident Commander* has overall authority for an incident or event. When the question is asked, “What are we going to do?” he/she is expected to have the answers. When feasible, he/she make decisions. During the planning process they set priorities and objectives. As leader, the Incident Commander decides which modules must be activated in order to respond to the incident.

Command activities include:

- Establishing command and establishing the Emergency Operations Center (EOC).
- Protecting life and property.
- Controlling personnel and equipment resources.
- Maintaining accountability for responder and public safety, as well as for task accomplishment.

QUICK TIP

When a lot is going on the Incident Commander must be able to make decisions, delegate and to effectively supervise.

Emerg

From: *Managing a School Crisis*, Los Angeles County Office of Education, Safe Schools Center, Division of Student Support Services.¹

- Establishing and maintaining an effective liaison with outside agencies and organizations.

There's a lot going on during an emergency—too much for any individual to manage in an effective manner. Many of the functions below can actually be accomplished through delegation. The Incident Commander management must supervise or execute the following:

- Establishing command.
- Ensuring responder safety.
- Assessing incident priorities.
- Determining operational objectives.
- Developing and implementing the Incident Action Plan.
- Developing an appropriate organizational structure.
- Maintaining a manageable span of control (e.g., there are the appropriate number of supervisors for different floors, wings or buildings).
- Managing incident resources.
- Coordinating overall emergency activities.
- Coordinating the activities of outside agencies.
- Authorizing the release of information to the media.
- Keeping track of costs.

QUICK TIP

An effective Incident Commander must be assertive, decisive, objective, calm and a quick thinker.

An effective Incident Commander must be assertive, decisive, objective, calm and a quick thinker. To handle all of the responsibilities of this role, the Incident Commander also needs to be adaptable, flexible and realistic about his or her limitations. The Incident Commander also needs to have the capability to delegate positions appropriately as needed for an incident. There should be a trained person (preferably with a backup) capable of being the Incident Commander on the premises during all operational hours.

Modules

As incidents become more involved, the Incident Commander can activate additional general staff sections (that is, planning, operations, logistics, and/or finance/administration) as necessary. Each section commander, in turn, has the authority to expand his/her section to meet the needs of the situation.

Command

Initially, the Incident Commander will be the trained senior first responder to arrive at the scene. A newly arrived senior member of your organization

may want to leave the acting Incident Commander in charge. As additional responders arrive, command will transfer on the basis of who has primary authority for overall control of the incident. In other words, in case of a fire at a school, the principal is the Incident Commander until the first firefighters arrive. At that point a fire captain might be in charge. As more equipment arrives, the fire captain defers to a fire chief. The fire chief assumes responsibility for tasks such as search and rescue that were previously the responsibility of the principal. The fire chief might then direct the principal to check if students and staff are accounted for.

In most organizations the CEO (e.g., Executive Director, Principal) will be the Incident Commander. There can be cases in which the CEO appropriately defers to a deputy. For example, a well-qualified director of security may be the most appropriate individual during a security breach, while the general counsel might take the lead in a legal-related crisis.

The senior police and/or fire department responders will always assume this command role unless the emergency is of such a great magnitude that they are needed elsewhere. They will be in charge and make many of the life safety decisions. The initial Incident Commander will need to brief the new Incident Commander to provide a detailed description of the incident as soon as possible.

The command staff may include a *liaison officer* who will be the point person for emergency workers/agencies and an *information officer(s)* responsible for communicating with the organization's staff and clientele as well as the press. Most command staffs also have a *record keeper*, or someone with primary responsibility to document the events and timing of the emergency. Such records may be useful for insurance purposes or if litigation arises as a result of the event.

Operations

The Operations Section is the “nuts-and-bolts” of any emergency response. These individuals actually carry out the Incident Action Plan and direct all resources. The Operations Section is responsible for carrying out the response activities described in the Incident Action Plan (IAP). The Operations Section Commander coordinates Operations Section activities and has primary responsibility for receiving and implementing the plan. The Operations Section Commander reports to the Incident Commander and determines the required resources and organizational structure within the Operations Section. The Operations staff should know which emergencies require immediate action and be prepared to respond without delay.

YOUR RESPONSE TEAM

The Operations Section is the “nuts-and-bolts” of any emergency response.

The Operations Section Commander's main responsibilities are to:

1. Direct and coordinate all operations, ensuring the safety of Operations Section personnel.
2. Assist the Incident Commander in developing response goals and objectives for any incident.
3. Implement the Incident Action Plan.
4. Request (or release) resources through the Incident Commander.
5. Keep the Incident Commander informed of situation and resource status within operations.

There can be many components within Operations. For example, if the Incident Commander orders an evacuation, the Operations Section carries it out and reports its progress and problems to the Incident Commander. The evacuation team can have several *divisions* covering different geographic areas (e.g., a multi-site organization needs a division for each facility, within a building each floor or wing might warrant a division).

In ICS lingo, groups are described as *functional* areas of operation. For example, in many emergencies building engineers or the computer staff have to shut down critical systems. Such specialized functions are assigned to groups.

Operations staff should know which emergencies require immediate action and be prepared to respond without delay.

Besides Operations there are three other sections. Often, these sections will not come into play until after the acute phase of an emergency. The other sections perform staff-like functions; they ensure that operations have the resources and record keeping needed to work efficiently and effectively.

The Operations Section is responsible for carrying out the response activities described in the IAP. The Operations Section Commander coordinates Operations Section activities and has primary responsibility for receiving and implementing the IAP. The Operations Section Commander reports to the Incident Commander and determines the required resources and organizational structure within the Operations Section.

Planning

Planning develops the action plan to accomplish the objectives during the emergency. In smaller events, the Incident Commander is responsible for planning, but when the incident is of larger scale, the Incident Commander establishes the Planning Section. The Planning Section's function includes

QUICK TIP

You may be reimbursed for some or all of your disaster costs. Designate someone to be responsible to track them.

the collection, evaluation, dissemination and use of information about the development of the incident and status of resources. The Planning Section helps the Incident Commander anticipate problems as they develop. This section's responsibilities can also include creation of the Incident Action Plan (IAP), which defines the response activities and resource utilization for a specified time period.

Finance/Administration

Though sometimes overlooked, the Finance/Administration Section is critical for tracking incident costs and reimbursement accounting. Unless costs and financial operations are carefully recorded and justified, reimbursement of costs is difficult, if not impossible. The Finance/Administration Section is especially important when the incident is of a magnitude that may result in a presidential disaster declaration which would qualify for federal reimbursement.

Each of these functional areas can be expanded into additional organizational units with further delegation of authority. They also may be contracted as the incident de-escalates.

Logistics

The Logistics Section is responsible for providing facilities, services and materials, including personnel to operate the requested equipment for the incident. During the incident the Logistics staff is responsible for assigning volunteers and the distribution of items such as water, food and batteries for the flashlights.

Assigning staff to core functions and sections

One key concept of ICS is that an institution does not have to hire new people for emergency duties. Existing staff members are assigned duties based on their jobs and competencies. Instructional staff, for example, will be expected to maintain control of their classrooms, account for their students or direct evacuation. Administrators will be responsible for making building/organization-wide decisions (e.g., the need for evacuation, the need to close, communication with the emergency services and communication of new procedures to parents or other clientele.) The financial staff will be in charge of recording costs, etc.

Other people have to be assigned as communicators, for search-and-rescue, or site security, for example. Thus, some staff will have to be freed of their usual assignments so that they can fulfill particular emergency functions.

QUICK TIP

You don't hire new people to be on your response teams. Existing staff are assigned duties based on their jobs and competencies.

Information cards

Cards should be printed so that the assigned staff keeps, on their person, information relevant to their ICS function. This information should include a brief description of their tasks and critical information needed to perform the task, especially names and telephone numbers. In most instances, a simple card with this information can be kept in a wallet or purse. This simple step will save valuable time during an emergency.

A modular organization

Your response team should be tailored to the emergency situation. The first arriving manager becomes the Incident Commander. As the incident warrants, the Incident Commander activates other functional areas (i.e., sections). In approximately 95 percent of all incidents, the organizational structure for operations consists of command and single resources (e.g., a fire truck, an ambulance or a tow truck). If needed, however, the ICS structure can consist of several layers. In this unit, we have described the two top layers: Command and General Staff. Other layers, covering building sections, many buildings or various functions, may be activated as warranted.

PLANNING TIP

A disaster could put your usual headquarters out of commission for an hour, a day, a week, a month, a year or forever.

Designated incident facilities

Emergency Operations Center (EOC) and Alternatives

The Emergency Operations Center is “command central,” the location from which the Incident Commander, the Command Staff and the General Staff provide centralized direction and/or coordination of the emergency response. The Emergency Operations Center is where resource allocations can be made, and responses tracked and coordinated with the appropriate operational area agencies. At the site level, the post may be in the principal’s office, a meeting room or special room designated for it. The location should have the resources to perform the required function, including the appropriate communications equipment (both to receive up-to-date alerts and to communicate with your clientele) and backups, lists and supplies should be available. Ideally, the Incident Commander should be able to survey the emergency operations from the command post so that he/she can appropriately modify the incident plan.

A disaster could put your usual headquarters out of commission for an hour, a day, a week, a month, a year or forever. When the World Trade Center fell, it destroyed New York City’s emergency command center. New York City’s Office of Emergency Management quickly established an alternate facility away from “Ground Zero” and eventually established another command center for the longer term.

Each alternative command post should have copies of essential documents and, to varying extents, disaster supplies, communication facilities and other critical information and equipment. Many emergency planning guides refer to the top alternate command posts as “hot sites” (EOC) and less likely backups as “cool sites” (alternative command posts). Hot sites are afforded more resources than cool sites.

For example, if an agency is providing meals for the homebound elderly and its facilities are damaged by a hurricane, that agency still must provide meals or its clientele will be put at risk. In the case of a hurricane, the agency staff will probably have time to close the facility and move some equipment and records to an alternate command site. This would not be the case for a tornado, earthquake or terrorist attack.

In such an event, an alternate command post close to the agency’s headquarters might be as likely to be affected as the existing facilities (although it might be fine in the case of a boiler explosion). After the initial evacuation and response that covered life safety, incident stabilization and property conservation the Incident Commander and response team have to focus on business continuity. That means meals have to be prepared and delivered and the staff must be paid, etc. How is this done without your existing site?

There are multiple answers to this question and most would include a mutual aid pact. Is there a sister agency or one in a similar business? Could you temporarily operate out of their facility? Can you keep backup software and data at home for payroll and other purposes? Can you subcontract with a vendor to provide meals?

As a rule of thumb, the alternate site should be far enough away so that it is not disabled by the same disaster event or susceptible to the same disaster (e.g., another storm surge evacuation zone, see the [Hurricanes and Tornadoes](#), section, P. 77).

The Command Post might be off site, e.g., in a building down the block. As much as possible identify each Command Post location with a sign, so that it is visible to staff and emergency responders. Signs can be pre-printed and stored with your emergency supplies.

Integrated communications

Your response teams must be able to communicate, no matter what. Plan

PLANNING TIP

Identify and prepare staging areas where people will meet or for equipment.

both primary and backup communication strategies (see the [Emergency Communication Tactics](#) chapter, P. 139). People should be trained with standard operating procedures, using clear text, common radio frequencies, and common terminology. In other words people should be able to communicate quickly, succinctly and clearly.

Staging areas

Your Incident Action Plan should identify designated staging areas where people or equipment will gather. There are different types of staging areas, e.g., where emergency responders put their equipment, where people assemble after an evacuation or where resources are kept while awaiting incident assignment. Other incident facilities may be designated for incidents that are geographically dispersed, require large numbers of resources or require highly specialized resources.

Other possible staging areas include designated areas for emergency equipment, areas of refuge and/or parental assembly or pickup areas. These facilities should be pre-identified and appropriate staff assigned to each.

Training and exercising are critical

Having response teams that exist only on paper may not work in an actual emergency. People who have been briefed and have quick access to the emergency plan can function well during longer emergencies. The response teams become real through training and exercises. They help staff become familiar with their responsibilities. They are necessary for new staff. By practicing what to do during and after an emergency, you will increase the confidence of clientele and staff that disasters can be manageable events.

In summary

- Every emergency, no matter how large or small, requires that certain core functions be performed: incident command, planning, operations, logistics and finance/administration.
- The system can be expanded or contracted depending on the situation and the immediate needs. One person can do more than one function.
- Every incident needs a person in charge, called the Incident Commander at the site level, or The Emergency Operations Center Director at the district level.
- No one person should be in charge of more than seven people (the optimum number is five). [Note: this does not apply to Student Su-

pervision.]

- See your local emergency management office to learn where you can access additional ICS training.

Helping Jo Schmo

Blessed with the power of temporary omniscience, let's rewind the tape. Once again, it's a day like any other day.

While reading the morning paper, Jo Ann Schmokenberg sees a story about a tornado hitting a school in Kansas. It makes her think, "We're not going to have tornadoes, but what about earthquakes? What would I do?"

Arriving at school, Jo sends an E-mail to a couple of colleagues asking whether they've made any emergency plans. She finds out that United Jewish Communities has put out a manual and one is forwarded to her. At first glance, the process seems daunting. "Hm-m-m-m, what could happen here? Earthquakes, wildfires, chemical leak . . . remember the crazy guy who went into the Jewish center? Could I plan for all of these eventualities? Should I even try?" Almost shaking, Jo dials a number she knows well. Whenever she has a big problem she reaches out to her mentor, Lotsa Mazel.

As usual, any conversation with her had a calming effect. "Slow down," said Lotsa, "I just started the emergency planning process last year. You take this one step at a time. Clearly, you have to be in charge, but if you're not around, who's the alternate?"

"Let's see," mumbled Jo, "there's the English principal, and the phys ed person is really good in a crisis."

Lotsa heard this and spoke up, "Done, the principal is the alternate and the phys ed guy will be your Operations Commander—that way someone's always available. You told me that you've identified a number of hazards, let's begin with those. I learned that for earthquakes you have to have drills to duck and cover and then evacuate, for wildfires you have to evacuate and for chemical leaks and snipers you should keep the kids inside in comparative safety. If those are your critical strategies how do you put together response teams? It's like most other kinds of planning."

"Yeah, I see," Jo reflected, thinking out loud. "My staff knows how to do a fire drill. That's an evacuation. I'm the fire/safety warden . . . that means that I would be the Incident Commander in any emergency. The phys ed

H M - M - M - M

Jo reflected, thinking out loud. "My staff knows how to do a fire drill. That's an evacuation."

teacher and the school nurse know first aid, CPR and how to use the defibrillator. Maybe I should have some more of the staff trained. What do I do now?” Deep in thought, Jo thanked Lotsa saying, “I’ve gotta get to work!”

By breaking the job into pieces Jo knew that she could do it. Calling in the appropriate staff (now elevated to be her emergency planning team) she described what she wanted to do. They started to talk about the differences between the fire drill and an earthquake. Together, they defined escape routes and how to get to the primary and backup exits.

One team member suggested that upon feeling an earthquake they should evacuate the kids as soon as the shaking stops. Someone added, “If a gas main breaks outside it might be more dangerous to bring the kids out of the building than to keep them under the tables in their classrooms.”

So, the discussion continued. The ICS team began to take shape. Teachers would be trained to take care of their classrooms and given supplies (see [Supplies and Go Kits](#), P. 146). Jo made sure that she had a first aid kit in her office and had others positioned around the building. Administrators would be assigned to supervise other areas and functions. Jo’s secretary was assigned to put together loose leaf notebooks with class lists, parents lists, home phone numbers, building plans and emergency procedures.

“But if the earthquake knocks out the intercoms and the phones, what do we do?” asked Jo at the next meeting. Cell phones were one alternative, but the earthquake could knock them out too. Finally, the fallback communication plan was developed. Pairs of the best kids would be assigned as “runners.” If the intercom didn’t work, when the shaking stopped these kids would take a note from their teacher reporting on conditions to Incident Commander and be prepared to return with further instructions. The discussion continued, with people outlining situations when the teachers should act on their own and when they should wait for directions. Jo went home and began to write up this phase of the plan.

There was still so much to do. How would parents be notified? Is there an adequate system to release the kids to their parents or caregivers? How would they keep all the right lists up-to-date? As the questions spun through her head, one important thought struck Jo. All of these issues were common to virtually any emergency. It only has to be done once!

Then there were the long-term problems. Of course, Jo’s finance director will head the finance component. The office secretary will take the lead in logistics. And what about planning? The Board must be involved in any repairs. What happens if the school can’t use its building for a week, a month or several months? Jo knew that these issues would take more meetings. Oh well, meetings are her life.

IMPLEMENTING YOUR EMERGENCY PLAN

Once both the lay and professional leadership have reviewed the plan, the board should formally adopt and implement it. An emergency management plan placed on a shelf in the executive director's office is a waste of time. Implementation begins with the distribution and explanation of the plan to everyone affected by it. While every staff member should have the opportunity to comment on the plan and its implementation, some special training will likely be required—and exercises and drills are a must.

Nonprofits are dynamic organizations that must adapt—on an ongoing basis—to new client needs, funding constraints and service delivery challenges. The dynamic nature of your agency requires that emergency management strategies be revisited at least annually. The planners should evaluate your strategy to ensure its continued relevancy, comprehensiveness and effectiveness. Have your risks changed due to the addition of new services or curtailment of programming? What resources are available for controlling or addressing them?

Having an emergency management committee, composed of lay leaders and staff members, that meets periodically can help ensure that the issue of risk management receives ongoing attention. This committee also needs to evaluate the strategies it implements. Have the emergency management techniques had the desired impact? Were injuries or accidents reduced? Did insurance premiums go up or down at renewal? Is the plan having the desired impact or do you need to make some revisions?

GENERAL RULE

Regularly evaluate your strategies to ensure their continued relevancy, comprehensiveness and effectiveness.

Drills and Exercises⁷

What are Drills and Exercises?

Drills and exercises are simply an extension of your scenario plotting—simulating plausible situations to expose staff and clients to various hazards and to explore how people react. They always involve a group of people who undertake specific roles and try to accomplish specific emergency response goals. Exercises and drills are different from the meetings where an emergency response topic or problem is discussed. Such educational and orientation meetings are necessary. Meetings are needed so that managers and operations staff members understand relevant parts of an emergency plan and how they fit together. Drills and exercises are not recommended before

⁷ Much of the content for this chapter was adapted from a FEMA independent study course IS-139 Exercise Design. While the course is designed for professional emergency planners, you are likely to find much of the advice of value, particularly if you are planning more complicated functional exercises.

participants have a good understanding of the roles and duties they are expected to perform.

There are many variations of training exercises, but FEMA provides useful definitions for three basic types of interest to this chapter.⁸ These basic types of exercises are discussed more fully later in this chapter:

- *Drills* are “coordinated, supervised activity normally used to exercise a single specific operation or function in a single agency.”
- *Tabletop exercises* involve an emergency situation [played out] in an informal, stress-free environment. They are designed to elicit constructive discussion as participants examine and resolve problems based on existing plans. There is minimal attempt at simulation, no utilization of equipment or deployment of resources, and no time pressures.” Tabletop exercises are typically based on a specific scenario.
- *Functional exercises* are “fully simulated interactive exercises. They validate the capability of an agency to respond to a simulated emergency testing one or more functions of the plans.”

QUICK TIP

Some of your best emergency planning can be done during a tabletop exercise, with key players discussing how to respond to a scenario.

Additionally, FEMA discusses *full-scale exercises* that are typically beyond the scope of exercises conducted by most nonprofit organizations. These are field exercises that involve multiple organizations, the mobilization and movement of agency personnel, equipment and resources. However, depending on their needs, your organization could be invited to participate, an opportunity that you would be wise to accept.

Why conduct drill and exercises?

There are three basic goals that drills and exercises can help you accomplish:

- Training so that individuals and groups will have a better understanding of their roles.
- Evaluation to find out whether the plan is likely to work during a real emergency.
- Feedback to discover problems so that the tactics of a plan can be improved.

⁸ Memorandum to Heads of Federal Departments and Agencies. Subject: Test Training and Exercise Program for Continuity of Operations (COOP) April 30, 2001, <http://www.fema.gov/pdf/library/fpc66.pdf>.

Who should participate?

The persons invited to participate depend on the goals you've selected. People who are not needed for the above goals should be excused from training. Requiring participation from people who have nothing to learn and who can't help evaluate or improve the plan tends to build resentment over their wasted time, and this will reduce your credibility as an emergency manager.

The people who are invited to participate should understand exactly why they are needed. These people are not always members of the emergency response team. From the standpoint of training, all building occupants may need to learn the routes of egress from a building. From the standpoint of plan evaluation, they may be needed to discover whether staff can effectively communicate procedures and instructions. Failing to explain these goals to building occupants and asking for their help in evaluating the exercise are common mistakes.

Drills

Drills are defined as a “coordinated, supervised activity normally used to exercise a single specific operation or function in a single agency.” They are also used to provide training with new equipment, to develop new policies or procedures, or to practice and maintain current skills.”

Drills are limited in scope and they do not require specific scenarios—they will usually apply to any number of different ones. Drills are conceptually related to strategies. Any given strategy might be used in response to a variety of different types of scenarios. Think of drills as an opportunity to exercise and fine-tune strategic responses to a range of scenarios.

Examples of drills:

- building evacuation
- security guard response
- sheltering-in-place
- notification and recall of key personnel
- reporting to emergency stations with GO kits and assuming duties.

Because of their limited scope, drills usually involve only a few objectives.

Examples of objectives include:

- Familiarize all participating occupants with the nearest emergency egress routes.
- Evacuate all occupants from the building within 3 minutes.

QUICK TIP

Think of drills as an opportunity to exercise and fine-tune strategic responses to a range of scenarios.

- Have the floor warden(s) sweep the entire building within 5 minutes.
- Test whether all reachable parents can be notified of the status and location of their children within 20 minutes and leave messages for all others.
- Have all on-site acting emergency team leaders report to their stations within 15 minutes.
- Contact two alternative sheltering resources.

Drills can be announced or they can be a surprise. However, surprise drills should be used sparingly for two reasons. First, surprise drills create a well-documented “cry wolf” effect by increasing the likelihood that participants will interpret alarm signals as not indicating real emergencies. This can cause slower and failed responses to future (possibly genuine) alerts. Second, surprise drills can be so disruptive that participants will develop a poor attitude towards emergency preparedness and want to reduce their future commitment. In general, reserve surprise drills for those occasions when you really must evaluate the readiness of participants.

HELPFUL TIP

Elicit feedback from all participants. They are a good resource for evaluating drill effectiveness.

To reduce the resentment of participants, ask yourself why each participant needs to participate and explain it to them. If you can’t answer this question, then consider excusing them from the exercise. Do not ask them to participate any longer than necessary. And finally, use participants as a resource for evaluating drill effectiveness. (For example, ask them if they heard the alarm signal or found out about the drill in some other way. The failure of many alarm notification devices often goes undetected simply because evaluators did not bother to ask occupants if they could hear the signal.)

Tabletop exercises

Tabletop exercises are defined as “an emergency situation in an informal, stress-free environment. They are designed to elicit constructive discussion as participants examine and resolve problems based on existing plans. There is minimal attempt at simulation, no utilization of equipment or deployment of resources and no time pressures. The success of these exercises is largely determined by group participation in the identification of problem areas. They provide an excellent format to use in familiarizing newly assigned/appointed personnel and senior officials with established or emerging concepts and/or plans, policies, procedures, systems, and facilities.”

Tabletop exercises are built around scenarios. If you have used the planning approach described in this manual, you already have scenarios that you used during the planning process to construct tabletop exercises.

Examples of table top exercises:

- A sniper could be operating in the general area.
- A chemical release in the area that could endanger occupants.
- A major earthquake that disrupts lifeline and transportation infrastructures.
- Recovery and business continuity scenario following a major fire.

Tabletop exercises are well-suited to detailing and improving emergency operations plans. Participants discuss a scenario from the perspectives of their roles and identify and cooperatively solve problems as they arise.

Here are some typical objectives for tabletop exercises:

- Increase awareness of the standard operating guidelines for sheltering-in-place.
- Plan the details of acquisition and storage of resources needed to provide 4 days of sheltering.
- Identify critical operations that need to be performed in response to a large earthquake.
- Identify and prioritize relevant policies and important procedures in response to a toxic chemical release that can potentially affect the facility.

During a tabletop exercise, the participants discuss their respective functions, roles and how to coordinate their responses to best meet each other's needs.

Tabletop exercises can involve various degrees of simulation, even though the activities are normally not conducted under time pressure and resources are not deployed. For example, a tabletop exercise can be performed in an emergency operations center, or a simulation of one. People and equipment can be used to present information in a chronological sequence to simulate an emergency. (People in this role are called “simulators.”)

Functional Exercises

Functional exercises are “fully simulated interactive exercises. They validate the capability of an agency to respond to a simulated emergency testing of one or more functions of the plans. They focus on policies, procedures, roles and responsibilities of single or multiple emergency functions before, during or after any emergency event.”

QUICK TIP

Participants in tabletop exercises discuss a scenario from the perspectives of their roles and identify and cooperatively solve problems as they arise.

FEMA has listed basic emergency management functions. Because these were developed principally for local, governmental offices of emergency management, you will probably find that only some are relevant to your situation:

- Alert and notification
- Communication
- Coordination and control
- Emergency public information
- Damage assessment
- Health and medical
- Individual and family assistance
- Public safety
- Public works
- Resource management
- Warning

Think about how these apply to your organization and facility. For example, “communication” may involve notifying parents about an emergency and where their children are located. “Coordination and control” may involve evacuating and sealing off a part of a building where a potential bomb is located. “Health and medical” may involve sending for some community members knowledgeable in assessing the likelihood that people have been exposed to some chemical or biological agent.

HELPFUL TIP

Start with an assessment of what objectives you or your team believe will be of the most value and then choose the type of exercise that best fits your needs.

Examples of functional exercises:

- Fire scenario including evacuation, blocked egress path and cooperation of fire department.
- Suspicious intruder scenario including security response, search and call to emergency dispatch or police department.
- Bomb threat scenario including threat assessment, search, securing and evacuating part of the building and calling the appropriate police contact.
- Medical emergency scenario including possible heart attack, security response, and call to emergency dispatch.

Some Advice about Choosing the Right Type of Exercise

- Start with an assessment of what objectives you or your team believe will be of the most value and then choose the type of exercise that best fits your needs.
- Develop a logical sequence of exercises. For example, using a single scenario, it usually makes sense to run a tabletop exercise before attempting a functional exercise. Similarly, drills should be used to test and refine important functions before they are incorporated in a functional exercise.

- When conducting a drill or functional exercise, choose a function that is in most need of rehearsal. You may have experienced problems in the past or the function may be particularly important given high risk scenarios.
- When choosing a scenario for a tabletop or functional exercise, don't pick a scenario that is too challenging. There are two negative consequences of choosing an overly challenging scenario. First, so much will not work right that it will be difficult to tease out which problems are most serious and in need of correction. Second, participants may feel disheartened and less likely to fix those problems and plan another exercise.
- When choosing a scenario for a tabletop or functional exercise, don't pick a scenario that is too easy. If the scenario is too easy, you will not achieve enough benefits to justify the time and energy needed and participants may feel that their time has not been well spent.
- If you are planning a table top or functional exercise, select a scenario that is important based on your risk analysis. If you are planning a drill, select a function important to several scenarios.

HELPFUL TIP

To be effective, exercises and drills should be carefully planned and the actual exercise should be evaluated.

Planning the Exercise

Who plans the exercise?

Typically, the same team that writes your emergency plan should plan drills and training exercises. Sometimes, the exercise may not be relevant to someone on the team, and they can be excused from this responsibility. For example, a team member responsible for your organization's business recovery and operational continuity may have little role in planning a drill limited to evacuations. But be careful. This person may have something important to say about actions needed to preserve records needed that the organization will need after an emergency.

The planning process

Exercises must be carefully planned. As an example, inadequate planning during fire drills is common when building occupants conduct fire drills.

- Little effort is made to collect information that is invaluable to improving their preparedness.
- Alarm signals may not have been heard in parts of the building, but this critical information is not collected or used.
- Some building occupants may refuse to participate, but no effort was made to discover why they declined to participate and how their concerns might be better accommodated.

Each exercise involves three distinct phases. These apply to all three types of exercises. (In a tabletop exercise, the execution and follow-up phases are likely to be accomplished at the same meeting):

1. Planning
2. Execution
3. Evaluation

Planning Steps

1. *Review plan.* Make sure that the exercise is consistent with the plan. Take this opportunity to correct problems with the plan.
2. *Address costs and liabilities.* Make sure that needed personnel and facilities are available. Ensure that salaries of personnel are covered, and that you can pay for incidentals such as materials and refreshments. Make sure that your liability insurance will cover any injuries that could occur during a drill or functional exercise.
3. *Acquire organizational support.* Make certain that you have the support of executives and board members. Make sure that they clearly understand the necessity of the exercise and that you are attempting to minimize disruptions. If needed, have your executive or board write a memorandum requesting the cooperation of key people.
4. *Assess roles and capabilities.* A single person should have the authority to undertake the principal design and execution of the exercise. However, in many situations, you may need to assemble a team to help. Representatives will probably be needed when the exercise requires cooperation from different organizations or organizational units.
5. *Set performance objectives.* Performance objectives are needed so that you can judge how well the plan worked as reflected in the exercise. Performance objectives are usually qualitative. Examples include whether participants clearly understood and executed their roles and whether communications were effectively transmitted, received and understood. Some performance objectives can be measured quantitatively. Examples might include when did the last occupant evacuate the building, and how many children were unaccounted for at the assembly site.
6. *Design procedure.* Drills are relatively straightforward and involve selecting an appropriate trigger. Tabletop and functional exercises are more involved because they require scenarios. Write a narrative based on your selected scenario. If you plan to conduct an exercise that requires input to the process beyond the narrative, you will need to design events and messages. Events dictate how the scenario plays out after the narrative ends and the exercise begins. Messages convey information about those events to participants. Each message needs to include a source, the method of transmittal, the content and the recipient.

QUICK TIP

In every phase of emergency planning, make certain that you have the support of the professional and lay leadership.

7. *Expected Actions.* In response to the narrative and events, you are likely to want your participants to complete certain actions and make certain decisions. These actions and decisions should be so closely tied to your objectives that their completion serves as a benchmark about the success of your exercise in meeting your goals. For this reason, you might want to start by writing your expected actions and decisions, and then design your narrative and messages to evoke those actions and decisions. However, keep in mind that you should rarely blame your participants for not performing expected actions. Instead, look for ways to improve both your plan and your training. Sometimes your participants may have thought of an approach that is better than your plan. FEMA lists four types of actions that you should consider:

- a) Deploy or deny resources
- b) Gather or verify information
- c) Consider information, discuss among players
- d) Defer action to later, prioritize activities

Execution steps

1. Prepare facility. Acquire and place the needed materials.
2. Brief participants. Unless you are running a surprise drill, you need to provide the participants with accurate expectations about what they are supposed to do. This would include providing the scenario narrative that sets the stage for the exercise.
3. Conduct exercise. In an exercise, this includes providing messages about events that are supposed to have occurred during the evolution of the scenario.
4. Document actions and measure the accomplishment of objectives. Make sure you have adequate observers or evaluators to document actions and measure objectives. Do not realistically expect the participants to recall this information.

Evaluation phase

1. Assess achievement of objectives. Remember to use your expected actions and decisions as criteria. Use quantitative measures where possible, but do not ignore qualitative measures.
2. Have post exercise meeting(s). Tell your participants how well the exercise worked by using your measures of achievement. Give everyone an opportunity to provide feedback and to suggest improvements.
3. Prepare documentation. You will need this information to maxi-

HELPFUL TIP

In a well-designed exercise, you can discover significant problems and improve the plan and its implementation.

mize the value of future drills and exercises.

4. Follow up with improvements to the plan. In a well-designed exercise, you will have discovered significant problems where you can improve the plan and its implementation. Some improvements that can potentially result include:
 - a) better standard operating procedures and guidelines
 - b) better or more operations equipment
 - c) identification of gaps in training and education
 - d) better management and coordination
 - e) suggestions for drills and exercises that will continue to improve your plan and associated operational responses

Writing Scenarios for Tabletop and Functional Exercises⁸

Tabletop and functional exercises are typically built around a scenario. In this manual, we recommend that you use scenarios as the basis for developing your emergency plan. The same scenario should serve as the basis for developing your exercises.

Tabletop and functional exercises are typically introduced by using a scenario narrative—a story that details a series of events that precedes the start of the exercise. Narratives typically have more detail than scenarios so that they are more realistic and so that they can include contingencies to which the participants need to adapt.

An example of a few narratives follows:

- It is 9:30 a.m. and one of the teachers hears some commotion outside. He looks out the window and sees people running down the street. A few moments later he hears some sounds that could be gunshots.
- It is 3:30 p.m. and the receptionist receives a telephone call from a Ms. Tennyson asking for the “manager in charge.” The receptionist asks what the call is regarding, and Ms. Tennyson explains that there has been a train derailling on the nearby tracks and that emergency services have asked all of the facilities within a five-mile radius to prepare for a possible evacuation.
- It is now four days since a large earthquake required the sudden and total evacuation of the building. The facility director has received a telephone call informing him that two people will be allowed to enter the building for a maximum of 10 minutes to retrieve essential documents.

QUICK TIP

Tabletop and functional exercises are typically built around a scenario.

⁸ Other examples of drills and exercises can be found at <http://mcoeweb.marin.k12.ca.us/emmerprep/Guide.PDF> and <http://mcoeweb.marin.k12.ca.us/emmerprep/SAMPLE%20DRILL.PDF>

PROTECTION STRATEGIES

“Protection strategies” will help you react to life-threatening emergencies. Simply put, in dangerous situations people have to be moved out of danger or sheltered from danger in some way. Evacuations move people from a dangerous location to one of comparative safety. Sheltering-in-place and lockdowns are used when the greater danger is external. Duck, cover and hold is an interim tactic for earthquakes. Together, these are the basic protection strategies.

The following chapters discuss some of the protection strategies and tactics available to you.

EVACUATION TACTICS

Whether the danger is from fire, bomb threat or something else, an effective evacuation strategy is one of the most critical components of life safety preparedness. The evacuation system identifies the strategies and procedures for efficiently and effectively notifying, relocating or evacuating occupants.⁹ This chapter relates closely to the one on response teams and focuses on special strategies of evacuation using ICS,

Building occupants' panic during the early stages of a fire can contribute to high casualty losses. Smoke, gases and super-heated air make it imperative that an emergency evacuation program be established for all institutional buildings.

The potential for high human losses makes it imperative that evacuation strategies be reviewed and updated as necessary. Uncontrolled evacuation complicates emergency situations. Because of differences in design, construction, fire-resistant qualities, height, floor layout, usage and occupancy, each building presents unique problems in emergency evacuations. For this reason, information contained in this chapter should be considered a guide to evacuation strategies rather than a specific program customized for a particular building. State or provincial and local codes and regulations concerning fire and emergency evacuation requirements should be checked, and, where variances exist, the more applicable measures should be adopted. Fire control and evacuation authorities (fire department, emergency management, consultants and insurance company or the OSHA evacuation etool at <http://www.osha.gov/SLTC/etools/evacuation/>) should be consulted for suggestions appropriate to a particular building.

REMEMBER

Uncontrolled evacuation complicates emergency situations. Evacuation strategies must be reviewed and updated as necessary.

Evacuation planning

Evacuation systems contain the following elements:

1. Emergency escape routes, whether evacuation will be from the entire building or a section of it;
2. Naming and training an evacuation team responsible for command, communication, supervision, first aid and searching the premises;
3. Procedures for employees who must remain to operate critical equipment;
4. Procedures to account for staff, students, clients and visitors;
5. Communication devices and alternative, back-up methods to initiate the evacuation; and

⁹ Some of this chapter is based on *National Safety Council Data Sheet 1-656-Reaf*: 85. Permission to reprint granted by the National Safety Council, a membership organization dedicated to protecting life and promoting health.

6. Communication devices and alternative, back-up methods to contact the fire or police departments.
7. Rehearsal, drill and evaluation.

Evacuation plans should be written! The evacuation team should be trained and the plan rehearsed and evaluated with the lessons learned from rehearsals and drills used to modify the plan. For example, toddlers and seniors take longer to evacuate than teens. If all the means of egress are blocked, will the evacuation be effective? Evacuation planners should think through various evacuation scenarios and experiment with different ones during drills.

Inspection and Evaluation

A complete inspection of the building should be made to ascertain regular and special needs before establishing an emergency evacuation program. Fire prevention specialists should be consulted, and the program evaluated by means of regular inspections. This is also necessary whenever changes are made to physical structures in the building, and for remodeling or renovating of quarters. (See checklist following this chapter.)

Regular inspections of all of your facilities should be made using an inspection and evaluation team that includes a representative of the facilities management, the safety/security manager and the emergency team captains of the areas being inspected.

Emergency escape routes

Floor plans, instructions and evacuation routes should be conspicuously posted throughout the building (e.g., halls, back of classroom doors) showing exits, primary and secondary evacuation routes, accessible egress routes, areas of refuge, fire alarm boxes, fire extinguishers and hoses. Floor numbering and direction of travel should be indicated in stairwells.

These plans should be regularly reviewed to ensure that items such as building occupancy, building construction and staff changes are reflected. Emergency fire procedure information should be prominently posted in corridors, near elevators, etc.

Areas of Refuge

Institutions should have pre-determined areas of refuge to use during evacuations. In case of bomb and other threats, the building occupants will have to move to an area some distance from the target building. Institutions should identify a nearby site where evacuees can move and be sheltered from the elements. (The first order of business upon reaching the area of refuge should be to account for all of the occupants of the evacuated build-

PLANNING TIP

Evacuation planning is best accomplished as a team effort with the programming, operational and/or educational staff working with the security staff, maintenance staff and others.

ing.) Classes, and similar groupings, should be kept together to facilitate the head counts.

While planning for evacuations, consult with fire officials in order to ascertain where they would stage their equipment so that the planned area of refuge does not interfere with the emergency responders.

One of the best ways to accomplish an appropriate area of refuge is to develop mutual assistance pacts with neighboring institutions (see the chapter on [Mutual Aid and Assistance](#), P. 111).

Emergency communication

Emergency communication systems should be in place, both to immediately notify the authorities of the emergency as well as inform the occupants to evacuate (see the chapter on [Emergency Communication Tactics](#), P. 139). You may eventually need phones to notify families or others.

Alarms

The most sophisticated systems perform both tasks automatically: sensors signal a central station or fire department of the location of a fire and trigger local alarms within the building.

The evacuation plan should indicate the type and location of alarms—are the smoke detectors connected to a building-wide alarm system, must alarms be pulled manually, and does the system signal the fire department? No matter how sophisticated the system, provisions must be made to alert everyone in the building of the possible danger.

Detection, automatic alarm systems or automatic sprinkler systems should be a part of the total fire protection preparedness program. However, if fire is detected or the start of a fire is witnessed, it should be reported immediately. Delays in reporting fires because of heroic but ineffective firefighting can result in needless time loss and allow a simple fire to get out of control. Fire-reporting systems must be handy (such as pull-boxes located around the building), direct and not subject to any delay. Reporting by telephone or personal contact should be discouraged when faster means are available.

Communications within the building

Public address systems and intercoms can supplement alarms. An adequate and effective system for two-way communications should be provided for every floor or area. The communication system will be used to direct the work assigned to floor evacuation teams and to assist in communications between the building's communications control center and fire department personnel using the system during firefighting and evacuation emergencies.

PLANNING TIP

One of the best ways to secure space to set up areas of refuge or access to backup facilities is by negotiating a mutual assistance pact with a neighboring institution.

Two-way systems are best because specific information regarding conditions can be passed back and forth.

It's a good idea to maintain a central list of staff cell phone numbers as another backup method of communication. Staff should be trained to turn on their cell phones in the event of an alarm.

Finally, the evacuation team should include “runners”—individuals who, if all else fails, can be used by the evacuation leadership to communicate.

Supplies

Go Kits (see [Supplies and Go Kits](#), P. 146) are prepared and maintained so that when the decision to evacuate or shelter-in-place is made, those affected will have, readily available, basic provisions and tools for coping with the task at hand.

Ideally, there should be several classes of Go Kits. Someone must be assigned the responsibility to maintain the Master Go Kit and the appropriate (redundant) backups. The master kit addresses the needs of the institution, in terms of tracking and managing people, detailing facilities and critical infrastructure and supporting the initial recovery process. Duplicate kits should be maintained off-site, especially the documentary portion of the kits: master lists of personnel, blueprints of building layouts and critical infrastructure and the Emergency Management Plan itself.

Additionally, area supervisors and individuals should have accessible individual Go Kits. For example, each teacher in a school should have a kit that will address his or her needs as well as those under that person's supervision. Moreover, each student should have a personal “Go Kit” stored and accessible. While these kits may seem like a lot to assemble and maintain, they are indispensable for an effective response to an emergency situation.

Each school or building should develop a master GO Kit that is readily available for use during an emergency situation. The Go Kit should be kept updated and should be readily accessible to use by the evacuation team in an emergency. The Go Kit, or a duplicate Go Kit, should be maintained in a safe, accessible area outside of the school building.

PLANNING TIP

Items such as tools, flashlights and batteries, water and first aid supplies are kept in a Go Kit. It also includes a binder with the plans of your building, attendance lists and contact lists.

Evacuation response

Command structure of emergency evacuation teams

The evacuation response command structure is based on your ICS tool. Each building should have an Incident Commander/Chief Fire /Safety

Warden (usually the Principal or Executive Director) and a deputy/backup. Other key staff positions include:

1. *Visitor liaison.* One or more members of the evacuation team should be trained and have responsibility of heading the evacuation of visitors, service persons, and others occupying the building during an emergency.
2. *Parent liaison.* The evacuation team should include one or more individuals to communicate with parents. If parents and their children are in separate programs in the same facility, the parents should be informed where their children's area of refuge will be. Parents trying to proceed to their children's program location can slow the evacuation.

Operations

The Operations section has deputy wardens (authorized to act in the absence of the chief warden, a.k.a. the incident commander) with responsibilities for areas of a building, area captains responsible for a particular floor or building area and searchers (responsible for checking unsupervised areas such as bathrooms). There must always be a trained substitute to take over in the absence of any fire/safety warden or acting fire/safety warden or area captains who may be out of the area, ill or on vacation. A system of alternates should be established so that no area evacuation team is depleted for even as short a time as a lunch period. If there is more than one shift, each shift should have its own emergency evacuation floor team.

In classroom settings, teachers are responsible for their students' safety and should be prepared to take attendance once the group reaches the area of refuge and report anyone that is missing. Substitute teachers must know their responsibilities.

Searchers

Each area evacuation team should include "searchers" who make sure that every person on a floor is aware of an emergency evacuation. Depending upon size and occupancy of building, searchers may need a list of programs or classes and individuals with disabilities. Searchers should be trained members of the emergency evacuation team. They should check lavatories, empty classrooms, unstaffed and isolated areas of each floor. Searchers should check for visible presence of occupants rather than a voice response from a possible occupant who might not hear, be temporarily indisposed, or rendered unconscious.

REMEMBER

During evacuations the first thing that rescue workers want to know is, "did everyone get out OK?" People should immediately go to their areas of refuge, take attendance and report back.

Other team members

It is important to delegate duties to members of the evacuation team, both for evacuations themselves and “evacuation maintenance.” Specific evacuation team members should be assigned to:

- individuals with disabilities (see [Persons with Disabilities](#), P. 159);
- shut down critical systems;
- take the latest computer backup;
- stairwells and elevators (if elevators can be used during the evacuation);
- first aid, CPR and emergency defibrillation with access to the appropriate equipment; the Red Cross suggestions are found at <http://www.redcross.org/services/disaster/beprepared/supplies.html> and a supply list by Harvard can be found at <http://www.health.harvard.edu/fhg/firstaid/kit.shtml>.
- establish a regular inspection program, including proper documentation, to maintain the detection and communication system in the best operating condition; and
- keep the class lists, faculty lists and parent contact lists up-to-date.

The evacuation team should remember that emergencies often occur at the least convenient times. Lunchrooms, assemblies and swimming pools all need coverage.

See the accompanying “Self-Evaluation Checklist” for details on evacuation team assignments.

PLANNING TIP

Make plans for complete and phased evacuations and decide when each is appropriate.

Evacuation Plan Considerations

In the event of emergency, the area captain should be assigned the authority to order evacuation of a given floor or several floors of the building. (Alternative individuals should be designated in case the primary authority is not available.) Additional floors may be evacuated at the direction of the local fire department.

Floors to be evacuated

In “fireproof” buildings it is sometimes preferable to evacuate an “at-risk” section of the building first and to delay on ordering a total evacuation.

Generally, evacuation will be from the floor on which the emergency has occurred and the two floors immediately below and above the “emergency floor” to a safe point below or above the critical area. The construction of the building will be an important factor when considering the direction of the evacuation and the number of floors to be evacuated. Often, the building’s architect or engineer will provide guidance about evacuation.

Evacuation should be accomplished by way of fire stairwells. If smoke or fire has penetrated a stairwell, alternate stairwells should be used. In the event of “bomb-threat” emergencies, the evacuation order will be controlled by joint decision of the police and fire department in consultation with building management. Often such decisions are left to the building management by emergency responders. Elevators can be used for “bomb-threat” emergencies, but never for fire emergencies.

The evacuation plan should provide for personnel who will proceed immediately to fire stairwells and assist in the evacuation of occupants of the involved floor or floors.

Elevator control

Immediately upon recognition of fire emergency, all elevators should be returned to the lobby floor in accordance with the American National Standard Elevator Code.

Automatic devices should be installed to allow elevator cars to bypass all fire-involved floors. Under no circumstances should elevators be stopped at the fire-involved floors.

All occupants of the building, including visitors, must be informed that there will be no elevator service to or from emergency floors, and that they must evacuate by way of fire stairwells to refuge areas or beyond.

Physically handicapped occupants should be moved down the fire stairwell to the uppermost floor served by an uninvolved elevator bank, and then moved by elevator under the direction of fire officials. Seriously handicapped persons should be assisted by assigned floor evacuation team members.

Evacuation control

The direction of traffic should be related to the number of persons on each floor, the number of emergency stairwells available, and the number of floors directly exposed to the fire or emergency.

Evacuation priority. Occupants should be notified to evacuate through the emergency communication system. Priority must be given to those floors directly involved (in case of fire or chemical spill) and floors immediately adjacent to the emergency.

Method of evacuation. The Chief Fire/Safety Warden will determine the safest and most efficient means of evacuation, depending on the nature of the

REMEMBER

During most evacuations it's dangerous to use the elevators.

emergency and scope of damage. This decision should be made known to all area captains. Area captains on the endangered floors should be notified first.

To regulate flow, and to control the number of building occupants moving down single stairwells, alternate floors may be assigned different stairwells, thus providing an interval of two full flights between evacuating floors. (Actual floor numbers, rather than odd or even, should be used when the building has no 13th floor number.)

On the emergency-involved floor, evacuation should be to the nearest available exit that can be reached safely.

Provisions should be made, and directions provided, to ensure that occupants move away from the building to the area of refuge to facilitate a “head count” inventory of evacuation.

QUICK TIP

New employees and clients need basic safety training and everyone needs regular “refreshers.”

Training

Employees should be trained in the procedures found in the evacuation plan. Awareness of the evacuation plan should be an important part of new employee orientation and regularly discussed at staff meetings. Employees should be well aware of the nature of the alarm system (is it local or connected to a central station?), how to operate it, the various means of egress, the designated areas of refuge and their specific assignments in case of emergencies. Requirements for multi-language announcements and instructions should be considered.

All staff members should be trained to be part of the emergency evacuation team. Training sessions should review basic fire safety information such as shutting the windows and doors as they leave a room, testing a door with the back of their hand before they open it, to proceed into the hall and to keep low in case of smoke.

Every staff member should learn where the closest fire extinguishers are, on what type of fires they can be used and how to use them. For their own safety they should be on the lookout for stored items blocking evacuation routes. Organizational emergency protocols, defining “imminent danger” situations, the proper method to report a fire or bomb suspicion or threat should be taught, and briefings should include tips on “keeping your eyes open” for suspicious objects and how to report them.

Semiannual or quarterly refresher training of emergency evacuation teams should be scheduled. Many jurisdictions require written records of training

sessions.

Community-wide evacuations

There may be situations when authorities order facilities to close. Whether the cause is weather or terrorist-related, confirm that the proper authorities have assessed that it is safe for the building occupants to travel and that their destination is as safe or safer than your building (e.g., to send someone from a school to a mobile home during a tornado warning may not be the ideal scenario). Consider the kind of vehicles needed for a community-wide evacuation and create a plan that includes a priority list of equipment and supplies that should be moved to your alternate location. Survey your sister agencies to ascertain what kind of equipment they might be able to lend in the event of an evacuation?

Another major consideration is children. Parents rightly expect schools to maintain their children in a safe environment throughout the school day. If a mass evacuation is ordered, parents should be contacted as soon as possible and provisions must be in place to adequately supervise children until they are picked up by their parents (or the parent's designates). It's a good idea to have parents designate additional contacts out of the region so that you can contact them if you can't reach the parents in a reasonable period of time.

As always, you and your staff should plot various evacuation scenarios. By doing so, you can identify the equipment necessary and develop plans for best achieving an evacuation.

Communication tactics

If there is a community-wide evacuation you must have the capacity to communicate with your core constituencies, even though they may be spread over a wide area.

- Websites can be valuable tools. Plan to be able to change your website from a remote location. If your website server goes down can you redirect your web address (URL) to a functioning server with critical information? Do you have your basic website structure "backed up" off-site so that you can re-establish your web page? Do you have the information and passwords necessary to redirect your URL?
- Sometimes local phone service will be down while long distance

PLANNING TIP

Don't allow drills to become rote. Vary the times, circumstances and throw in a few "curves" to keep people on their toes.

service remains functional. Have the phone numbers of several people out of the region. You can try to call them and have them relay the call.

Drills

Emergency evacuation drills are exercises performed to train and evaluate the efficiency or effectiveness of occupants and staff in carrying out emergency evacuation procedures. Regularly scheduled emergency evacuation drills are required by law in most buildings. An emergency evacuation drills program should be established that will include periodic practice of movement of occupants to areas of refuge. The frequency of these drills—monthly, quarterly, etc.—depends on local fire codes and the staff and occupant turnover in the institution. New employees, new students, new campers and new program participants should all experience drills soon after starting their programs.

The drill should include the progressive movement of personnel to areas of safety (i.e., to evacuate the people most in danger first). The purpose of “progressive movement” should be explained to the occupants at this time—to keep all occupants a safe distance from the fire hazard without evacuating the building all at once.

Drills should include rehearsals of basic fire safety techniques. Someone should be assigned to close doors and windows. Leaders should test the temperature door with the back of their hands before they enter the hall. Evacuees should be instructed to stay low if they smell smoke.

Don’t allow drills to become a “rote” experience. They should be at different hours. In schools, drills should be conducted during lunch and “class change.”

Special conditions can be simulated. Surprises can help everyone refine their fire safety consciousness. Erect a sign saying, “FIRE HERE” somewhere in the primary evacuation route to force evacuees to rethink (and recall) the secondary route. Drama can be helpful. Use dry ice and fans to simulate smoke so that the evacuees remember how to act. Use the rehearsals to experiment in order to ascertain the fastest way to evacuate the building.

Many jurisdictions require institutions to keep records of drills. Records should include the person in charge of the drill, the date and time, notification method(s) used, evacuation team members participating, special conditions simulated, problems encountered and the time required to evacuate.

EVACUATION PREPAREDNESS SELF-EVACUATION CHECKLIST

Note: All questions in this checklist should be answered with “yes,” “no,” “NA” (not applicable), or “U” (undetermined). For all answers that are not “yes,” or “NA,” the specific areas needing correction, the persons responsible, etc., should be noted in the “comments” column.	Yes/ NA	No	U	Comments
<p>Floor Diagrams:</p> <p>Are floor plans prominently posted on each floor?</p> <p>Is each plan legible?</p> <p>Does the plan indicate every emergency exit on the floor?</p> <p>Is a person looking at the plan properly oriented by an “X” (i.e., “you are here”)?</p> <p>Are room number identifications for the floor as well as compass directions given?</p> <p>Are directions to stairwells clearly indicated?</p> <p>Are local and familiar terms used on the diagram to define directions to emergency exit stairwells? For example, are particular areas identified, such as mail room, cafeteria, personnel department, wash rooms and lavatories, etc.?</p>				
<p>Exit paths to stairwells:</p> <p>If color coding of pillars and doors, or stripes and markings on floors are used, are they properly explained?</p> <p>Is additional clarification needed?</p> <p>Are paths to exits relatively straight and clear of all obstructions?</p> <p>Are proper instructions posted at changes of direction en route to an emergency exit?</p> <p>Are overpressure systems and venting systems operational?</p>				

	Yes/ NA	No	U	Comments
Elevators: Are signs prominently posted at and on elevators warning of the possible dangers in use of elevators during fire and emergency evacuation situations? Do these signs indicate the direction of emergency exit stairwells that are available for use?				
Elderly and physically handicapped: Are there elderly or physically handicapped persons who will need assistance during a fire and emergency evacuation of premises? What provision is made for their removal during an emergency? Who will assist? How will the handicapped be moved?				
Emergency exit doors: Are all emergency exits properly identified? Are exit door location signs adequately and reliably illuminated? Do exit doors open easily and swing in proper direction (open out)? Are any exit doors blocked, chained, locked, partially blocked, obstructed by cabinets, coat racks, umbrella stands, packages, etc.?				
Are blockages prohibited and removed immediately? Are all exit doors self-closing? Are there complete closures of each door? Are all exit doors kept closed, or are they occasionally propped open for convenience or to allow for ventilation? NOTE: This practice must be prohibited.				

	Yes/ NA	No	U	Comments
<p>Emergency stairwells</p> <p>Are stair treads and risers in good condition?</p> <p>Are stairwells free of mops, pails, brooms, rags, packages, barrels, or any other obstructing materials?</p> <p>Are all stairwells equipped with proper handrails?</p> <p>Does each emergency stairwell go directly to the grade floor exit level without interruption?</p> <p>Does the stairwell terminate at some interim point in the building?</p> <p>If so, are there clear directions at that point that show the way to completion of exit?</p> <p>Is there provision for directing occupants to refuge areas out of and away from the building when they reach the ground floor?</p> <p>Are directions provided where evacuees can congregate for a “head count” during and after the evacuation has been complete?</p> <p>Is there adequate lighting in the stairwell?</p> <p>Are any bulbs and/or fixtures broken or missing?</p> <p>Where? Describe locations.</p> <p>Are exits properly identified?</p> <p>Are they illuminated for day, night, and power loss situations?</p> <p>Are any confusing non-exits clearly marked for what they are?</p> <p>Are floor numbers displayed prominently on both sides of exit doors?</p>				
<p>Emergency lighting:</p> <p>In the event of an electrical power failure or interruption of service in the building, is automatic or manually-operated emergency lighting available?</p> <p>If not, what will be used?</p> <p>Where are standby lights kept?</p> <p>Who controls them?</p> <p>How would they be made available during an emergency?</p>				

<p>Is there an emergency generator in the building?</p> <p>Is it operable?</p> <p>Is it secured against sabotage?</p> <p>Is a “fail-safe” type of emergency lighting system available for the exit stairwells that will function automatically in the event of total power failure?</p> <p>How long can it provide light?</p> <p>Is the emergency lighting tested on a regular monthly basis with results recorded? Who maintains such records?</p>				
<p>Communications:</p> <p>How should occupants of the building be notified that an emergency evacuation is necessary?</p> <p>Are one or more forms of communication system available to each floor? (P.A. system, Musak, stand-pipe phones, battery-operated “pagers,” cell phones, etc.)</p> <p>If messengers must be used, have they been properly instructed?</p> <p>Is the communication system in good working condition?</p> <p>Under what emergency conditions is it used and who operates it?</p> <p>Is the communications system protected from sabotage?</p> <p>Do all occupants know how to contact building control to report a dangerous situation?</p> <p>Is the building’s emergency communications system tested monthly? By whom and to what extent?</p>				
<p>INSPECTION COMPLETED BY:</p> <p>Name:</p> <p>Title:</p> <p>Date of Inspection:</p>				

SHELTERING-IN-PLACE & LOCKDOWNS

What if the emergency situation that you are faced with requires that you stay inside your building because there would be a greater danger in evacuating?

In emergencies, two protection strategies can be preferable to an evacuation: sheltering-in-place and lockdown. Sheltering-in-place procedures may be ordered in situations involving chemical leaks, biological or chemical attacks.

The purpose of lockdowns is to minimize accessibility to a school or rooms in that school, thus reducing the risk to staff, students or patrons of some sort of victimization from dangerous intruders. The recent series of attacks in the Washington, D. C. area by a pair of snipers is a good illustration of the need to designate a room or rooms for lockdowns. Under such circumstances, not only would everyone be compelled to stay inside the building, but they would need to be secured in a room that had no direct access to the outside.

Lockdowns might be necessary in situations of: persons armed with firearms on school property, gunshots directed at or near school and grounds, police incidents involving dangerous person(s) that are adjacent to or within a short distance of the school site, intruders, Plan on sheltering-in-place in the event of hazardous chemical spills, gas leaks, electrical conditions, or disasters close to the school or grounds. Severe weather conditions can also involve sheltering-in-place. These lists are not all inclusive.

Lockdowns involve securing the building from outside intruders and moving students away from exposed areas such as doors and windows. Ideally, clients, students and staff congregate in safe rooms, locked from the inside.

For more specific information on sheltering-in-place, see the Israel Defense Forces web site at <http://www.idf.il/english/organization/homefront/homefront2.stm> or a report from the Lawrence Berkley National Laboratory. at <http://securebuildings.lbl.gov/images/BldgAdvice.pdf> A good training document is available from the Centers for Disease Control at <http://www.bt.cdc.gov/planning/shelteringfacts.asp>.

QUICK TIP

Evacuations move people from areas of danger to areas of relative safety. These strategies keep people in, away from the danger.

Sheltering-In-Place Planning

Essentially, the procedures for both of these protection strategies are similar. The critical issue is the pre-selection of safe areas within your building. The best area for lockdowns may be dangerous for sheltering-in-place. Your planning should include the following elements:

- Identifying rooms that are internally located within the building, i.e., containing no windows and no external walls, with doors that lock from the inside.
- Naming and training a team (can be the same as the evacuation team) who will be responsible for directing personnel to the shelters.
- The designated rooms should be stocked at a minimum with canned food and bottled water, plus plastic sheets and tape to seal any openings in the doors in the event of a biological or chemical attack.
- Procedures to account for staff, students, clients and visitors.
- Communication devices and alternative, backup methods to initiate the evacuation to the designated rooms.
- Communication devices and alternative, backup methods to contact the fire or police departments.
- Rehearsal, drill and evaluation.

The same planning that should be done for evacuation strategies should also be done for sheltering-in-place. All of the same concerns are relevant; the only difference is that you will be moving people to a location inside of the building instead of outside. Planners need to consider various scenarios and revise strategies after conducting drills.

QUICK TIP

The critical issue is the pre-selection of safe areas within your building. The best area for lockdowns may be dangerous for sheltering-in-place.

Internal safe zones

Internal safe zones or “sheltering-in-place” areas are rooms that can be created or identified for people to occupy in the event of an outdoor chemical or biological release. The goal is to create areas where outdoor air infiltration is very low. Usually such rooms will be in the inner part of the building, with no windows accessing the outdoors. They should have doors that are fairly effective at preventing airflow from the hallways. At the minimum, there should be no gaps around the edges of the door, and preferably there should be a gasket to completely seal the room. If that is not pos-

sible, plastic sheets and duct tape should be helpful for sealing the openings in the event of a biological or chemical attack. Keep in mind, though, that not all adhesives have been tested for resistance to biological and chemical elements.

Bathrooms are a logical but usually bad choice, because they often have an exhaust duct that leads directly to the outside. If the exhaust fan is turned off, then the duct, which leads directly outside, can allow toxin-bearing outside air to enter the bathroom, which could be very harmful during an outdoor release.

Additionally, natural ventilation patterns⁹ can draw air into the bathroom from within the building, eventually contaminating the building during an indoor release. If the exhaust fan is left on, then air will be drawn into the bathroom from other parts of the building, which will eventually contaminate the bathroom.

Conventional doors can act as a pump—sweeping significant amounts of outside air into the safe room. If local building and fire codes permit, replacing the conventional door with a sliding door can substantially reduce this effect.

PLANNING TIP

Areas that might be safe for lockdowns (e.g., basements) are the worst places in case of the discharge of chemical or biological agents.

General Sheltering-in-Place/Lockdown Considerations

Planning

The plan should clarify the authority for declaring the emergency as well as staff responsibilities. Areas of responsibility include command (including backup decision makers), communicators (including announcers, runners and individuals assigned outside the building, if possible), area supervisors, room supervisors and searchers.

Initial announcement

Announce the sheltering-in-place procedure using the public address or intercom system. When a sheltering-in-place order is given, it should be given in “Plain English.” Do not use codes!¹⁰ No one can be sure that everyone in the building will know the code. If at all possible, 911 should be called prior to notifying the main office!

⁹ This is called the “stack effect.” Buoyancy-driven vertical air flow between floors of a building, caused by a temperature difference between indoor and outdoor air, will tend to rise (if indoor air is warmer than outdoor air) and escape through the upper parts of the building shell, and be replaced by air entering the lower part of the building. If the indoor air is cooler than outdoor air the reverse occurs.

¹⁰ Some people feel that there are two advantages to coded announcements: 1) the intruder is not further alarmed; and 2) there is less panic. The importance of clear and concise orders outweighs those considerations.

While sheltering-in-place and lockdowns are similar, make sure that the announcements are clear so people go through the proper procedures.

Staff responsibilities

- All staff members, who are in control of students at the time of the sheltering-in-place/lockdown, are responsible for their students at that time. Students without staff supervision must be directed to the nearest room by the searchers.
- All staff shall immediately secure their rooms and must also address any other pre-planned areas of responsibility. Minors should not be left without responsible supervision.

Securing each room

1) Room supervisors

- Close windows, blinds and in the event of a lockdown, cover the door glass. If you have metal doors, a piece of cardboard with magnets, cut larger than the door window, can be affixed to the door and moved over the window to cover it.
- Turn off lights.
- In the event of a lockdown, lock doors in area of assigned responsibility beyond your room/work area.
- When sheltering-in-place, use duct tape to seal the door.
- In the event of a lockdown, direct students to line up against the longest portion of the door wall. Record names/emergency numbers for those present and also list those now missing. Tape the list to a wall, close to a phone if possible.
- Have students sit so that they are below window height.
- Once your area is secure, do not let anyone in your room without confirming their identity.
- Staff should then use phones or intercom only if their room is called or there is a life threatening emergency in their room. Keep all lines of communication clear of non-emergency talk!

2) Searchers

- Take control of any wandering students.
- Check bathrooms, empty rooms, auditorium and other unstaffed areas.
- Upon completion searchers should re-enter their work area and lock themselves in, making sure the exterior door handle is in a locked position.

3) Reporting

- While it is desirable to have the various rooms or sections report that they are secure, such reporting is usually limited by the capacity of the communications system. A flood of calls to the Incident Commander may interfere with an emergency call. It is best to de-

PLANNING TIP

No matter how sophisticated your plans, worried parents will show up during emergencies wanting to take their child home. Make plans for, and assign talented staff to handle worried parents.

sign your response team so that section chiefs can ascertain whether their area is secure and only report problems.

- If the dangerous person enters a particular area, the person responsible for that area should report it to the Incident Commander, who will be coordinating with police. By doing so the police can track the dangerous person and appropriately respond.

Note: There are situations (police activity nearby) where a sheltering-in-place/lockdown is appropriate but activity *inside* the building can continue as usual. This guide suggests actions in extreme emergency conditions. Less restrictive sheltering-in-place/lockdown conditions may be used based upon facts known to the administrator in consultation with the proper authorities.

Subsequent announcements

After the initial lockdown announcement, consult with law enforcement personnel about whether a second announcement should be made describing the reason for the lockdown and a description of the suspect if available.

Parents

One other important consideration is to have a pre-designated site for parents to meet when there is an emergency that requires a sheltering-in-place or lockdown procedure. This site should be several blocks away from the campus and have plenty of parking. If possible, staff members should be designated to respond to this site immediately after the conclusion of the sheltering-in-place procedure to instruct parents on how the students will be released from school.

Rehearsals

Sheltering-in-place is very different from fire drills. A sheltering-in-place drill program should be established that will include periodic practice sheltering-in-place procedures. The frequency of these drills—monthly, quarterly, etc.—depends upon the employee/student turnover in the area. The schedule should be maintained and documented. The building's emergency plan should include a schedule of programmed fire, sheltering-in-place and evacuation drills. Fire, sheltering-in-place and evacuation procedures should be conspicuously posted in each room.

QUICK TIP

A chemical spill on the street is more likely than a terrorist attack. Your planning should consider all possibilities.

Specific Threats Requiring Sheltering-In-Place

Threats From Chemical, Biological and Radiological Agents

Chemical, biological and radiological (CBR) attacks may require a different type of safety approach from a physical assault from a person/people. Most experts who study terrorism are more concerned with the possibility of a small-scale CBR release in a relatively confined area than a large-scale, widespread attack. It is difficult to weaponize and distribute biological, chemical or radiological materials effectively, and therefore it is not easy to do large-scale damage.

CBR concerns are not limited to terrorist sources. Industrial chemical spills could have the same effect and require the same preparedness. As always, check with your local Office of Emergency Management and ask them to conduct a risk assessment of your facility. They should be aware of any factories, refineries or other repositories of toxic materials in your area. An industrial accident can be far more serious than a terrorist incident. Organizations located near such facilities should devote considerable resources to their evacuation and sheltering-in-place plans and preparations.

Chemical and biological attacks fall into two major categories: outdoor releases and indoor releases. The procedures to be followed vary by whether the release is outdoor or indoor, and whether it is chemical or biological. For an indoor release of either a chemical or biological substance, the priority is to evacuate the building and move upwind and uphill. For an outdoor release, moving everyone into pre-designated internal safe zones is the recommended procedure.

In the event of a chemical or biological attack, once it has been established that the attack has occurred outside of the building, all occupants within the building should be directed to a safe area in a room that is as remote and as sealed off from the outside as possible.

Post-release Shelter-In-Place Procedures

In the case of a chemical or biological attack, it is critical that a determination be made first as to whether the attack has occurred inside the building or outside. If it is established that the attack has occurred outside of the building, it is possible to minimize the risk of exposure by taking the following actions:

- Keep people indoors.
- Close all windows and doors to the outside.
- Close all internal doors.
- Shut off all HVAC fans and close all HVAC dampers, including ex-

haust dampers.

- Shut off other fans such as kitchen and bathroom exhausts.
- Do not use elevators—they create a piston effect and can pump air into or out of the building.
- Have people gather in pre-identified “shelter-in-place” rooms that have no or low air exchange with the outdoors and have low air exchange with the rest of the building.
- Once the outdoor concentration has diminished to safe levels (as determined by emergency response teams), evacuate the building and flush it with outdoor air. After the contaminated plume passes, the concentration of contamination will actually be higher inside the building than outside, because the building will tend to retain contamination that managed to enter.

Minimizing the rate of air exchange with the outside will keep the indoor concentration as low as possible for as long as possible. Normal operation of the HVAC system will exhaust some building air and pull in some outdoor air. If the outdoor air is contaminated, the HVAC system will spread the contamination throughout the building. Air exhausted from the building by exhaust fans will also be replaced by outdoor air. Shutting off the HVAC fans and exhaust fans will help minimize the air exchange with the outside. Once the emergency response teams have determined that the air outside is safe (generally not more than 2-3 hours), the building should be evacuated.

Lockdowns During a Threat by Dangerous Persons

Pre-planning and proper skill drills help eliminate mistakes and misunderstandings. Each building should maintain a written lockdown plan that is distributed to staff, posted and rehearsed.

Preparations should include having the necessary hardware in place so that a lockdown is possible. Doors should be lockable from the inside, but accessible through master keys. Do not retrofit doors with “sliding bolts” or similar hardware as these can be misused by an intruder taking hostages.

Can different parts of the building be locked? Plans must ensure that children outside their classrooms are moved to the closest safe area (and their teachers are notified that the children are accounted for). The safest part (e.g., away from doors and windows) of each “safe room” should be identified.

If possible, keep a reasonable amount of canned food and water available in the area designated as the safe area.

DUCK, COVER & HOLD

If your hazard analysis indicates the risk of earthquakes, you should plan and drill for that eventuality. The common protection strategy is known as, “Duck, Cover & Hold.”¹¹

Tips

When an earthquake strikes take immediate action:

- When in a *high rise building*, move against an interior wall if you are not near a desk or table.
- Protect your head and neck with your arms.
- Do not use the elevators.
- When *outdoors*, move to a clear area away from trees, signs, buildings, or downed electrical wires and poles.
- When on a *sidewalk near buildings*, duck into a doorway to protect yourself from falling bricks, glass, plaster and other debris.
- When *driving*, pull over to the side of the road and stop. Avoid overpasses and power lines. Stay inside your vehicle until the shaking stops.
- When in a *crowded store or other public place*, move away from display shelves containing objects that could fall. Do not rush for the exit.
- When in a *stadium or theater*, stay in your seat, get below the level of the back of the seat and cover your head and neck with your arms.

No matter where you are, know how to protect yourself and your clientele during an earthquake. Practice taking cover as if there were an earthquake and learn the safest places in your home and work. Practice getting out of your home and check to see if the planned exits are clear and if they can

¹¹ From Governor’s Office of Emergency Services, for more information see http://www.oes.ca.gov/CEPM2001.nsf/htmlmedia/body_dch_drill.html

become blocked in an earthquake.

Know how to turn off your electricity, gas and water. If there is a gas leak do not turn off the power until the gas leak is addressed. Turning off the electrical power could cause a spark leading to an explosion.

In the event of an earthquake, once you turn off your gas, only your utility company should turn it back on for safety reasons.



DUCK or DROP down on the floor



Take COVER under a sturdy desk, table or other furniture. If that is not possible, seek cover against an interior wall and protect your head and neck with your arms. Avoid danger spots near windows, hanging objects, mirrors or tall furniture.



If you take cover under a sturdy piece of furniture, HOLD on to it and be prepared to move with it. Hold the position until the ground stops shaking and it is safe to move.

Creating a drill scenario¹²

After school in New York City, Tremor Howard took a job out West. As a conscientious new teacher in the Hebrew school, he read all the materials given to him by the synagogue of East Cupcake. His classes and lesson plans are going well. It's two months into the school year, and . . .

He hears a low, rumbling or roaring sound. The noise builds, getting louder and louder, for about ten seconds. Then WHAM! There's a terrific jolt. He feels as if someone suddenly slammed on the brakes in the car, or like a truck just rammed into the side of the building.

One of the students shouts, "EARTHQUAKE, DROP AND COVER!" The floor seems to be moving beneath him. It's hard to stand up or even stay in your seat.

He notices that the students are taking cover under their desks as quickly and quietly as possible (thankfully the students have earthquake drills in public school). The students are waiting for instructions. He dives under his desk, too.

The shaking and commotion lasts as long as 60 seconds. The building is creaking and rattling. Books are falling from the bookcase. Hanging light fixtures and plants are swaying. Suddenly a pot falls to the floor and smashes. Tremor's desk begins to slide a little too.

The sliding reminds him and he calls out, "Stay put, be sure to stay in the covered position under your desk and hold on to the legs so that the desk cannot slide away from you."

He hears noises outside. People are shouting and screaming. The shaking is making some distant church bells ring and there are the sounds of crashing. Then there's silence. The shaking stops, and the room grows quiet.

Tremor is jolted into action and remembers what he should do next. "Please, everyone get back in your seats," he says, "it is important to sit quietly now and wait for instructions about what to do next. If it is safe to leave the building and evacuation is ordered by the principal, I will lead you outside to a safe place. Prepare to take cover again at any second if an after-shock strikes and the shaking starts again."

¹² Adapted from the School Earthquake Preparedness Guide, Arkansas Office of Emergency Preparedness, 1993.

Tremor checks if everyone is OK. He thinks, “Well, I don’t smell gas or smoke, that’s a good sign.” Soon the announcement comes over the PA system.

Questions:

1. What if there’s a power failure?
2. What if the PA system doesn’t work?
3. What if the halls or stairways are cluttered with debris—ceiling tiles or plaster from walls?
4. What if the halls are blocked by fallen lockers or trophy cabinets?
5. What if there’s smoke in the hallway?
6. What if the exit doors or windows are jammed and will not open?
7. Are the students prepared for aftershocks that could hit while they’re evacuating? (If this happens, students drop and cover where they are.)
8. What if there’s not a safe area to evacuate to? (There might be bricks, glass and debris piled up outside or electrical wires on the ground).
9. What if there are students with special needs?

The issues of communication, accountability, dismissals, etc. are virtually identical to those listed in the [Evacuation Tactics](#) (P. 51) section.

HURRICANES AND TORNADOES

The weather forecasters were tracking the third storm of the season, Hurricane Chaim, for a week. All too soon it became clear that the East Cupcake Federation Home and Hospital for the Aged was probably in its path.

The staff consulted with their local emergency management officials. Each forecast and every discussion caused more anxiety. The Home was probably at risk. Quickly, they reached a decision to evacuate the Home and move the residents to the West Cupcake Federation Home and Hospital for the Aged. The experts said that everyone would be safe there.

It was a dark and stormy night. It became darker and stormier. Some of the residents in West Cupcake were a little bit disoriented, but in general the plan was a model of efficiency, until . . .

Chaim didn't cooperate. It veered west and the West Cupcake Home ended up directly in the path. A good portion of the roof was ripped away. There was no electricity and no air conditioning, but everyone inside was safe.

Hurricanes

The good news about hurricanes is that the business of hurricane prediction is becoming more accurate. The bad news is that major components of forecasting are an art rather than a science. Nothing is perfect. Depending on location, similar considerations should be given to nor'easters and tropical cyclones. Consult with your local emergency management office.¹³

No storm combines duration, size and wind speed more destructively than a hurricane. Hurricanes cause damage in three ways:

- storm surge
- wind damage
- rainfall and flooding

¹³ For more information on hurricane and hurricane preparedness, see <http://meted.ucar.edu/hurricane/chp/hp.htm>, http://www2.sunysuffolk.edu/mandias/38hurricane/hurricane_introduction.html

Saffir-Simpson Scale for Hurricane Classification					
Strength	Wind Speed (kt)	Wind Speed (m.p.h.)	Pressure (millibars)	Pressure (inches Hg)	Storm Surge (ft.)
Category 1	65-82 kt	74-95 mph	>980 mb	>28.94 in.	4-5 ft.
Category 2	83-95 kt	96-110 mph	965-979 mb	28.50-28.91 in.	6-8 ft.
Category 3	96-113 kt	111-130 mph	945-964 mb	27.91-28.47 in.	9-12 ft.
Category 4	114-135 kt	131-155 mph	920-944 mb	27.17-27.88 in.	13-18 ft.
Category 5	>135 kt	>155 mph	<919 mb	<27.16 in.	>18 ft.
Tropical Cyclone Classification					
Tropical Depression		20-34 kt or 23-39 mph			
Tropical Storm		35-64 kt or 40-73 mph			
Hurricane		65+ kt or 74+ mph			

Storm surge is a dome of water that is pushed ashore by the storm. Historically, storm surge causes 90% of the deaths and damage caused by a hurricane. The storm surge can make landfall before or after a hurricane strikes (often related to the local tide table). Low-lying areas are most at risk.

The United States Army Corps of Engineers has surveyed most of the coastal United States, producing detailed SLOSH (Sea, Lake, and Overland Surge from Hurricanes) maps. Your local office of emergency management should have access to these maps. FEMA makes some local maps available at <http://www.esri.com/hazards/>. These maps show areas most at risk and those that are likely to be evacuated during hurricanes of varying intensities. These maps also identify areas susceptible to flooding.

Wind damage is usually a secondary problem in a hurricane that can still do significant damage by felling trees, power lines and utility poles, damaging buildings and sending debris flying.

Forecasting and preparations

Forecasters will issue a *hurricane watch* when there is a threat of hurricane conditions in 24-36 hours and a *hurricane warning* when dangerously high water and rough seas are expected in 24 hours or less.

Your emergency plan should anticipate which conditions would lead to closing of your facilities, if possible, and how to alert your clientele about that decision. The unpredictable nature of the storm should lead you to check your supplies and Go Kits (See [Supplies and Go Kits](#)). Remembering that multiple disasters often occur simultaneously, you should anticipate a power outage (See [Power Outage Tips](#)). You should also scan the area immediately outside your facility for objects that could be propelled by the wind and cause damage.

In areas where flooding might occur review your evacuation plans and move valuable objects to safer areas.

Often governmental officials order community wide evacuations in low-lying areas and/or those directly in the path of a significant storm. See [Community-wide evacuations](#) (P. 59).

Tornadoes

Although tornadoes occur in many parts of the world, these destructive forces of nature are found most frequently in the United States, east of the Rocky Mountains, during the spring and summer months. In an average year, 800 tornadoes are reported nationwide, resulting in 80 deaths and over 1,500 injuries.¹⁴

Tornadoes can occur at any time of the year. In the southern states, peak tornado occurrence is in March through May, while peak months in the northern states are during the summer.

When conditions are favorable for severe weather to develop, a severe thunderstorm or tornado watch is issued. Weather Service personnel use information from weather radar, spotters, and other sources to issue severe thunderstorm and tornado warnings for areas where severe weather is imminent. If a tornado warning is issued for your area and the sky becomes threatening, move to your pre-designated place of safety. Organizations should have someone assigned to monitor radio stations so that appropriate measures can be taken.

Institutions in “tornado alley” should consider specially-reinforced safe areas and be prepared to move occupants there in the event of a warning. Buildings without these areas should have a pre-designated shelter such as a basement.

If an underground shelter is not available, move into interior hallways or small interior rooms on the lowest level. Avoid auditoriums, gymnasiums and other large rooms with long free-span roofs. Corridors with exposed entrances (as opposed to interior hallways) can be dangerous. Avoid glass display cases, glassed-in stairwells and doorways.

It’s a myth that open windows equalize pressure and minimize damage when a tornado strikes. Opening windows allows damaging winds to enter the structure. Leave the windows alone and immediately go to a safe place.

¹⁴ For more information on tornadoes, see <http://www.nssl.noaa.gov/NWSTornado/>.

Since weather services can provide some warning about hurricanes and tornadoes it is imperative that a responsible individual monitor such information. Advisories are immediately passed on to the media. If no one is available to constantly monitor radio or TV there are numerous services that send weather alerts to E-mail addresses, pagers and cell phones. A list of some of these services can be found at the government weather web site, <http://iwin.nws.noaa.gov/emwin/winven.htm>.

Organizational plans

Develop a severe weather action plan. You should identify the area of your safest area(s) and have frequent drills. Some specific issues of concern:

- Make sure someone knows how to turn off electricity and gas in the event the building is damaged.
- Keep children in the building beyond regular hours if threatening weather is expected. Children are safer inside than in a bus or car. They should not be sent home early if severe weather is approaching.
- Lunches or assemblies in large rooms should be delayed if severe weather is anticipated. Large rooms, such as gymnasiums, cafeterias, and auditoriums offer minimal protection from tornado-strength winds.
- Move students quickly into interior rooms or hallways on the lowest floor. Have them assume the tornado protection position (shown below).

SUSPICIOUS OBJECTS, BOMBS AND BOMB THREATS

It could be a letter, an anonymous phone call or an unattended knapsack. Suddenly your institution and the occupants are placed at risk. What should you do? Should you be suspicious? When is your reaction legitimate? Are you ever overreacting?¹⁵

Bomb threats can be delivered in a variety of ways. Sometimes they are sent through the mails, but most frequently they are called in to the threat target. Occasionally the call comes through a third party, e.g., someone calls a local paper to say that a bomb has been planted at the East Cupcake Jewish Center.

Why?

There are two primary purposes for calling in a bomb threat. The first is that the caller genuinely has knowledge of, or believes that he (or she) has knowledge of, an explosive or incendiary device that has been, or will be placed, at the location and wants to minimize personal injuries and/or property damage. In these cases, the caller may be the person who placed the device or someone who has become aware of such information.

The second purpose is to create an atmosphere of anxiety, terror and panic that will result in a disruption of the normal activities at the facility where the device has supposedly been placed. The sender gets his/her wish whether there is a legitimate bomb or not.

As always, plan

Proper planning will instill confidence in the leadership, reinforce the notion that those in charge do care and reduce the potential for personal injury and property loss. Appropriate planning can also reduce the threat of panic, the “most contagious” of all emotions.¹⁶ Once a state of panic

QUICK TIP

A bomb threat either comes from someone with knowledge of a device and wants to minimize injuries or a person who wants to create an atmosphere of terror.

¹⁵ Much of this section has been adapted from Bomb Threats and Physical Security Planning, published by the United States Bureau of Alcohol, Tobacco and Firearms ATF P7550.2 (7/87).

¹⁶ Recent consequences of “sudden, excessive, unreasoning, infectious terror” at nightclubs resulted in people being unnecessarily crushed to death by stampeding club-goers. When terrorists unleashed sarin gas in the Tokyo subway, more people were trampled to death than died of the poison.

has been reached, the potential for injury and property damage is greatly increased. Panic and hysteria are two of the main goals of bomb-threat callers—with or without the use of an actual bomb.

How to prepare

To adequately prepare to cope with a bomb incident, you should develop two separate but interdependent plans: a physical security strategy (see [Security Planning](#)) and a bomb incident strategy. Physical security deals specifically with prevention and control of access to the building. The bomb incident strategy provides detailed tactics to be implemented when a bomb attack is threatened or carried out. An interactive planning tool for bomb threat response is available from <http://www.threatplan.org>.

QUICK TIP

“Hardening” your facility through security measures should make it harder for a “bad guy” to get in to place a device and also should reduce the places to hide one.

Physical Security Strategy

Physical security provides for the protection of property, personnel, facilities and material against unauthorized entry, trespass, damage, sabotage or other illegal or criminal acts.

Through proper preparation, the danger to your facility can be reduced. It is important to identify the areas of access that can be “hardened,” or made more difficult to breach. This will help deter a potential bomber or other assailant from attempting entry to your facility. You can also harden areas within your facility to reduce the number of places a bomb can be hidden. This will also help reduce the amount of time spent searching, if that is determined to be necessary.

Physical Security (Target Hardening) Strategies

No single security plan is right for all facilities. Most buildings were not designed with security in mind. Beyond the normal level of security planning and appropriate perimeter security, the following are general security recommendations that can help reduce your facility’s vulnerability to bomb attacks:

Building Exterior

Vehicles are a viable method for delivering bombs. They can be driven up and into the building or simply left nearby with the bomb inside. There are some steps that you can take to reduce the danger:

- Visitor parking should be as far from the building and sensitive areas (e.g., playgrounds) as possible. In an ideal world, visitors should park over 300 feet away from your facility or building complex.

- “Friendly” vehicles (e.g., employees or long-term clients/volunteers) should be identified with tags or stickers, and should be parked closest to your facility.
- Shrubs, bushes and vines should be kept trimmed close to the ground to limit their ability to conceal assailants and/or bombs.
- Consult with security experts whether bollards or security planters should be installed to deter a vehicle bomb.
- Window boxes and planters make good receptacles for bombs and should be removed unless absolutely necessary.
- Any remaining outside receptacle should be checked by members of the security staff on a regular basis.
- Staff members should take regular (daily or several times a day) tours of the building exterior to check if there are any suspicious objects placed near the building.
- Keep in mind that it is important to know what *belongs* outside the building in order to recognize something that is out of place.

HELPFUL TIP

Do a careful tour of your facilities and try to anticipate where suspicious packages could easily be hidden.

Building Interior

- Access to critical areas should be carefully limited to authorized personnel.
- All packages and materials should be inspected before being brought into critical areas.
- Security and maintenance personnel should be alert for people who act in a suspicious manner.
- Security and maintenance personnel should be on alert for packages, objects, items or parcels that are left alone or appear suspicious or out of place.
- Potential hiding places such as stairwells, empty offices or classrooms, and rest rooms should be included in routine tours and surveillance.
- Doors to areas such as boiler rooms, mailrooms, computer centers, switchboards and elevator control rooms should remain locked when not in use, and keys should be carefully accounted for.
- Trash areas should be free of debris, as bombs can be easily concealed in the garbage.
- If possible, visitors should be channeled through a reception area.
- Visitors should be asked to sign in and the person they are coming to visit should be contacted for approval before the visitor is given access to the building.
- Train staff to be alert for suspicious mail.

Special events

A [special event](#) (e.g., a lecture or speech by a prominent or controversial figure) is often “high profile,” with advertising and press coverage. These occasions might require extra planning, precautions and a review of your policies.

As a matter of course the Secret Service requires “bomb sweeps” of a protected facility by trained, explosives-detecting dogs. Does your event necessitate similar precautions? Should each attendee go through a metal detector and have his/her bags searched? If a bomb threat is phoned in, should you immediately evacuate even if such precautions have been taken?

Special events require close coordination with your local police to ensure proper security and crowd control. Make sure that you consult with them well in advance.

HELPFUL TIP

Special events require special security planning, including the possibility of bomb threats.

Ask for help

Work with your local police and/or fire department to develop your security and your bomb incident responses. If possible, have them inspect your building to identify areas where explosive devices could be concealed, and make sure that list is posted in the command center and available to all designated personnel. Learn about bomb disposal units and how and when to contact them. Find out if the bomb disposal unit will assist in searching your facility in the event of a bomb threat.

BOMB INCIDENT STRATEGY

Bombs

Bombs can be constructed to look like almost anything. Most bombs are homemade and do not look anything like the “stereotypical” bomb you might expect to find. People have hidden bombs in books, radios and other innocuous-looking packages.

Bombs can be delivered or placed in myriad ways, which makes it particularly important that you and your staff are alert for anything that looks odd or out of place. *If you do see something suspicious that you believe might be a bomb, call the police. Do not attempt to investigate it yourself. Do not move or disturb the object.*

Suicide bombers

Law enforcement officials are also concerned about the possibility of suicide bombers. Israeli counter-terror officials have been able to train the public to recognize possible bombers. A recognition card with tips based on their system can be found at www.perelmansecuritygroup.com.

Suspicious objects or packages

It's virtually impossible to predict what a dangerous object or package looks like. Problematic packages can also contain non-explosive dangerous substances, e.g., Anthrax. A flyer suitable for posting in your mailroom can be found at <http://www.fbi.gov/pressrel/pressrel01/mail3.pdf>. The FBI and ATF cite some physical characteristics of suspicious packages and letters, including the following:

- Excessive postage
- Handwritten or poorly typed addresses
- Incorrect titles
- Title, but no name
- Misspellings of common words
- Oily stains, discoloration or odor
- No return address
- Excessive weight
- Lopsided or uneven envelope
- Protruding wires or aluminum foil
- Excessive security material such as masking tape, string, etc
- Visual distractions
- Ticking sound
- Marked with restrictive endorsements, such as "Personal" or "Confidential"
- Shows a city or state in the postmark that does not match the return address
- Foreign Mail, Air Mail and Special Delivery

When a suspicious object or package is discovered:

1. Remain calm.
2. Ensure that no one moves or disturbs the suspected object.
3. Clear all persons from the immediate vicinity.
4. Call 911.
5. Retreat to a safe distance and warn others to avoid the area. Be available to provide the whereabouts of the suspected object to the police.
6. Wait for further direction from the Incident Commander.

7. Do not spread rumors.

Bomb threat response tactics

Phone threats

Everyone answering the phone should be trained how to handle a bomb threat (see [Telephone Bomb Threat Checklist](#) below). The checklist should be placed next to each phone. If possible, a system should be developed to signal a second person to listen to the call. Record the call if a recorder is available and take notes on the form.

After completing the primary steps of the checklist, people should be trained to call 911 immediately to report the threat, and then to call the designated Incident Commander or his/her designee.

Communications

People should be alerted that in the event of a bomb threat they should not use their cell phones, cordless phones or two-way radios, which might trigger a radio-controlled device. Communications should be limited to telephones and intercoms—if they are hard-wired—and bullhorns and runners.

If you generally use the fire alarms to signal an evacuation, how will the evacuees know that this is specifically a bomb threat evacuation? This might be germane if your fire evacuation strategy includes a phased evacuation or sheltering for the disabled. If your fire evacuation plan leaves people inside you might be leaving people in danger.

Call the Police Department at 911 and relay information about the threatening call. Did the caller appear familiar with building (by his/her description of the bomb location)? Write out the message in its entirety and any other comments on a separate sheet of paper and attach to this checklist. Hang up and dial *57 from the same phone (and phone line on a multi-line system, if possible) that the call was received in order to have the telephone company record the caller's number. Notify the appropriate authorities immediately.

Written bomb threats

When a written bomb threat is received, save all materials, including any envelope, package or container. Once the message is recognized as a bomb threat, handling should be minimized. Do not pass it around! It is important to try to retain evidence such as fingerprints, handwriting or typing,

LIFESAVER

In the event of a bomb threat people should not use their cell phones, cordless phones or two-way radio. They might trigger a radio-controlled bomb.

paper and postal markings. These will prove essential in tracing the threat and identifying the sender.

While written messages are usually associated with generalized threats and extortion attempts, a written warning about a specific device may occasionally be received and should never be ignored.

Deciding what to do

If a suspicious object is found or a threat is received by phone or mail, a decision regarding evacuation must be made immediately. While the use of bomb threats presents pranksters with a golden opportunity, most experts believe that in today's environment threats must be taken seriously. While statistically very few bomb threats turn out to be real, ignoring the threat can result in problems, e.g., if employees learn that a bomb threat was received and ignored, morale problems could result.

The Incident Commander must evaluate the threat and has to choose from three basic tactics:

- Ignore the threat.
- Search and evacuate, if warranted.
- Evacuate immediately.

There may or may not be time to consult with emergency personnel. In many cases the emergency responders leave the decision as to whether to evacuate to the principal or executive director.

Even if your policy is to evacuate immediately, it might be wise to have searchers quickly inspect the evacuation routes to ascertain if there are any suspicious objects. If, for example, someone left a device in your lobby, you might be sending people from a place of relative safety into danger.

There may be limited situations when there is time to postpone any evacuation while a search is conducted (e.g., the caller says that the bomb will explode in two hours). While many experts recommend making a thorough search before making any decision to evacuate, we feel that *absent any solid indication that the bomb threat is phony, it is wise to order an evacuation.*

Special circumstances might negate the generalized recommendation favoring immediate evacuation, e.g., for hospitals and nursing facilities. Every facility should have a decision plan in place, developed in consultation with

BOMB THREAT OPTIONS

- *Ignore the threat.*
- *Search and evacuate, if warranted.*
- *Evacuate immediately.*

local emergency personnel.

Another word of caution

Some people have used bomb threats for harassment, or simply to avoid a test in school. While evacuation is the safest policy, that policy can be modified in the event that a pattern of phony threats develops. However, be aware that there are other situations when individuals started by merely making threats and, when the threats were ignored, they chose to escalate and did something violent.

Bomb Incident Response

The bomb incident plan provides detailed procedures to be implemented when a bomb attack is threatened or executed.

Developing a response team module

Using ICS, establish a clear chain of command which will help inspire confidence, save lives and reduce panic.

Command

Using the three relevant bomb response tactics, the Incident Commander must make the relevant decisions and give clear directions. Command staff members perform their usual functions.

Operations

There are two critical operational components of the bomb incident plan: evacuation and search.

Evacuation. The evacuation team (see [Evacuation Tactics](#)) should be trained in how to evacuate the building during a bomb threat. You should consider priority of evacuation, such as evacuating the floor levels above and below the immediate danger area in order to remove those people from danger as quickly as possible.

Search. A unique and critical component of a bomb threat response is the search of the premises. After a threat is received the building must be searched. No one knows a building (and what seems out of place) better than its occupants. Emergency responders have differing policies as to searches. Some expect the building operators to conduct a search. Others will only conduct a search in conjunction with a building representative. Be sure to talk to the appropriate emergency agencies to ascertain their policy and assign responsibility.

¹⁷ As opposed to the evacuation searchers who check if all of the occupants have left the building.

Search Techniques

The building searchers¹⁷ should be trained in bomb search techniques. Volunteers should be solicited and team leaders assigned. Search personnel must be thoroughly familiar with all hallways, rest rooms, false ceiling areas and every location in the building where an explosive or incendiary device may be concealed. Usually the maintenance staff members are best suited for this task. They know the building and have keys.

When police or firefighters arrive at your facility, they will be unfamiliar with the particulars of the layout. After a room is searched it should be marked or sealed to indicate it is “clear.”

Evacuation teams should be trained in evacuation and search techniques only. They should not be trained to have any contact with the device, and if a device is located it should not be handled. Its location should be noted, isolated and a route back to the device should be clearly marked.

The following list of basic search techniques is based on the use of two-person search teams:

First Sweep

- When the team enters a room to search, they should separate and stand and listen carefully to familiarize the searchers with the “normal” background noise of the room.
- Today’s devices rarely emit a “ticking” sound. A “ticking” sound can also come from air conditioner fans, dripping sinks, etc.
- The senior team member should determine how to divide the room for searching, including floor-to-ceiling, furniture and other objects, into equal parts.
- The first search should cover from the floor to the average height of the furniture, which is usually approximately hip-height.
- After the room has been divided and a searching height has been determined, both individuals should go to one end of the room “division line” and start from a back-to-back position.
- Each person should work his/her way around the room, toward the other person, checking all items resting on the floor around the wall area of the room. This completes a “wall sweep.”
- Together they should check all items in the middle of the room up to hip-height, including the floor under rugs.
- This first sweep should also include items mounted on or in the walls such as air-conditioning ducts, baseboard heaters and built-in wall cupboards if those fixtures are below hip-height.

Second Sweep

- The senior team member again looks at the height of the objects in the room and determines the height of the second sweep. This is usually from hip-height to the chin or top of the head.
- The team returns to the starting point and repeats the searching technique at the new height.
- This sweep usually covers pictures on the wall, built-in bookcases and tall table lamps.

Third Sweep

- The third sweep is repeated at a new height, generally from the top of the head up to the ceiling.
- This sweep usually covers high mounted air-conditioning ducts and hanging light fixtures.

LIFESAVER

Under no circumstances should anyone touch a suspected device. That's a job for professionals.

Fourth Sweep

- If the room has a false or suspended ceiling, investigate it during the fourth sweep.
- Check flush or ceiling-mounted ventilation ducts, sound or speaker systems, electrical wiring and structural frame members.

Other

- After the searches are completed, conspicuously post a sign indicating "Search Completed" in the area, or place tape across the door and door jamb approximately two feet off the floor.
- Encourage the use of common sense and logic in searching.
- Do not rely on random or spot checking of only logical target areas—the bomber may not be a logical person.

To recap the sweep search method:

1. Divide the area and select a search height.
2. Start from the bottom and work up.
3. Start back-to-back and work toward each other.
4. Go around the walls and proceed toward the center of the room.

What if a suspicious object is located?

Under no circumstances should a searcher move, jar or touch a suspicious object or anything attached to it. The removal or disarming of a bomb

must be left to professionals. Personnel should follow these procedures:

1. Report the location and an accurate description of the object to the appropriate authority. Authorities should be met and escorted to the location.
2. Identify the danger area and block it off with a clear zone of at least 300 feet, including floors above and below the object.
3. Check to see that all doors and windows are open to minimize the primary damage from blast, and secondary damage from fragmentation.
4. Evacuate the building.
5. Do not permit re-entry into the building until the device has been removed and/or disarmed, and the building has been declared safe for re-entry.

TELEPHONE BOMB THREAT CHECKLIST

Instructions

Be Calm, Be Courteous. Listen. Do Not Interrupt the Caller. Keep the caller on the phone as long as possible and get as much information as possible. Ask him/her to repeat the message. Record every word spoken by the caller. A calm response to the bomb threat caller could result in obtaining additional information, particularly if the caller wishes to avoid actual injuries or death. If the caller is told that the building is occupied and cannot be evacuated in time, he may be willing to give more specific information on the bomb's location or components. Law enforcement agencies are most interested in the facts about the bomb. Alert the appropriate people and call 911. Then, hang up and dial *57 from the same phone (and phone line on a multi-line system, if possible) that the call was received in order to have the telephone company record the caller's number.

YOUR NAME:			Time:	Date:
CALLER'S IDENTITY SEX:	Male <input type="checkbox"/>	Female <input type="checkbox"/>	Adult <input type="checkbox"/>	Juvenile <input type="checkbox"/>
APPROXIMATE AGE:				
ORIGIN OF CALL:	Local <input type="checkbox"/>	Long Distance <input type="checkbox"/>	Telephone Booth <input type="checkbox"/>	Cellphone <input type="checkbox"/>

Bomb Facts

Pretend difficulty hearing—keep caller talking. If caller seems agreeable to further conversation, ask questions like:

When will it go off?	Certain hour time remaining?
Where is it located?	Which area of building?
What kind of bomb?	What kind of package?
How do you know so much about the bomb?	What is your name and address?

Your impressions about the caller's speech are important, but shouldn't require a lot of time.

VOICE CHARACTERISTICS		SPEECH		LANGUAGE	
<input type="checkbox"/> Loud	<input type="checkbox"/> Soft	<input type="checkbox"/> Fast	<input type="checkbox"/> Slow	<input type="checkbox"/> Excellent	<input type="checkbox"/> Good
<input type="checkbox"/> High Pitch	<input type="checkbox"/> Deep	<input type="checkbox"/> Distinct	<input type="checkbox"/> Distorted	<input type="checkbox"/> Fair	<input type="checkbox"/> Poor
<input type="checkbox"/> Raspy	<input type="checkbox"/> Pleasant	<input type="checkbox"/> Stutter	<input type="checkbox"/> Nasal	<input type="checkbox"/> Foul	<input type="checkbox"/> Other
<input type="checkbox"/> Intoxicated	<input type="checkbox"/> Other	<input type="checkbox"/> Slurred	<input type="checkbox"/> Other		
ACCENT		MANNER		BACKGROUND NOISES	
<input type="checkbox"/> Local	<input type="checkbox"/> Southern	<input type="checkbox"/> Calm	<input type="checkbox"/> Angry	<input type="checkbox"/> Factory	<input type="checkbox"/> Trains
<input type="checkbox"/> Foreign	<input type="checkbox"/> Northern	<input type="checkbox"/> Rational	<input type="checkbox"/> Irrational	<input type="checkbox"/> Machines	<input type="checkbox"/> Animals
<input type="checkbox"/> Eastern	<input type="checkbox"/> Midwestern	<input type="checkbox"/> Coherent	<input type="checkbox"/> Incoherent	<input type="checkbox"/> Music	<input type="checkbox"/> Quiet
<input type="checkbox"/> Hispanic		<input type="checkbox"/> Deliberate	<input type="checkbox"/> Emotional	<input type="checkbox"/> Office	<input type="checkbox"/> Voices
<input type="checkbox"/> African		<input type="checkbox"/> Righteous	<input type="checkbox"/> Laughing	<input type="checkbox"/> None	<input type="checkbox"/> Airplanes
<input type="checkbox"/> Slavic				<input type="checkbox"/> Street	<input type="checkbox"/> Party
<input type="checkbox"/> Other				<input type="checkbox"/> Traffic	<input type="checkbox"/> Other

Emergency Planning: *Disaster and Crisis Response Systems for Jewish Organizations*

Call the Police Department at 911, and relay information about call. Did the caller appear familiar with building (by his/her description of the bomb location)? Write out the message in its entirety and any other comments on a separate sheet of paper and attach to this checklist. Hang up and dial *57 in from

SECURITY PLANNING

In today's fast-changing world every public institution is reviewing its security situation. Jewish institutions should be changing their culture to institute measures to mitigate many situations ranging from terrorism to vandalism to workplace violence.

Emergency mitigation planning for Jewish communal institutions must include a security plan. A sound security plan will leave an institution in the best as possible condition to thwart and, if necessary recover from, a security breach. Remember: The best way to protect your institution is to prepare for and prevent an incident's occurrence in the first place.


A sound security plan in a Jewish communal institution is often as much a management issue as it is a technological one. It involves motivating professionals, leaders and community members to understand the need for security and to create and implement a coherent security plan.

Professionals and leadership should assess the risks and realities of the institution and develop a security plan— seeking professional guidance if needed. Of course, not all institutions run the same risk, but all run some risk. Most critically, leaders must make sure that security is part of an institution's culture. When planning or participating in events, everyone—ranging from the board president to the custodial staff—must think security.

Community members have an important role in helping to ensure the safety of their Jewish communal institutions. Leadership should help them know their role in a plan. They should:

- be watchful and be willing to report suspicious activity;
- know their building — report anything that is out-of-place or missing;
- actively cooperate with security directions, check-in procedures and ticket policies;
- help create a culture that is both secure and welcoming; care about this issue — and let people know that they do; and
- support the board and professionals when they make the decision to create and implement an effective security plan.



©  Since 1913, the Anti-Defamation League has worked “to stop the defamation of the Jewish people and to secure justice and fair treatment to all citizens alike.” Now one of the nation's premier civil rights/human relations agencies, ADL fights anti-Semitism and all forms of bigotry, defends democratic ideals and protects civil rights for all. As part of ADL's effort to protect the safety and well-being of the Jewish community, the League continues to provide the Jewish community with tools and training to effectively create secure environments.

Creating a Security Plan

While no guide can provide you with a one-size-fits all security plan, there are certain basic considerations that security planners must take into account. This chapter will help you understand those elements.

Analyze the risks and realities of your institution and create a security plan—seeking professional guidance if needed. ADL has published—and will continue to publish—material to help you through this process. Check the ADL web site for updated material at www.adl.org/security. Another excellent list of links for security information and resources is found on the National Clearinghouse for Educational Facilities web site, www.edfacilities.org/rl/disaster.cfm.

Merely creating a plan, and even installing hardware and/or hiring additional staff is not the end of the process. Once the plan is written, make sure that all leaders, employees and constituents know it, practice it, review it and implement it.

Creating a secure environment is a three-step process: Assessment, Planning & Implementation. You may wish to consult with your local police and/or hire a professional security firm for assistance in this process.

Assessment

Identify the potential threats specific to your institution:

- What does the news tell you about the current national and international climate?
- What do the local police and other information sources tell you about the local climate?
- What does your ADL regional office and/or local JCRC say about extremist and anti-Semitic activity in your area?
- Is there something about your building or your staff that would attract a terrorist attack, such as high-profile programs, high-profile members or an extremely visible building?
- Are you at risk from collateral damage from an attack on a high-risk neighbor (e.g., a family planning clinic)?
- Are you at risk from employees or other “insiders”?
- Identify what it is that you want to protect (e.g., people, property or data) and what makes them vulnerable. There are different strategies for protecting children, adults, property and data, and your planning must account for them. Note also that sometimes these things are related: the theft of a computer that contains member-

QUICK TIP

Security threats exist, even in low crime areas. You must have a security plan for your organization.

ship lists and payment information can do great damage to an institution's reputation and the members' safety.

- Remember that your local police department may have a crime prevention officer who will do an on-site security inspection and review your plan.

Planning

- Identify the most appropriate measures to reduce, and even in some cases eliminate, your risk. Your most appropriate steps may be as simple as replacing the locks to get control over who has keys to the building.
- Planning should include creating and maintaining a bomb search plan and emergency evacuation plan. This is an important time to contact and include your local bomb squad. They will help you understand what steps you are responsible for implementing in a bomb emergency (searching, see [Search Techniques](#), P. 88) and when they will come (many bomb squads will not come to a site until a suspicious item has been discovered). Your evacuation plan should include ways to notify and, if necessary, evacuate everyone in your facility in an emergency. Designate a meeting point (see [Areas of Refuge](#), P. 52) to ensure that everyone is safe.
- You should create plans that deal with the varied uses of your buildings. Schools, high-traffic events (such as the high holidays) and days when the facility is not used all create different security circumstances.
- Planning should include business recovery plans, which are discussed elsewhere in this manual.
- Work with security specialists, the police, other emergency services and ADL.

Implement

- Designate a security manager who is accountable for implementing, reviewing and constantly updating the plan. Make sure everyone is trained to implement the plan—especially those who will be on the front lines of using the plan and those who know your building best, your maintenance personnel. The security manager is responsible for continued training and for updating the plan.
- Training is critical: conduct communal and staff training, drills and role playing—and for regular refresher exercises. Drills and role playing ensure that the plan is workable, up-to-date and fresh in people's minds.
- At every stage, work to build relationships with your local emergency services, including police, fire and emergency management. Simply: Get to know them — and get them to know you, before

there is trouble. Invite local officers to use your gym, to join you for a events or to visit your building and get to know it.

Other thoughts about the planning process

No one should enter your building unscreened. There are many ways to screen, using volunteers, staff or a combination of the two. The installation of closed-circuit TV cameras, intercoms and door-release systems can assist in this process. Your security plan should develop and implement policies to ensure that screening is ongoing.

Minimize the number of open entrances to your facility (consistent with fire codes). For safety reasons, all necessary exits should be operational – even if they are alarmed. While people might complain about having to walk to their car a culture that emphasizes security consciousness leads people to tolerate a minimal inconvenience.

No one plan works for everyone, but depending on your institution, you may wish to:

Have the number for calling the police readily available and have a cell phone to use to call them from outside your facility in an emergency. But note: *do not use a cell phone during a bomb-related emergency.*

Have a disposable camera available in order to take pictures that may assist police if a suspicious individual or car is seen.

Regularly inspect your building so you can quickly ascertain if something is amiss and help law enforcement if there is a problem.

Use the security devices you already have. Ensure that security devices are functioning, that outdoor lighting is working, that windows and fence lines are kept clear of bushes, and that access to your building is appropriately limited consistent with fire codes.

Finally, **have a security expert help you to fully examine these issues, and create a plan to implement.**

QUICK TIP

Chances are that you're not a security expert.

Have your local police or other appropriate professionals do a crime prevention survey.

MANAGERIAL AND ADMINISTRATIVE CONSIDERATIONS

The goal of the managerial and administration section is to help you to put in place the basic organizational structure to help to mitigate emergencies. Many such issues, such as managing risk, insurance or personnel policies, are not simply operational and should be developed in consultation with your Board.

MANAGING RISK AND LIABILITY

The operation of any community, nonprofit or religious organization exposes it to a wide variety of liability risks. Exposure to liability risks exists at all times—it's part of doing business. Liability concerns should not normally prevent an organization from running any particular program.

If you are faced with a lawsuit, some of the first questions that you will be asked (by your insurer and both your attorney and theirs) will include, “What did you do to avoid this thing from happening?” Were the handrails adequate? Did you make the appropriate background checks of employees? Did you do proper training?

An organization needs to determine how to assess and plan to meet liability risks just as it needs to assess and plan for its programs and any emergency (see [Risk Management Strategies](#), P. 17). Liability risks fall into fairly predictable categories depending upon the type of institution and programs being run.¹⁸

Property

Unless an organization has no site (which is pretty hard to do) it has property liability risks. Whether the organization is a property owner or tenant, the risks include: accidents to organizational personnel, clients and anyone on the premises; any cars used by personnel for organizational work; organizational off-site events; on-site events by tenants or temporary site users, fire, theft and/or environmental problems.

Even an organization renting, or borrowing, space can incur property liability. One aspect of this problem is how the host organization shares the risk with the guest. A host organization is at risk of being named in a lawsuit if someone is injured at an event sponsored by a guest.

Some examples of common ways of addressing property risks are through:

1. *Avoidance*—barring admission to dangerous areas of a building;
2. *Minimization*—implementation of safety measures and procedures (e.g., security, maintenance, safety);

QUICK TIP

Risks are inherent in every enterprise. With risk comes the potential for liability. Proper risk management allows you to accomplish your mission while minimizing your exposure.

¹⁸ If a particular program is part of the core mission of your agency, risk avoidance is not a viable alternative. If you must run a pre-school program, the attendant risks are inherent. Therefore, you concentrate on the other three risk management strategies.

3. *Retention*—tolerate the risk;
4. *Sharing*—rent space from another organization, purchase insurance.

Personnel

Every organization has a board of directors (or trustees), many have paid staff and others have only volunteers or a mix of staff and volunteers to provide the organization's services. All organizations run liability risks such as sexual harassment or abuse, child abuse, discrimination in hiring and/or dismissal, theft, conflicts of interest, unauthorized use of organization's name, facilities, logo, etc., liability for negligent hiring (or use) of staff and volunteers, negligent training of staff and volunteers, professional services, malpractice claims and negligent referrals, or inadequate steps to protect staff, clientele or others.

In the risk management sphere volunteers are considered staff, i.e., if they do something wrong or injure someone while acting as your agent, you are liable. If they slip while delivering a holiday package to a homebound senior, are they covered by your insurance policy? If they are in a traffic accident and their driver's license is suspended (remember: plausible worst-case scenarios) could you be sued? If they steal something, what is your responsibility?

Some examples of common ways of addressing personnel risks are through:

1. *Avoidance*—don't hire anyone or use volunteers;
2. *Minimization*—implementation of sound policies and procedures, e.g., screening, background checks, record-keeping, guidelines and training;
3. *Retention*—tolerate the risk;
4. *Sharing*—subcontract programs (e.g., hiring a security contractor rather than your own guards) or insurance.

GENERAL TYPES OF RISKS

- *property*
- *personnel*
- *clients*

Clients

Each type of client brings its own set of risks such as children, teenagers, seniors.

Some examples of common ways of addressing client risks are through:

1. *Avoidance*—don't have any clients;
2. *Minimization*—implementation of sound policies and procedures;

3. *Retention*—tolerate the risk;
4. *Sharing*—subcontract programs (e.g., hiring a bus company to supply vehicles and drivers) or insurance.

Looking at a scenario

The [East Cupcake Jewish Center](#) (P. 19) is a basic community organization with a variety of programs and therefore a variety of liability issues. Besides the pre-school, health club, senior citizen and other similar programs operated on-site it also has a senior “friendly visitor” program and a street fair once a year.

Discussion

In the East Cupcake Jewish Center expanded scenario the general liability risks which would be present whether there was a terrorist emergency or not are:

1. *Fire or any accident*: property damage liability to the building, injury to personnel, clients and occasional users/guests, as well as loss or damage to their property.
2. *Me & Mommy program and the pre-school*: Is this an internal program or are they a tenant? If it is internal, the East Cupcake Jewish Center is liable for code compliance (both in terms of property and personnel), recruiting, screening and training its staff in age-appropriate learning, safety, sexual harassment, child abuse, etc.

If either program is a tenant:

- a. Are the tenants or groups/other organizations which are occasional users of space integrated into the safety plans of the facility?
- b. Does the lease have a waiver of liability for its programs and personnel?
- c. Is East Cupcake Jewish Center specifically covered under their insurance?
- d. What about business interruption?
3. *Swimming pool/gym*: Who is responsible for the hiring, certification and training of staff, including the lifeguards/personal trainers and any teachers or coaches? Is there adequate life-saving/medical equipment in the event of an emergency? Are there differing li-

abilities depending on the ages using the pool or gym, and whether under programmatic supervision or not (e.g., free swim)?

4. *Senior on-site programs*: Similar issues as above whether staff or volunteers.
5. *Senior off-site visiting program*: In addition to the on-site considerations there are separate issues relating to off-premises work, e.g., adequate supervision, vehicle liability.
6. *Business interruption*: What if the East Cupcake Jewish Center can not re-open its building for an extended period? Who pays the staff salaries or unemployment? Can its tenants sue because they are out of business? What if the parents of the pre-schoolers find another program when you're out of business?
7. *Street fair*: Special events bring other liability issues. Does your insurer know that you are engaged in such an activity? Does your accident liability coverage cover off-site claims for personal injury and property damage?

INSURANCE CONSIDERATIONS

One post-September 11th effect on almost all businesses was escalating insurance rates. With rising costs, institutions also faced lower limits per accident and lower aggregate limits (i.e., successive incidents during the term of the policy might not be covered), higher deductibles and more restrictive terms. Recent changes in federal terrorism insurance will provide some relief, but these unfortunate trends in the insurance business are likely to stay with us. While this manual does not presume to offer a primer on insurance, it does advise that effective insurance coverage is a prerequisite for business recovery.

Most clients want their insurance problems to go away. They want a “Dr. Welby” insurance broker who they can trust, and they want every claim covered. Good brokers are hard to find. Your insurance broker should be one who thoroughly understands your programs and activities so that you are appropriately covered. They should also, of course, understand non-profit organizations.

You should do your part. Keep no secrets! Send your broker your annual report, brochures and newsletters so that s/he can check if your policy is appropriate.

HELPFUL TIP

Make sure that your insurance broker understands everything that your organization does. Keep no secrets!

Exclusions

While the very purpose of insurance is to transfer risk away from your organization to the insurance company, insurance companies often limit their exposure to certain risks and list “exclusions” in their policies.

Sometimes exclusions are broad, while others are very specific, e.g., terrorism or floods. Since the excluded items might be the hazard that you are most concerned about, make sure that you review your policy to ensure that it covers you for the appropriate risks. Consult competent legal counsel.

Insurance reviews

Underwriters are now demanding more information about risk exposures. They want to know more about your activities so that they can properly assess their risk.

Property

Before each organization's annual insurance renewal there should be a thorough review of property. When major new purchases are made, major new gifts received, new equipment bought or leased or buildings renovated, discuss the change with your insurance broker to be sure that the change is covered. For example, a careless worker touched off a catastrophic fire at a landmarked house of worship. Millions of dollars of renovations were not covered under the existing policies.

Insurance policies should cover replacement costs, including inflation and any new construction.

Operations and Program Activity

In general, insurers cover the activities that they know about. If you engage in a type of activity that differs from your regular program, discuss it with your insurance broker to check if you are covered.

If a community center sponsors a subsidized housing project or a school sponsors a rally, their existing policy might not cover the risks arising out of the new endeavors. Discuss new activities with your broker to assure coverage. Special events carry unusual risks. When planning such an event, consult with your broker to plan for risks ranging from liability to cancellation.

Your insurance must also cover actions by all of the various actors in your entity: board, staff, volunteers and clientele. In our litigious society, anyone can sue anybody for anything. While a plaintiff's complaint might not have merit, it can cost thousands of dollars to defend a lawsuit. Your insurer's willingness to pay, in advance, for legal representation can be critical to the viability of your agency.

Additional named insured

When working with an independent contractor, it is important that you receive a certificate of insurance from their carrier, naming your organization as an "additional named insured." This will give you an insurable interest for claims arising out of the activities of your independent contractor (if the policy limits are not exhausted by the independent contractor).

The additional named insured certificate covers only the individual(s) or corporation(s) specifically listed. Consider whether the certificate should also cover the site owner, property manager, tenants or program manager.

When you receive your certificate of insurance, make sure that it is an *original* rather than a fax or copy. Some contractors have pulled an old certificate from their files and inserted their current client's name. If you are the victim of such a scheme you will not be protected in the event of a claim.

On occasion, you will be asked for a certificate of insurance by an entity with which you have a joint activity, e.g., if you sponsor a street fair or rally, the municipal authorities often ask for just such certification. Your insurance broker can easily arrange for your certificate. There is usually no extra charge for this service.

When something happens

Things can, and will, happen. The first defense is to train your staff to record unusual incidents. Establish a standard procedure. For example, if someone gets injured, even slightly, it's a good idea to write up a formal accident report describing what occurred and the steps taken in response to the accident (e.g., Was first aid administered? Were parents called?). As a matter of course these reports should be reviewed by a specific individual to ensure that the procedure is being followed and to see if similar incidents can be avoided in the future.

If a claim becomes necessary (or even likely), it is essential that you give your insurance company—*both your agent/broker and the carrier itself*—notice. If your broker volunteers to notify the carrier for you, be sure that s/he sends you a written copy of the notice for your records.

Different types of liability coverage

In general, nonprofits should consider three types of liability coverage:

General liability

Broadly speaking, this type of insurance provides coverage for “negligent” acts—something a reasonable person would not do under the circumstances or failing to do something a reasonable person would do. This insurance covers claims that your organization, its employees or volunteers (including board members) negligently caused someone “bodily injury, personal injury or property damage.”

These insurance policies also cover claims that the insured failed to take reasonable steps to avoid or minimize injury or damage.

Professional liability

Professionals, such as social workers, clergy, attorneys and medical personnel, must have separate insurance covering claims arising from their professional actions. This is commonly known as malpractice.

Directors and officers liability (D&O)

These policies vary widely, but generally provide coverage for the normal and usual business activities by an organization's board of directors or managers that lead to a claim of damages to an individual or property. For example, your D&O policy is applicable if an employee is terminated and claims that the organization's decision was based on discrimination.

Note that while D&O will pay for legal representation to defend the action, it does not generally cover illegal acts. For more information on D&O and other insurance considerations visit the web site on nonprofit insurance at: <http://www.niac.org>.

Fidelity Bonds

Bonding usually covers employee/volunteer dishonesty, e.g., theft, fraud, forgery or alteration, computer fraud and/or embezzlement. A blanket coverage policy can be purchased that applies to all employees, directors, etc., or specific policies can cover employees or jobs (e.g., cashier, controller).

Business Interruption Coverage

While most nonprofit organizations consider casualty insurance when considering disasters, many don't feel that they need business interruption insurance—after all, they're not in business.

However, every entity bears consequences if it cannot provide services for a period of time. Parents rely on daycare services in order to be able to work. If a daycare cannot open because its facilities are damaged, these parents will find alternative providers.

Business interruption insurance can help to pay for an alternative site or alternative facilities while the primary facilities are being repaired and help to make up the income from parents who left the daycare. Some policies also cover the costs of additional personnel.

This coverage can be costly, but consider what would happen to your agency if

you could not use your facilities or your staff could not report for work for a week or a month. If the impact is intolerable, then the cost of business interruption insurance could be worth it.

Inventory

After a disaster you will work closely with your broker and a claims adjuster to expedite your claim. One important step is to have an up-to-date inventory of the contents of all of your facilities.

One of the easiest ways to compile such an inventory is by making a videotape. Using a video camera, walk slowly around every room in your facility, carefully taping items such as furniture, books, pictures and fixtures. By panning the whole room you will effectively inventory its contents.

These tapes should be maintained, with a duplicate tape stored off the premises. In case of a disaster the claims adjuster can base his/her settlement offer based on the inventory. Your claim can be paid weeks or months faster than one based on making lists and sorting through debris.

CREATING AND IMPLEMENTING POLICIES AND PROCEDURES

Crises come in all shapes and sizes. With only a cursory scan of the [Hazard Analysis Worksheets](#) (P. 117) in the Appendix, you will note that natural and security hazards are but a tiny proportion of the risks faced by nonprofits. One of the most effective risk reduction strategies is to create sound policies and procedures and to implement them.

Whether the risk is from a natural (e.g., hurricane) or man-made (e.g., blackout or security) disaster in your area or a slip-and-fall lawsuit, an allegation of sexual or child abuse by a staffer or volunteer, a job discrimination allegation, a school bus accident, or professional malpractice claim (to name a few), your vulnerability can be reduced with practical, continually-updated and tested policies and procedures.

QUICK TIP

Sound policies and well-thought-out procedures can help to avoid or minimize problems.

Do you take reasonable precautions?

How good is your organization at:

- making your policies and procedures on recognized hazards and risks explicit;
- training your staff, documenting reports on a variety of problems; or
- investigating and acting on the results of the investigations?

Your actions will have a major impact on the organization's legal exposure. There is an emerging new concept in negligence law called negligent failure to plan.²⁰ The Canadian Parliament recently enacted a law establishing criminal liability for organizations and individuals failing to prevent workplace accidents. The general test found in the law is, "lack of care."

Currently there is a general (civil, not criminal) duty under the U.S. federal occupational health and safety laws (OSHA) for an employer to "furnish each of his employees ... a place of employment that is free from recognized hazards ..." If your services or facilities don't have adequate plans and policies for safety from recognized hazards, your organization may be hit with a liability claim. It's just not a wise way to run any organization. If the responsible individuals in an organization have spent time developing policies and procedures, they are likelier to "get it right" when the hazard/crisis occurs. "Getting it right" should reduce an organization's legal exposure.

²⁰ This new theory at this time has not been raised in any lawsuit yet, however, the legal argument behind it is just a small stretch from what is now existing law.

Preventative Procedures

There are many good resources for policies and procedures. Your insurer may have materials. Other good resources for nonprofits include:

<http://www.nonprofitrisk.org/advice/advice.htm#online> and <http://www.insurancefornonprofits.org/>.

OSHA publishes guidelines and tips on many situations at <http://www.osha.gov/SLTC/index.html>. These web sites provide a wealth of information, recommendations and forms for risk issues facing organizations. Remember, only your organization can really put together and implement the policies and procedures tailored to your organization's specific programs and populations.

The policies and procedures that need to be implemented by organizations track the same issues covered in the liability and insurance section of this manual. You should have policies in all of your areas of operation such as:

Employment. Are you checking potential employee and volunteer references, and, when appropriate, doing criminal background checks? Remember: there are federal, state and local regulations that require such checks on various positions ranging from security guards to child care workers and/or teachers.

Vehicular operation. Do you check and document that your vehicle drivers (staff or volunteers) have appropriate and up-to-date licenses and insurance? Do you have a policy that drivers are automatically suspended from work for non-compliance? Are your vehicles in good and safe working order and are they inspected as necessary? Subcontracting this function may share some of this liability with the subcontractor, but your contract with them must be specific.

Professional. Do your professionals have a current license to practice and appropriate malpractice insurance and do they act according to their profession's ethical standards?

Fiscal. Are there fiscal checks and balances no matter how small the organization? For example, does the same person sign for check authorization and the check? Are the books audited? Do representatives of the board regularly review budgets and actual expenditures?

Employee and Client Manuals

Employees

Employment attorneys disagree on the value of an employee handbook or personnel policies manual. Some argue that a manual provides an appropriate statement of various employment policies and helps ensure wide understanding of the policies. Others argue that it may convert the at-will employment relationship to a contractual one, therein imposing additional duties on the nonprofit. Employment law experts do agree on one thing—a nonprofit employer that ignores its handbook is at greater risk than an organization that operates without a handbook.²⁰

A nonprofit should never develop and adopt any policy or handbook, employment or otherwise, that it is unwilling or unable to follow. Many nonprofits get into trouble when they fail to keep their handbooks up-to-date, do not insist that all staff be familiar with the provisions in the handbook, or randomly exempt certain employees from the directives in the handbook.

Whether or not a nonprofit uses an employment handbook, the following risk management practices are important:

- Ensure that the organization's personnel policies are clear, consistent and within the law.
- Make certain that the nonprofit conveys its employment policies to its employees in a clear and concise manner.
- Ensure that the organization fulfills its end of the employment relationship.
- Seek legal counsel before taking any adverse employment action.

Clients

In some situations clients have specific rights. The most well-known case is the “patients’ bill of rights” provided for in many states. Professional codes of ethics in some fields grant others rights. Make sure that you are complying with all of the applicable laws and codes.

HELPFUL TIP

When there is a serious charge it's best to consult with your attorney and to inform the appropriate member of your board.

²⁰ Adapted from <http://www.riskcenter.org/knowledge/normac/written.html>.

Investigations

Clients, staff members and outsiders can make all sorts of allegations about your organization, your staff or your volunteers. Such charges may, or may not, be founded. When there is serious charge, it's best to immediately consult with your attorney and the appropriate member of your board.

No one expects you to be a detective or expert investigator. General rules of thumb include:

- Take the complaint seriously.
- Begin the investigation in a timely manner.
- Question all the relevant witnesses in an atmosphere where they feel free to answer truthfully.

During some categories of investigations (e.g., harassment or abuse) it is often wise to separate the alleged victim from the alleged harasser during the investigation to minimize any potential for continuing harm.

Make certain that you complete your investigation and take remedial action in a timely manner and make sure you inform the complainant about the conclusions of the investigation. This is particularly important when an investigation does not yield evidence of illegal conduct, but does yield evidence of unprofessional conduct. The “victim” needs to know what disciplinary steps were taken, otherwise the victim will believe that his or her complaints were not taken seriously and be more likely to call an attorney.

Keep detailed records of complaints, including notes on the steps taken in response to any complaint. These records will become evidence in mounting an affirmative defense.

It's a good idea to involve an outside facilitator, such as legal counsel, in any internal investigation, since employees may be more comfortable speaking candidly to an objective outsider.

Keeping up-to-date

Finally, no matter how good your policies and procedures are, they are worthless if they just stay “on the shelf.” People need training and supervision, and policies and procedures need regular review. Having good, up-to-date policies and procedures is one of the most effective strategies for reducing risk.

MUTUAL AID AND ASSISTANCE

Suddenly there was a big BOOM and the floor shook at the East Cupcake Pre-school. The teachers were well-trained and sprang into action. They quickly got the kids' coats and started moving them outside. But it was 19° F outside.

No, it wasn't terrorism. The boiler had exploded. The kids were getting on their overcoats, but soon they were shivering. Where should the teachers take the kids to stay warm? Where would they get phones to contact everyone? Would there be school tomorrow?

No one expects you to lease a nice, safe, unused, but fully stocked, building a few blocks away from your site waiting for such eventualities. But how would you handle similar situations?

Mutual aid agreements are a common method of handling emergency gaps. Such agreements are known as Memoranda of Understanding.

It is important to put such agreements in writing.

Drafting your memorandum of understanding

An effective Memorandum of Understanding (or MOU)²² prevents misunderstandings and disputes by clarifying the expectations of the partners. The process of developing an MOU is an instructive and potentially invaluable experience in partnering. You will learn how responsive your partner will be—are your calls returned promptly? Does your partner give the partnership the attention and seriousness it requires? You may also learn how your partner reacts when you disagree on an issue.

The refusal to put anything in writing is a red flag and may be the sole reason not to proceed with the arrangement. There are a number of elements that should be contained in a typical Memorandum of Understanding. Since each project and its partners are unique, the following suggestions are provided as an example. As with any contract, it's critical to obtain legal counsel before obligating your nonprofit.

²² Adapted from <http://www.niac.org/CollaborationRisks>.

Overall Intent

Many MOUs begin with a brief description of the overall intent of the parties, such as

“Whereas the mission of We CARE is to provide hot meals to homebound elderly living in North East Cupcake, and the mission of We DELIVER is to deliver food to the homebound elderly living in the South East Cupcake, the organizations hereby agree to work together to ensure that all of our clients are served in the event of an emergency or disaster.”

The overall intent clause must accurately reflect what the parties are intending to do. Ulterior motives have no place in effective partnerships.

The Parties

The next clause in an MOU describes the parties to the agreement. It should be specific to indicate the types of organizations (“a nonprofit corporation headquartered in East Cupcake in the State of Oklahoma”).

The Period

Specify a time period for the partnership. Definite time periods help to ensure that the terms of the partnership can be periodically reviewed and renewed.

Assignments/Responsibilities

This important section of the MOU describes the duties and responsibilities of each partner. It’s generally more effective to describe each organization’s responsibilities separately, beginning with the items that are an organization’s sole responsibility. List each group’s sole responsibilities, followed by a description of shared responsibilities, if any. In many cases, this section of the agreement will be the most detailed and lengthy. Clarifying responsibilities is the number-one purpose of a written agreement.

Disclaimers

Many MOUs will contain one or more disclaimers, including one indicating that employees of Organization A are not to be considered employees, borrowed or otherwise, of Organization B and vice versa. It may also be worthwhile to disclaim what the partnership is not intended to do, guarantee or create.

Financial Arrangements

A typical partnership will have financial implications. These should be spelled out in detail including which entity will pay for each item and when payment is due.

Risk Sharing

Another critical element of an MOU is a description of who will bear the risk of a mishap. What if something goes wrong? What if the partnership's activities result in injury, death or a financial loss? An important tenet of risk management is that an organization should never assume responsibility for something over which it doesn't have control. For example, a nonprofit renting a building to hold a dinner meeting shouldn't assume responsibility for unrelated damage caused by a leaky roof. A formal MOU may include an indemnification provision, promising that Organization A will pay for losses suffered by or caused by Organization B. Ideally, indemnification provisions should be mutual in that each party will be responsible for its own negligent acts or omissions. Remember that an organization's agreement to indemnify your nonprofit without their having the financial resources (including insurance) to meet this responsibility is a hollow promise. So make certain your partner is not only willing but also able to pay for losses it causes. An "insurance requirements" section is one way to do this.

Insurance Requirements

This section indicates the insurance requirements that each organization places on the other. In some cases, one organization will require that its partner have certain insurance in place. If the parties have agreed to a mutual indemnification provision (see Risk Sharing, above), the insurance requirements should be bilateral. For example:

The parties to this agreement hereby agree that each will maintain insurance throughout the duration of the collaboration, that meets or exceeds the following:

- Commercial General Liability policy in the amount of at least \$1 million combined single limit for each occurrence, written on an occurrence form;
- Auto Liability policy including coverage for owned (if any), non-owned and hired vehicles in an amount not less than \$1 million;
- Workers' Compensation Coverage covering all employees working on the collaboration and having statutory limits for each jurisdiction where the work under the collaboration is performed, and an Employers' Liability policy with at least the following limits: \$250,000 per accident and \$500,000 per disease.

In addition, each party to this agreement will name the other party as an Additional Insured on all applicable policies and provide valid Certificates of Insurance indicating coverage.

Signatures

A representative from each partner with authority to bind their organizations contractually should sign the MOU. Each partner should retain a copy of the signed agreement.

Site considerations

What if you cannot use your primary site for an hour, a day, a week or longer? What functions must be taken care of immediately? What can wait?

The pre-school scenario above might be solved in a fairly simple manner. Is there a house of worship, another school or appropriate building nearby? Could the teachers bring the kids there until their parents could be contacted and come to pick them up?

The answer is that such mutual aid agreements are quite common. For example, two schools in the same neighborhood agree that if there is an emergency in the first, the staff will relocate to the second, and vice versa. This is a no/low cost solution. The agreement should detail which room(s) would be available (e.g., gymnasium or auditorium), for how long, what phones or other equipment would be available, etc.

Data considerations

It is often expensive to have a backup computer system off-site. Many emergency planners turn to the option of a mutual aid agreement with another organization with a similar computer configuration.

A reciprocal agreement should be entered into carefully because each site must be able to support the other, in addition to its own workload, in the event of a disaster. All parties to a data-related reciprocal agreement should pre-define their priority data and the MOU should specify the recovery sequence for all organizations. The recovery plan should be prioritized from a joint perspective, favorable to both parties. Testing should be conducted at the partnering sites to evaluate the extra processing thresholds, compatible system and backup configurations, sufficient telecommunications connections, compatible security measures, and the sensitivity of data that might be accessible by other privileged users, in addition to functionality of the recovery strategy.

MOU's should be developed specific to the organization's needs and the partner organization's capabilities. The legal department of each party must review and approve the agreement. In general, the agreement should address elements, including:

- Contract/agreement duration
- Cost/fee structure for disaster declaration, usage and occupancy
- Disaster declaration (i.e., circumstances constituting a disaster, notification procedures)
- Site/facility priority access and/or use
- Site availability
- Other clients subscribing to same resources and site, and the total number of site subscribers, as applicable
- Contract/agreement change or modification process
- Workspace requirements (e.g., chairs, desks, telephone, PCs)
- Supplies provided/not provided (e.g., office supplies)
- Additional costs not covered elsewhere

Larger organizations might wish to turn to a provider in the field, in which case a detailed contract is appropriate. Less formal arrangements should be memorialized by letter.

APPENDICES

HAZARD ANALYSIS WORKSHEETS

Hazard analysis involves identifying all of the hazards that potentially threaten an organization and analyzing them individually to determine the degree of threat that is posed by each. Hazard analysis determines:

- What hazards can occur.
- How often they are likely to occur.
- How severe the situation is likely to get.
- How these hazards are likely to affect your organization.
- How vulnerable your organization is to the hazard.

This information is used in the development of both mitigation and emergency plans. It indicates which hazards merit special attention, what actions might be taken to reduce the impact of those hazards and what resources are likely to be needed.

The hazard analysis worksheets that follows²² may seem redundant. Believe it or not, that's good news. Your mitigation program will generally be appropriate for a wide variety of hazards. If your security program is in place, if you have an evacuation plan (and practice it regularly), if you have solid policies and procedures and if your insurance is appropriate (to name a few contingencies), you will have gone a long way in preparing your organization for a multitude of emergencies.

Using the worksheets

As noted in our introduction to hazard analysis, there are many types of risks and hazards. This manual divided them into eight broad categories: terrorism, natural hazards, financial operations, legal, misconduct by employees or volunteers, activities and services, property loss and technology.

Each section has examples of things that can happen, possible adverse effects and risk management strategies. As you identify the hazards that apply to you (and not all will apply), look for suggestions to be incorporated into your emergency plan. Consider this section a checklist to begin your planning process and a springboard to launch your own scenario plotting.

²² The hazard analysis framework is adapted from: *Risk Identification and Analysis: A Guide for Small Public Entities*, by Claire Lee Reiss, J.D., ARM, 2001, published by the Public Entity Risk Institute, www.riskinstitute.org.

1. Terrorism

Some Risk Sources:

- ☐ Mega-event (e.g., World Trade Center/Pentagon)
- ☐ Chemical, biological or radiological Attack
- ☐ Bomb
- ☐ Shooting
- ☐ Kidnapping

Possible Losses or Adverse Results:

- ☐ Damage to buildings and infrastructure
- ☐ Disruption of transportation
- ☐ Disruption of utilities (gas, electricity, water, sewers)
- ☐ Disruption of communications
- ☐ Disruption of food supply and deliveries
- ☐ Disruption of program revenues
- ☐ Disruption of mandated services and other activities
- ☐ Environmental contamination
- ☐ Opportunistic criminal activity
- ☐ Injury of clientele and employees
- ☐ Fires and explosions
- ☐ Release of hazardous materials into environment
- ☐ Loss of/inability to mobilize workforce
- ☐ Loss of/inability to access equipment
- ☐ Loss of computer-based information
- ☐ Clientele's perception of your agency as a terrorist target

Possible Strategies:

- ☐ Maintain situational awareness of world events and ongoing threats.
- ☐ Ensure all levels of personnel are notified via briefings, E-mail, voice mail and signage of any changes in threat conditions and protective measures.
- ☐ Encourage personnel to be alert and immediately report any situation that may constitute a threat or suspicious activity.
- ☐ Take any threatening or malicious telephone call, facsimile, or bomb threat seriously. Train appropriate personnel to use bomb threat information forms if such a call is received.

- ☐ Adopt a written emergency action plan, have it available on short notice and practice it regularly.
- ☐ Assign disaster responsibilities to specific employees in advance.
- ☐ Enter into mutual aid agreements with other entities for potentially disrupted or overwhelmed services.
- ☐ Pre-arrange financing for disaster response activities.
- ☐ Pre-arrange with vendors for emergency equipment, supplies and additional workers.
- ☐ Adopt and publicize evacuation plans.
- ☐ Include natural hazard vulnerability and mitigation techniques in initial development and post-disaster redevelopment decisions.
- ☐ Prepare contingency plans for shelter of displaced key staff.
- ☐ Review security arrangements and prepare a presentation²³ on security.

²³ Obviously, you never disclose all of your security arrangements. However, you should be prepared to convince clients that security is an important consideration and appropriate measures have been taken.

2. Natural Hazards

Some Risk Sources:

- ☐ Winter Storm
- ☐ Earthquake
- ☐ Landslide, Mud slide
- ☐ Sinkholes
- ☐ Erosion
- ☐ Windstorms
- ☐ Hurricanes
- ☐ Tornadoes
- ☐ Thunderstorms and Lightning
- ☐ Wildfire
- ☐ Flood
- ☐ Tsunami
- ☐ Volcanic eruptions
- ☐ Drought
- ☐ Heat
- ☐ Power outage *
- ☐ Aircraft Disaster *

Possible Losses or Adverse Results:

- ☐ Damage to buildings and infrastructure
- ☐ Disruption of transportation
- ☐ Disruption of utilities (gas, electricity, water, sewers)
- ☐ Disruption of communications
- ☐ Disruption of food supply and deliveries
- ☐ Disruption of program revenues
- ☐ Disruption of mandated services and other activities
- ☐ Environmental contamination
- ☐ Opportunistic criminal activity
- ☐ Injury of clientele and employees
- ☐ Fires and explosions
- ☐ Release of hazardous materials into environment
- ☐ Loss of/inability to mobilize workforce
- ☐ Loss of/inability to access equipment
- ☐ Loss of computer based information

* While power outages and aircraft disasters are technically not natural occurrences the risk analysis framework is similar to that of natural hazards.

Possible Strategies:

- ☐ Assess and determine vulnerability to natural hazard events.
- ☐ Adopt a written emergency action plan, have it available on short notice and practice it regularly.
- ☐ Assign disaster responsibilities to specific employees (e.g., in response teams) in advance.
- ☐ Enter into mutual aid agreements with other entities for potentially disrupted or overwhelmed services.
- ☐ Pre-arrange financing for disaster response activities.
- ☐ Pre-arrange with vendors for emergency equipment, supplies, and additional workers.
- ☐ Adopt and publicize evacuation plans.
- ☐ Include natural hazard vulnerability and mitigation techniques in initial development and post-disaster redevelopment decisions.
- ☐ Prepare contingency plans for shelter of displaced key staff.

3. Financial Operations

Some Risk Sources:

- ☐ Financial transactions
- ☐ Investment of funds
- ☐ Cash handling
- ☐ Dependence on governmental revenue sources
- ☐ Entity credit rating
- ☐ Community economic conditions
- ☐ Financial records
- ☐ Client records
- ☐ Contracts for purchase or supply of goods and services
- ☐ Contracts to perform or receive construction services
- ☐ Real estate leases (lessor or lessee)
- ☐ Real estate purchase or sale
- ☐ Contracts for joint use of owned or non-owned facilities
- ☐ Contracts to jointly operate program with another entity
- ☐ Equipment and motor vehicle leases
- ☐ Notes, mortgages and loans
- ☐ Mutual aid agreements
- ☐ Grant agreements
- ☐ Insurance contracts
- ☐ Employee credit/purchasing cards or phones for which entity is responsible

Possible Losses or Adverse Results:

- ☐ Reduced revenues (Examples: economic recession; loss of state, federal or grant funding for projects or activities; reduced income from investments)
- ☐ Inability to borrow funds
- ☐ Loss of funds through theft/embezzlement/negligence
- ☐ Loss of funds through bad investments
- ☐ Loss or alteration of financial records
- ☐ Unauthorized transfer of entity funds via computer
- ☐ Violation of client's right to privacy and confidentiality
- ☐ Failure to comply with mandatory procurement practices
- ☐ Civil rights violations
- ☐ Contract executed beyond authority

- ☐ Third party default on contract with public entity
- ☐ Contractor/vendor/franchisee provides defective goods or services
- ☐ Agency liability for contractor/vendor/franchisee actions
- ☐ Agency default on contracts and agreements
- ☐ Public entity liability for providing defective goods or services
- ☐ Cost overruns on construction projects
- ☐ Damage to property leased by public entity
- ☐ Entity's insurance contracts fail to cover its insured losses
- ☐ Contracts (including insurance) lost or destroyed and cannot be enforced
- ☐ Employee credit/purchasing card is lost or stolen by a third party and used for non-entity transactions
- ☐ Employee misuse of credit/purchasing card
- ☐ Entity liability for employee default on obligations incurred under "government rate" purchasing plan for personal services

Possible Strategies:

- ☐ Implement and enforce system of internal financial controls.
- ☐ Implement and enforce system of controls for investment of entity funds.
- ☐ Provide adequate security where entity handles cash.
- ☐ Provide adequate security for hard copy and computer based financial records.
- ☐ Provide adequate security for any computer site used by the entity to conduct its financial transactions and transfer funds.
- ☐ Provide adequate security for financial records.
- ☐ Back up financial records.
- ☐ Stay aware of governmental initiatives that may impact revenue sources, and develop contingency plans to replace those sources.
- ☐ Ensure adequate performance on projects funded by governmental or other sources.
- ☐ Conduct risk management/legal review of all contractual relationships.
- ☐ Conduct legal review of purchasing procedures.
- ☐ Include indemnity/hold harmless clauses and insurance requirements in entity contracts.
- ☐ Require ongoing, documented compliance with contractual insurance requirements.
- ☐ Include surety and performance bond requirements in contracts where appropriate.

- ☐ Perform due diligence investigation of potential contract partners to determine solvency and ability to fulfill contractual obligations.
- ☐ Create contract language assigning responsibility for cost overruns.
- ☐ Implement loss prevention/quality assurance program to ensure high quality of agency-provided goods and services.
- ☐ Make advance financing arrangements for agency liability arising from contractual relationships.
- ☐ Ensure that agency satisfies all contractual or lease requirements for insurance or performance/surety bonds.
- ☐ Conduct thorough review and analysis of entity's insurance coverage and other risk-financing mechanisms at least annually.
- ☐ Keep all current and past insurance policies safe and accessible.
- ☐ Conduct regular actuarial review of self-insured program.
- ☐ Establish and enforce security, appropriate use and reporting procedures and requirements for all purchasing/credit cards issued to employees.

4. Legal

Some Risk Sources:

- ☐ Employment practices (examples: hiring, discipline, incentive programs, termination, turnover, retirement, right to privacy and confidentiality, benefits).
- ☐ Employees or volunteers under age 18 (in some states 16).
- ☐ Workplace policies, procedures, and rules.
- ☐ Employment of workers who are not legal residents.
- ☐ Employees with pre-existing health conditions.
- ☐ Employment-related laws and regulations.

Possible Losses or Adverse Results:

- ☐ Litigation: attorney's fees and verdicts or fines.
- ☐ Fines or penalties for noncompliance with federal or state occupational safety and health requirement.

Examples: lockout, electrical work, lateral support for excavation, tree trimming, walking surfaces and ladders, hazardous materials, record keeping and posting, machinery guarding, respiratory protection, job safety analysis, confined space entry, manual material handling, ingress and egress or first aid.

- ☐ Liability for judgment and defense costs for employment-practices litigation.

Examples: discrimination in any facet of employment based on race, age, pregnancy, religion, national origin, marital status, number of children, disability and other factors under state and federal law; sexual harassment; failure to accommodate or other violations of Americans with Disabilities Act; Family Medical Leave Act; breach of employee confidentiality or privacy.

- ☐ Litigation alleging defamation of employee.

Examples: during disciplinary activities, post-employment references.

- ☐ Liability to injured third parties for negligent hiring, training, supervision or retention of employees.

Examples: inadequately qualified, trained or supervised employee injures third party during hazardous operations; employee intoxicated on the job injures third party.

- ☐ Losses from employee's intentional acts against the employer or other employees.

Examples: theft, arson, pilferage, violent acts, harassment.

- ☐ Penalties or liability for failure to properly administer employee benefits.

Examples: failure to enroll or incorrect enrollment for benefits, failure to maintain benefits, failure to provide notice about post-termination benefits continuation, negligent selection of vendors for employee benefit plans, breach of fiduciary duty related to retirement plans.

- ☐ Penalties for employing non-citizens in violation of federal immigration laws.
- ☐ Liability to third parties for actions of independent contractor.

Examples: contractor operations damage property of or cause injury to third party.

- ☐ Liability to third parties for actions of volunteer.

Examples: volunteer damages property of or causes injury to third party, volunteer abuse of children, elderly or disabled in volunteer's care.

Possible Strategies:

- ☐ Train staff and volunteers about their legal and ethical obligations.
- ☐ Prepare written policies and procedures governing all aspects of the employment relationship from hiring through post-employment. Have these policies and procedures reviewed and approved by legal counsel prior to implementation and adequately train all supervisors and managers. Institute a review process to ensure that policies and procedures are implemented in every phase of the personnel process.

Examples: job advertising, job application, job interview, hiring, probation, family medical leave, reasonable accommodation of employees with disabilities, supervision, discipline, references for prior employees, off-duty recreational and fitness activities, substance-abuse testing for employees in sensitive or hazardous positions, benefits, termination, workers' compensation procedures and prompt reporting of work related injuries, written records of employment matters, confidentiality of employee information, due process in employee discipline/termination proceedings.

- ☐ Prepare and periodically update written job descriptions for all positions, including identification of essential functions of the job, and review for compliance with the Americans with Disabilities Act.

Example: identify the essential functions of the job concentrating on what needs to be accomplished rather than precisely how it must be accomplished.

- ☐ Implement written policies addressing areas of employee activity that pose potential or particular problems. Have these policies reviewed by legal counsel or others before implementation and then, train employees in such policies.

Examples: sexual harassment, internet and E-mail use, requirements for driving entity-owned vehicles, use of cellular phones while driving, use of passenger-restraint systems while driving, use of entity-owned vehicles on non-entity business, transporting non-employees in entity-owned vehicles, off duty employment, intoxication/drug use on the job, commercial drivers' license driver requirements, violent or intimidating employee conduct in the workplace.

5. Misconduct by Employees or Volunteers

Some Risk Sources:

- ☐ Criminal acts by staff
- ☐ Conflicts of interest
- ☐ Volunteer workforce
- ☐ Independent contractors
- ☐ Worker substance use
- ☐ Employee recreational activities
- ☐ Worker injury or illness
- ☐ Providing references for former employees
- ☐ Inadvertently creating contractual employment relationship with employees rather than maintaining “employment at will” status.

Possible Losses or Adverse Results:

- ☐ Costs of employee work-related injury or illness.
Examples: workers’ compensation benefits, medical expenses, liability for employee injury not covered by workers’ compensation, lost productivity during recovery, cost of replacing skilled employee, employer responsibility for pre-existing health conditions.
- ☐ Client dissatisfaction due to inadequate services .
Examples: inadequate hiring procedures, inadequate on-the-job training, inadequate pool of potential employees, excessive turnover or early retirement due to lack of competitive pay and benefits or unpleasant working environment.
- ☐ Non-employee work-related injury or illness .
Examples: independent contractor without workers’ compensation insurance, volunteers)
- ☐ Costs of worker injury during after-hours recreational/fitness activity .
Examples: employer-sponsored teams during non-working hours, on-site or off-site employee fitness classes.

Possible Strategies:

- ☐ Adopt a safety program to reduce injuries and property damage arising out of operations
Examples: enlist visible upper management support of the safety program, entity-wide safety committee, individual department safety committees, reporting and review of all accidents, injuries and near misses; analysis of entity loss experience to identify problem areas for intervention, establish safety rules and impose

discipline for failure to comply, recognize operations with good safety records, identify and comply with applicable OSHA standards, identify and comply with other applicable standards, such as National Fire Protection Association; conduct regular inspections of entity premises, equipment and tools for safety hazards, train all employees about safety issues applicable in general and to their specific operation, ensure employees have adequate training and experience before undertaking hazardous operations, periodically retrain employees to update information.

- ☐ Require independent contractors to have appropriate safety program and commit to follow applicable OSHA standards.
- ☐ Require independent contractors to comply with federal and state laws and regulations relating to employment.
- ☐ Require independent contractors to indemnify and hold harmless the entity for liability arising out of its operations under the contract.
- ☐ Prepare written volunteer job descriptions and orient volunteers to safety issues and required standards of conduct before they begin working.
- ☐ Reduce workforce turnover .
Examples: improve hiring practices, improve benefits and pay, improve work environment.
- ☐ Administer employee benefits program through well-qualified internal or external personnel.
- ☐ Require Americans with Disabilities Act-compliant health examination of employee after a contingent job offer has been made, but before the employee has begun work.
- ☐ Document all employee training.
- ☐ Obtain prior legal review of any employee handbook and offers of employment.

6. Activities and Services

Some Types of Activities and Services:

- ☐ Management and administrative functions
Examples: personnel, purchasing, legal, finance, risk management, fleet management, grounds and building maintenance, record-keeping.
- ☐ Communications with the public
Examples: advertising events, materials promoting the jurisdiction, web site content, warnings, notice of public meetings, statements to the media, E-mail, letters, newsletters and articles.
- ☐ Operation of equipment and machinery
Examples: motor vehicles, construction equipment, watercraft, mobile equipment.
- ☐ Recreational facilities and activities
Examples: amusement parks, athletic facilities, auditoriums, beaches, campgrounds, golf courses, ice skating rinks, marinas and docks, parks, playgrounds, recreation centers, shooting ranges, summer camps, skateboard/rollerblade facilities, sporting events, swimming pools and water parks, winter sport/skiing sites, zoos.
- ☐ Educational facilities
Examples: day care, pre-schools, K-12, supplementary schools, vocational and training schools, higher education, miscellaneous classes.
- ☐ Social services
Examples: day care for children and elderly, housing, homeless shelters, welfare, foster care, child protective services, senior services.
- ☐ Buildings and premises
Examples: existing buildings, new construction projects, parking facilities, vacant buildings, unimproved land.
- ☐ Professional services and activities
Examples: physicians, psychologists, social workers, accountants, lawyers, architects, engineers, information technology, nursing, dental, physical and occupational therapists, teachers.

Some Possible Adverse Results:

- ☐ Liability for bodily injury or property damage due to unsafe condition of agency-owned or occupied buildings.
Examples: unsafe walking surface conditions, inadequate lighting and security, overcrowding and lack of crowd control, lack of fire

and building code compliance, contamination with hazardous materials including lead paint, asbestos, PCB's; infestation with vermin, plumbing and electrical system malfunction.

- ☐ Liability for bodily injury or property damage due to unsafe condition of grounds

Examples: unsafe walking and driving conditions, surface damage, missing manhole covers and grates, unsafe road design, banking, visibility, railings, emergency shoulders, drainage, inadequate lighting, inadequate signage, inadequate hazard warnings, malfunctioning traffic signals, failure to clear after storm, falling trees and other objects, unsafe design or condition of playground or other outdoor recreational sites, drowning hazards, overcrowding and lack of crowd control, inadequate spectator protection, inadequate supervision such as lifeguards for pools and beaches, inadequate severe weather contingency plans for outside recreational areas such as beaches, pools, golf courses, camp grounds, injuries due to inadequate planning for emergencies or inadequate security.

- ☐ Liability for bodily injury or property damage at construction sites

Examples: adjacent property, underground utilities and resulting disruption of service, unsafe conditions of premises affecting building occupants, contractor and subcontractor employees, suppliers and public employees.

- ☐ Liability for discrimination/violation of civil rights

Examples: discrimination based upon age, disability, gender, national origin, personal views, pregnancy, race, religion, sexual orientation or other categories protected under state or federal law. Includes discrimination in access to facilities and programs and employment (Note: Religious organizations and private clubs may have more discretion in this area). Also may include free speech and privacy issues in various settings.

- ☐ Liability for bodily injury or property damage due to operation of watercraft, motor vehicles, school or activity transit systems and mobile equipment

Examples: liability for bodily injury and property damage arising out of the use of owned, non-owned and hired equipment, unlicensed operator, inadequate operator training, inadequate background check/reference check for operator, intoxication of operator

- ☐ Food service

Examples: food poisoning, foreign object in food, unanticipated closure of facility due to unsanitary conditions or infestation.

- ☐ Environmental contamination

Examples: underground and above-ground storage tanks, vehicle accidents, pipelines, waste disposal, incinerators, landfills, sew-

age overflow, water treatment plant malfunction, release of contaminants in building components and systems, such as asbestos, PCB's, halon or chlorine.

☐ Schools

Examples: student bodily injury, student privacy and confidentiality, student discipline, student speech, student and non-student on-campus violence, school social events, lack of parental consent and waiver for off campus activities, student internet access, physical or sexual abuse of students by staff or other students.

☐ Professional liability

Examples: failure to comply with standard of care in the profession, lack of informed consent for medical services.

Possible Advance Preparation:

☐ Hire responsible, well-qualified workforce and keep turnover low

Include: appropriate investigation of incoming employees who will work with children, the elderly, or the mentally disabled; verification of job history, credentials and licensing; reference checks; skills testing; and other investigation as indicated by the requirements of the position.

☐ Adopt and require employees to follow appropriate standard operating procedures

Include: a periodic review of standard operating procedures to ensure that they remain effective and relevant with revisions if necessary.

☐ Require ongoing, job specific training for all employees

Include: loss prevention and quality of service issues, thorough and accurate record keeping procedures, safe operation of motor vehicles, safe operation of heavy equipment and trucks, job specific standard operating procedures, good relations with citizens, what to do when an accident or injury occurs.

☐ Conduct regular and thorough safety inspections of public premises and correct identified problems

Include: periodic, documented inspections by risk management, safety personnel, or other employees external to the operation; frequent, documented inspections by supervisory personnel within the operation; education of all employees in the operation to assume responsibility for safety and address safety issues as they arise. Include inspection of grounds and outdoor recreation facilities and playgrounds. Encourage employees to report problems they observe with streets, sidewalks and other infrastructure; establish system for residents of agency-owned housing to report problems.

7. Property Loss

Some Risk Sources:

- ☐ Buildings
- ☐ Construction projects
- ☐ Recreational sites and equipment

Examples: amusement parks, athletic facilities, beaches, campgrounds, exercise equipment, golf courses, ice skating rinks, marinas/docks, parks, playground equipment, shooting ranges, skateboard/rollerblade facilities, swimming pools, winter sports sites, zoos.

- ☐ Valuable objects

Examples: art works, antiques, zoo animals, valuable books and papers

- ☐ Motor vehicle fleet, buses, watercraft, aircraft, mobile equipment
- ☐ Property leased or borrowed from others

Examples: art works, leased motor vehicles or other equipment

- ☐ Computer technology

Examples: personal computers, main frame computers, laptop computers, palm pilots, data and media, software, web site

- ☐ Business records

Examples: articles of incorporation, bylaws, deeds, leases, insurance policies corporate minutes, IRS recognition letter, state sales tax forms and charities registrations, tax submissions, financial records and pledges.

- ☐ Communications technology

Examples: antenna, satellite dishes, cellular phones, portable radios, phone systems.

- ☐ Trees

Possible Losses or Adverse Results:

- ☐ Building or facility damage or total loss; repair or replacement cost

Examples: fire, boiler or machinery failure, explosion, failure of water pipes or sprinkler system, criminal activity, natural hazard or extreme weather damage, failure of electrical system, third party negligence, obsolescence.

- ☐ Inability to use building or facility to deliver services

Examples: physical loss or damage, utility or service disruption, inaccessibility, contamination with hazardous materials/chemicals,

asbestos, lead, biohazards, etc.

- ☐ Extra expense to continue providing services at alternate site

Examples: cost of renting temporary substitute premises and equipment; cost of expediting repairs.

- ☐ Loss of or damage to other equipment and furnishings

Examples: repair or replacement costs, extra expense pending repair or replacement

- ☐ Revenue lost on damaged/destroyed property leased to others

- ☐ Loss of/damage to valuable objects

Examples: replacement cost, repair and restoration cost, expedited restoration of deteriorating objects, proper drying of wet paper or cloth.

- ☐ Loss of/damage to motor vehicle, bus, watercraft, aircraft, mobile equipment

Examples: cost of repair or replacement of equipment or a portion of the fleet and/or the cost of temporary replacement equipment to continue delivery of services.

- ☐ Property leased or borrowed from others

Examples: cost of repair or replacement, for leased items, lessor's loss of rental income while under repair.

- ☐ Computer technology

Examples: cost of repair or replacement of hardware due to damage, loss or obsolescence; sabotage or theft of data by hacker or employee; cost to restore software and data; extra expense to replace resources pending replacement or repair.

- ☐ Business records

Examples: cost of restoration of records, loss of contributor information, lost or delayed revenue.

Possible Strategies:

- ☐ Fire alarm and sprinkler systems; fire extinguishers; fire resistant construction when feasible.
- ☐ Regular and documented fire drills and regular inspection of premises for fire hazards.
- ☐ Maintain thorough and accurate inventory of building contents with values.
- ☐ Regularly assess condition of water supply and waste pipes and address maintenance issues.
- ☐ Assess security needs of each building, both during the workday and after hours, and implement appropriate building and perimeter security precautions.

- ☐ Regular inspection of boilers and machinery.
- ☐ Assess and control for hazards posed by operations on adjacent property.
- ☐ Assess susceptibility of location to natural hazard events before building

Examples: wildfire, flood, earthquake, landslide, sinkholes, hurricane, tsunami, windstorm.
- ☐ Construct or retrofit buildings to withstand reasonably expected natural hazards events.
- ☐ Conduct due diligence investigation of all property for environmental contamination before acquisition.
- ☐ Train all employees about fire safety issues presented in their operations.
- ☐ Conduct routine maintenance of public infrastructure
- ☐ Business records: hard copy and computer

Example: regular, off-site back up of software and data; advance planning for restoration

- ☐ Computer technology

Examples: regular inventory and labeling of equipment, sign-out policies for portable equipment, surge protection, internal access to system areas limited to need, security against unauthorized internal and external penetration, off-site backup of all software and data, limit employee access to internet to employees with a business need, regularly update virus protection, train employees about virus hazards, establish and enforce written procedures regarding use of computer and internet technology.
- ☐ Identify in advance all hazardous materials used or stored on premises and take appropriate action to avoid contamination of public facilities and land with these materials.

Examples: strictly enforced procedures for disposal of hazardous substances; regular inspection of storage tanks and pipelines, ensure compliance of landfills and incinerators with environmental regulations.
- ☐ Confirm licensing and/or appropriate training of all employees and contractors operating motor vehicles, aircraft, watercraft, fire and rescue equipment or other hazardous machinery on behalf of the public entity.
- ☐ Consider lightning protection systems where needed to protect property, such as rooftop mounted antennas and satellite dishes.
- ☐ For construction projects, require appropriate financial security that contractor will complete the project on time, within budget and in compliance with project specifications, building and fire codes, and other state and federal legislation and regulations.
- ☐ Property of others held or used by organization: reach agreement

in advance as to risk of loss during use, and make appropriate arrangements to finance any loss

Examples: works of art on loan, personal effects of clientele, leased equipment and motor vehicles, borrowed equipment.

- ☐ Plan for financing replacement or repair of damaged or destroyed property, including property under construction; replacement of obsolete property and equipment; and extra expense associated with continuing operations following loss of, or damage to, business property.

Possible advance preparation:

- ☐ Ensure adequate security for premises

Include: security to prevent criminal acts and special events on premises.

- ☐ Limit and carefully control use and storage of hazardous materials in operations

Include: compliance with federal and state OSHA and EPA regulations, substitute less hazardous materials when possible, regularly check storage and use areas for potential leaks.

- ☐ Require outside sponsors of events held on agency property to provide evidence of insurance or other financial responsibility for all potential losses arising from the event.

Include: general liability and coverage for hazardous activities that may require specialized coverage, such as fireworks.

- ☐ Properly inspect and maintain all equipment and vehicles used in conjunction with public operations

Include: motor vehicles, buses, mobile and non-mobile equipment, medical equipment, playground equipment, athletic equipment, power tools, ladders, ventilation equipment.

- ☐ Train all employees about requirements of laws relating to discrimination and civil rights

Include: specialized training of employees who hire others, training of all employees to avoid discrimination and civil rights violations against fellow employees, volunteers and clientele.

- ☐ Develop contingency plans to ensure continuation of critical services and operations

Include: post-disaster, disruption of lifeline services, disruption of supplies to programs, lack of employee availability, inadequate equipment or workforce.

- ☐ For all construction projects, confirm potential contractors' ability to conduct the project in a safe and responsible manner, in compliance with state and federal laws and regulations

Examples: OSHA compliance, "Before You Dig" precautions relating to underground utilities, safeguarding of adjacent property

and passersby, dealing with asbestos and lead during renovation of existing older buildings)

- ☐ Form a public risk management committee with representatives from all public operations
- ☐ Develop a system for documentation, reporting, and review of all accidents, injuries, and potential liability causing events, and for implementing any required corrective action
- ☐ Ensure that the governing board has appropriate legal advice to support its exercise of functions

8. Technology

Some risk sources:

- ☐ External attack by viruses or worms
- ☐ Sabotage of web site
- ☐ Internal sabotage (e.g., disgruntled employee erases data or passwords falling into the wrong hands)
- ☐ Theft of confidential data
- ☐ Destruction of equipment
- ☐ Equipment failure
- ☐ Power failure

Possible advance preparation:

- ☐ Installation of anti-virus software with a regular updating regime.
- ☐ Maintaining documentation for recreating your computer working environment while off site and distributing updated copies to appropriate personnel.
- ☐ Applying application and operating system security patches as they are released.
- ☐ Installation of firewall and testing that “back doors” are securely shut.
- ☐ Data mirroring of server hard drive(s) either on site or to a remote location.
- ☐ Implementation of daily, weekly and monthly backup routines (using automated utilities onto removable media such as tape or CD or through an internet backup service).
- ☐ Scheduling regular backups of all data, keeping copies off site (whether at a commercial facility or at an employee’s home).
- ☐ Backup copies, serial numbers and installation codes and instructions of application software, both on and off site.
- ☐ Installation of secure, remote access capabilities for your server.
- ☐ Installation of UPS or other power failure systems.
- ☐ Monitoring of critical passwords so that they are not easy to guess.
- ☐ Changing of system and personal passwords when an employee resigns or is terminated.
- ☐ Training employees regarding data security.
- ☐ Encryption of sensitive data.

EMERGENCY COMMUNICATION TACTICS

The movie *Cool Hand Luke* focused on a key problem in emergencies when the warden said, “What we have here is a failure to communicate.”

Communication is a key component of any emergency response and communication failure can be lethal. Those in command must receive the right information and be able to give instructions. Response teams must be able to coordinate their efforts and get information to the appropriate parties.

Two ongoing problems with communication strategies are: 1) key equipment is often knocked out by a disaster, and 2) the natural tendency for people to reach out to see if their loved ones are OK leads to system overloads.²⁴

As in all emergency planning, the key strategies are redundancy and backups.

Emergency alerts

To varying extents there is sometimes some warning before a hazard appears on the scene. Weather forecasters can predict the path of hurricanes some time in advance and post tornado warnings and watches. It is critical that each organization have a system to receive weather or security alerts as they are posted.

Emergency Alert System (EAS)

The United States Federal Communications Commission designed the EAS in cooperation with the National Weather Service (NWS) and the Federal Emergency Management Agency (FEMA). The NWS provides emergency weather information to alert the public about dangerous conditions. FEMA provides direction for state and local emergency planning officials to plan and implement their roles. The Department of Homeland Security (DHS) will also use this system under certain circumstances.

The EAS uses state-of-the-art digital technology to distribute messages. The system provides state and local officials with a method to quickly send out important local emergency information targeted to a specific area. Also, the EAS digital signal is the same signal that the National Weather Service (NWS) uses on the National Oceanic and Atmospheric Administration’s Weather Radio (NWR). This allows NWR signals to be decoded by the EAS equipment at broadcast stations and cable systems. Broadcasters and cable

NEW TECHNOLOGY

New, inexpensive all-hazard alert radios and televisions can notify you of weather and non-weather emergencies, e.g., hazardous material and chemical spills, nuclear power plant emergencies, train derailments, terrorist attacks (not colored threat condition status) and other life-threatening emergencies.

The radio or television monitors the appropriate emergency notification frequencies and will notify you using light and sound alarms.

Many of these devices have a battery backup in case of a power outage. An internet search for “all hazard emergency alert” will list manufacturers and dealers.

²⁴ For example, natural disasters such as earthquakes, tornados or hurricanes often interrupt phone and electrical service. On September 11th, 7 World Trade Center collapsed into a main Verizon facility. Not only were (land line) phones knocked out over a wide area, but most cell phone providers use these facilities so that cell phone service was compromised for a period. The collapse also disrupted some internet and E-mail service for weeks.

operators can then send NWS weather warning messages almost immediately to their audiences and can be tailored for a specific region.

Specially-equipped consumer products, such as televisions, radios, pagers and other devices can decode EAS messages. Consumers can program these products to “turn themselves on” for the messages they want to receive.

Having staff members monitor a dedicated weather radio or stations with “all-news” formats are usually effective means to receive emergency information. However, someone (and a backup) must be specifically assigned this responsibility and the organization should have a clear protocol for notifications and subsequent steps.

Many news outlets will also send out E-mail alerts or have special software that plays a message on your computer if news or severe weather alerts are in effect.

Public agencies

During the Cold War many municipalities had a siren notification system used to announce weather or other hazards. Many are updating their equipment. Some are using automated notification systems.

Commonly, emergency services rely on the media for notifications. If you don’t know your community’s plan, consult your local emergency management office.

Emergency notification services

Recently, a new industry has developed to provide emergency notification services. Many companies provide warnings on a subscription basis through computerized calling systems, fax, E-mail, or digital messaging to all types of devices. Subscribers can receive a variety of warnings via currently available technology. The Partnership for Public Warning (www.partnershipforpublicwarning.org) is a good clearinghouse for information about vendors.

Organizations can also use such technology to notify their networks and affiliated agencies. Individuals can receive an alert by fax, E-mail, phone, cell phone, pager and text message (remember, redundancy is good). Many vendors have the technology to deliver thousands of messages in minutes.

United Jewish Communities and the Conference of Presidents of Major Jewish Organizations have established the Secure Community Network(SCN) to communicate with national Jewish organizations, and through them, with hundreds of local organizations, federations, schools,

SECURE COMMUNITY NETWORK

United Jewish Communities and the Conference of Presidents of Major Jewish Organizations established the Secure Community Network (SCN)). Conceived and launched to address the need for better coordination and the dissemination of timely and accurate information about security concerns, SCN is an important first step toward a more secure, connected Jewish community.

We urge you to make sure that your Jewish institution will receive SCN alerts. For more information about SCN go to its website at www.scnus.org.

JCC's and other communal institutions in the event of a security emergency.

The Jewish Community Relations Council of New York (info@jcrcny.org) works closely with the New York City Police Department to alert synagogues, schools and other Jewish organizations.

Internal communications

Most modern, multi-line phone systems rely on external power supplies. If a power outage occurs, your phones and intercoms will, most likely, become inoperable. So what can you rely on? As always the answer is planning, redundancy and multiple backups.

You can explore battery backups and generators to solve this problem. In the very least have a "power outage", single line phone plugged into the fax line so that you can call out in the event of an outage.

Remember: Do not use wireless phones, cellular phones, walkie-talkies or other wireless communication devices in the event of a bomb threat!

Your modern phone system

As noted above, these rely on external power supplies and a flood, wind-storm or power spike could ruin the system. The installers had to program these systems, specifying, e.g., which extension is which or how to handle busy signals. It took them a lot of time to do so. If your programming is knocked out in an emergency it could delay your return to normal business.

The data on these systems can be backed up, usually to a floppy disk. Consult with your phone vendor to have them prepare a backup and keep one off site. In the event of a disaster, you can quickly restore your system.

Intercoms/public address systems

These systems are often in place. Instructions can be given from the command center and two-way systems allow for information gathering. However, they require external power.

Cellular phones

While cellular networks can become overloaded in emergencies they are a

CRITICAL TIP

During most emergencies many different things go wrong. Communication with both your responders, staff and clientele is more important than ever. Plan for various contingencies and have varied backup systems.

good communications backup strategy. Because cell phones are becoming so common, it's likely that every teacher in a school has one. Test if there are any "dead spots" in your building where cell phones will not work.

Cell phones are only useful if users have previously exchanged phone numbers. It is critical to assemble a phone number list and keep it updated. Everyone in the organization should have the emergency command cell phone number. The emergency command cell phone should have a charger and backup batteries ready for an emergency.

Nextel is a cellular phone provider that combines phone service and a walkie-talkie in a single device. They also have a "group connect" feature that allows you to contact multiple other individuals in your group (with Nextel phones) simultaneously.

All cell phones are dependent on "land line" phone systems. If the central phone switches are inoperative, the cell phone systems will also be out. In addition, your cell phone signal must be relayed by a cell tower which must have electrical power. The better cell phone providers have battery backups, backup generators and ways to power the backup generators.

Katrina destroyed many cell towers and made it impossible to refuel the generators on others. The top cell phone providers pre-positioned portable cell towers (known in the industry as COWs – celltowers on wheels) in the region but could not move them to many areas because of flooding.

Satellite phones are expensive, but they are the most reliable systems (see page 146).

ICE

Have your staff, clients and students add an "ICE" number to their cell phones. ICE, stands for In Case of Emergency." It was the brainchild of British paramedic Bob Brotchie, who thought it would be useful if people used the acronym to store the name and number of an emergency contact in their cell phone in case of accidents, crimes or disasters.

Tell people to:

- make sure the person whose name and number you are giving has agreed to be their ICE partner;
- make sure their ICE partner has a list of people they should contact on your behalf - including their place of work;
- make sure their ICE person's number is one that's easy to contact, for example a home number could be useless in an emergency if the person works full time;

IMPORTANT TIP

Not all cell phone, internet or wireless service providers are created equal. Check if your providers have solid disaster plans and capabilities (e.g., redundant equipment, backup power generators). Ask your local and state emergency agencies about the vendors they use. Also, check your facility for "dead" spots where you can't receive cell phone or other wireless services.

- Make sure your ICE partner knows about any medical conditions that could affect your emergency treatment - for example allergies or current medication;
- make sure if they are under 18, their ICE partner is a parent or guardian authorised to make decision on your behalf - for example if you need a life or death operation.

SMS/Text Messaging

Even if you can't connect on your cell phones you can often get a text message through. One hospital in New Orleans was able to send an SOS message to rescuers even though they had no telephone or cell phone service. Blackberries and similar devices use similar technologies.

Wireless Internet

Many emergency workers in the gulf states relied on their wireless internet/broadband access, giving them full access to their email, the internet and with additional equipment, internet phone service (see below). Note: this service is not yet available in all areas.

Internet Phones

While some complain that VOIP or internet phone service is not of the same quality as most "landline" providers, it has improved in quality and is a viable emergency alternative. Some systems utilize a microphone along with your computer's speakers (or a headphone). Others allow a user to plug a standard single-line telephone into a special internet router.

Many systems will allow users to begin making outgoing phone calls almost immediately after registering on a website. If you have explored the various options and have purchased the proper equipment you can actually register (and begin paying) only when you need the service. However, some services have a disconnect charge. VOIP is available through many internet providers and other companies. It is possible, for a additional fee, to reserve a phone number, receive voice mail, etc.

Two-way radios/walkie-talkies

These are one of the very few communication devices that are independent of central providers. These radios are usually battery-operated devices of limited range. Their range can be extended through "repeaters," but most technologies need power. If you rely on repeaters you will need backup batteries or generators. Pre-test devices in your building and make sure that you have extra batteries.

Runners

No technology is perfect. The Blackout of 2003 reminded us that virtually every service provider was out for a while. Your emergency planning should prepare for the possibility that none of the above communications devices

POWER OUTAGE TIPS

Professionals in business continuity planning claim that a power outage is the most common disaster that any business faces. Problems are usually quite local in nature but can affect tens of millions of people. Most nonprofits should make contingency plans but can rarely afford the sophisticated backup systems used by hospitals and emergency services. At the same time, you may need sufficient backup power for some functions.²⁵

When making your plans you should consider both local and regional power failures. During your hazard analysis process you should identify your mission-critical functions and plan how to continue them.

Equipment

Alternative power

Although it is expensive, many critical services (e.g., hospitals or emergency agencies) have made provisions for alternative power such as generators, fuel cells and batteries. At a minimum, you should choose to power certain functions (e.g., emergency lighting) and provide UPS backups for your computers so that they can be shut down without damaging the data.

If you have an alternative power source you must have contracts, in place, for equipment and fuel delivery. It is unlikely that you will find a vendor when an outage is underway.

In the event of a power outage it is a good idea to unplug sensitive equipment so that there is no damage if there is a power surge when the power returns.

Recharging

In the event of a power outage cell phone and laptop batteries can be recharged using an inexpensive inverter, widely available at consumer electronics stores. These devices plug into the “cigarette lighter” of your car and can supply some AC power. The inverter works as long as the car battery is charged or if the engine is running. Recharging your cell phone uses approximately 10W of power, your laptop 75W.

²⁵ For more information see <http://www.contingencyplanning.com/Channels/Power/preparingforoutage.asp>.

Phones

We usually don't think about which equipment needs to be "plugged in" to operate. While most phone lines provide enough low voltage current to power "plain-vanilla phones," most of today's instruments aren't plain-vanilla. If you have auto-attendant or voicemail options or your phone system or a phone with lights, displays or is cordless it probably needs additional outside power. If that is the case you should plan on having a plain-vanilla available to use during a power outage.

Ask your telephone (dial tone) provider about their backup capacity. During the Blackout of 2003 some of the low-cost providers could not provide service whatsoever while the bigger names continued to provide reliable service throughout the outage.

Your office phones often connect to a central unit, which needs power to work. So, make provisions to plug your power-outage phones into a single-line, analog phone jack. Often a fax machine is plugged into just such a line.

Cellular phones

While cellular networks can become overloaded in emergencies they are a good communications backup strategy. Because cell phones are becoming so common, it's likely that nearly every employee has one. Test if there are any "dead spots" in your building where cell phones will not work.

Cell phones are only useful if users have previously exchanged phone numbers. It is critical to assemble a phone number list and keep it updated. Everyone in the organization should have the emergency command cell phone number. The emergency command cell phone should have a charger and backup batteries ready for an emergency.

Nextel and other cellular phone providers combines phone service and a walkie-talkie in a single device. They also have a "group connect" feature that allows you to contact multiple other individuals in your group (with Nextel phones) simultaneously.

All cell phones are dependent on “land line” phone systems. If the central switches are inoperative, they too may be out.

Satellite phones

The only phone technology that doesn’t rely on local switching systems is based on satellite technology. Emergency managers are purchasing satellite phones because they will probably operate as long you can see the appropriate sector of the sky and their batteries last—except if there is a major solar flare-up.

These phones are expensive (most \$2000+) to purchase and operate. Before you purchase a system make sure to check if it works in your area. Service is sometimes limited in urban or mountainous areas.

Supplies

What should you have, in stock, In the event of a power outage?

If you are simply going to shut down during the outage and your employees and clients can drive home, you need minimal supplies on hand. In areas where people rely on public transportation, you should plan to provide basic food and water for those employees and clients who are stranded.

You will be surprised at the number of functions that depend on outside power. Flashlights²⁹ and battery operated radios are a must, along with plenty of extra batteries in various sizes. Even if you have emergency backup lighting in the halls and near the exits, there might not be provisions for emergency lighting in the bathrooms.

It is possible that some employees can not make it home due to the electrical interruption or other disaster. You should keep an adequate supply of water and canned food (remember the can opener) and consider whether you need cots, mats, pillows and/or blankets.

Contingency plans

Usually people pitch in when a crisis occurs. However, it’s a good idea to know where people live in case you need to arrange car pools, etc.

Contact the local radio stations and find out about their emergency announcement protocols. Usually they need to know who is authorized to announce a facility closing and will arrange a password. Employees may not

SUPPLIES AND “GO KITS”

“Go Kits” are prepared and maintained so that when the decision to evacuate or shelter-in-place is made, those affected will have readily available, basic provisions for coping with the task at hand.

Ideally, there should be several classes of “Go Kits.” The Emergency Management Group (EMG) maintains the Master “Go Kit” and the appropriate (redundant) backups. The master kit addresses the needs of the institution, in terms of tracking and managing people, detailing facilities and critical infrastructure, and supporting the initial recovery process. Duplicate kits should be maintained off-site, especially the documentary portion of the kits: master lists of personnel, blueprints of building layouts and critical infrastructure, and the Emergency Management Plan itself.

Additionally, area supervisors and individuals should have accessible individual “Go Kits.” For example, in schools, each teacher should have a kit for his or herself, and also one that considers the needs of those under that person’s supervision. Moreover, each student should have a personal “Go Kit” stored and accessible. While these kits may seem like a lot to assemble and maintain, they are indispensable to effectively responding to an emergency situation. Comparable provisions should be made for other types of facilities.

Each facility should develop a “Go Kit” that is readily available for use during an emergency situation. The “Go Kit” should be kept updated and should be readily accessible to use by the evacuation team in an emergency. The “Go Kit”, or a duplicate “Go Kit”, should be maintained in a safe, accessible area outside of the school building.

The American Red Cross (<http://www.redcross.org/disaster/masters/supply.html>) has developed supply lists for classrooms and school-wide needs.

How Much Food and Water

There is no simple answer to the question of emergency supplies. When experts discuss emergency planning they stress the fact that no two situations are alike. Institutions differ, there are geographic variations across North America and beyond, and there are different types of disasters. Each institution must make its own assessment.

When you did your hazard analysis you asked yourselves relevant questions: What disasters are likely in your area? What kind of warnings will you get?

Would the collapse of a bridge, tunnel or highway prevent access to your building? What don't you really have to worry about?

Once you know what you're planning for, you can begin to assess your supply needs. You create a logical, worst-case scenario. For example, schools face the potential of a hazardous chemical spill or an intruder situation which could lead to a "lockdown". A six to eight hour supply of food and water is a must for such contingencies.

Those recommending keeping a three-day supply of food and water are probably projecting simultaneous disasters: the water supply is poisoned, our water pumping stations are out and there is a stoppage of commerce and transportation (e.g., the ATMs are out and merchants can't use their cash registers or credit card machines).

The Blackout of 2003 shows that the above scenario is not outlandish. If you are a residential facility, you must have sufficient supplies to provide your charges with their needs.

However, schools and houses of worship might face a different situation. Is it likely that parents won't get to the school to pick up their kids in, say, six hours? What percentage of your student body and faculty will be your responsibility for a day, two days or three. You should have food, water, games, flashlights and other items described below, but your planning should be for likely, worst-case scenarios.

Role Identification

The members of the response team and their roles should be clearly identified using hats, armbands or vests. A stock of such items identifying the incident commander, deputies, searchers, first aid people and others should be readily available. An Israeli company manufactures such items, see www.mciresponse.com.

The Red Binder

Many of the lists, maps and plans mentioned in the "Go Kits" below should be kept in an accessible place and updated on a regular basis. One suggestion is to keep a red, loose-leaf binder with all of the information next to the door or in another convenient location. The information in the red binder should be regularly reviewed (e.g., when personnel change, after building alterations) so that it is up to date.

Master “Go Kit”

There should be one “red binder” (see above) with lists, plans and information; keys, tools, first aid supplies, etc. in an area that will be accessible in case of emergency, including:

- ☐ **Emergency plans**, including copies of building’s evacuation plan, including the chain of command, areas of refuge, etc.
- ☐ **Lists**
 - ☐ Class lists (e.g., names, digital files of individual’s photos and identification information, schedules, daily attendance status, and locations. Include list of emergency stockpiled student medication)
 - ☐ Parent’s (and alternate contact person’s) names, work and home telephone numbers.
 - ☐ Faculty and staff lists (including special skills) and schedules, home telephone numbers, alternate contact information and digital files of individual’s photos and identification information.
 - ☐ Procedural checklists.
 - ☐ Students and staff needing special assistance.
 - ☐ Phone numbers (business and cell phones) of coordinating agency contacts (e.g., UJC, JCPA, JCCA, your local federation or JCRC).
 - ☐ Emergency Response contact names and numbers.
 - ☐ Mutual Assistance Participants locations, telephone numbers and names of contact persons.
- ☐ **Maps and Plans**
 - ☐ Floor plan of building(s) marked with evacuation routes, shelter-in-place locations, exits, telephones, emergency supplies (first aid kits, fire extinguishers, emergency response stockpiles).
 - ☐ Updated as-built blueprints of building, including utilities and critical infrastructure and hazardous materials locations. Plans should highlight the location of water, gas, electrical and other shutoffs.
 - ☐ Map of local streets with primary and alternate evacuation route(s).

- ☐ **Building keys and access codes, if applicable (interior and exterior)**
- ☐ **Recent Computer backup discs or tapes (Institutions should consider routine backups to a secure off-site storage location.**
- ☐ **Equipment**
 - ☐ Bullhorn
 - ☐ Two-way radios and/or cellular telephones
 - ☐ AM/FM Weather Radio
 - ☐ Pre-programmed emergency services radio/scanner
 - ☐ Calling card and change
 - ☐ Flashlight with extra batteries and bulbs and light sticks
 - ☐ Whistle with lanyard
 - ☐ Safety glasses, goggles or face shields for eye protection
 - ☐ Dust masks and disposable N95 respirators
 - ☐ Visible identification (function or title emblazoned on back) uniform jacket, hat, vest or badge
 - ☐ Water purification tablets
 - ☐ Leather work gloves
 - ☐ Scissors
 - ☐ Tools
 - ☐ Pocket-size multi-tool with can opener
 - ☐ Hard hat
 - ☐ Shut-off wrenches
 - ☐ Crescent wrench
 - ☐ Vise grip
 - ☐ Utility knife
 - ☐ Poly Rope 1/4" x 100'
 - ☐ Poly Rope 3/8" x 100'
 - ☐ Crow Bar 24"
 - ☐ Sledge Hammer 3 lb.
 - ☐ Supplies
 - ☐ Notebooks and pens
 - ☐ White peel-off stickers and markers, or duct tape (for name tags and site marking)
 - ☐ Duct tape (2" wide)

- ☐ Orange spray paint
- ☐ Official organization stamp

- ☐ **Pre-printed forms with spaces for: directions, actions taken, or instructions, name of authority, contact information and date and time, effective date and cancellation date.**

Additional items:

Supervisor's or Classroom "Go Kit"

- ☐ Customized lists and checklists (see Master "Go Kit")
- ☐ Customized maps and plans (see Master "Go Kit")
- ☐ Record keeping forms
- ☐ Decontamination Protocols
- ☐ Clipboard
- ☐ Location signal flag (as simple as an expandable pointer and a bandana)
- ☐ Keys and access codes
- ☐ Duct tape
- ☐ Chewing gum, bottled water, snacks (quantities)
- ☐ Age appropriate activities sheets
- ☐ Spares of special needs items for those under direct supervision
- ☐ Lightweight, folding luggage cart.

Master First-Aid Kit

There are commercially available first-aid kits and many similar lists (see <http://www.redcross.org/services/disaster/beprepared/supplies.html> or <http://www.health.harvard.edu/fhg/firstaid/kit.shtml>). Some of this equipment requires training, others items require a prescription and should only be administered on the advice of an appropriate medical professional. It is always a good idea to have a person trained in first-aid on staff.

- ☐ First-Aid Manual (current) multiple copies
- ☐ Defibrillator and oxygen
- ☐ Disposable resuscitation face shields, 1 box
- ☐ IV tubing and dextrose solution
- ☐ Suture thread and needles, 1 dozen
- ☐ Scalpel blades, 1 gross
- ☐ Antiseptic solution, 32 ounces
- ☐ Tetracycline
- ☐ Bee sting kit (epinephrine pills and injection)
- ☐ Lomotil, 1 bottle
- ☐ Aspirin/Acetaminophen, 1 large bottle
- ☐ Sunscreen (SPF30), 1 bottle
- ☐ Alcohol wipes, 2 boxes
- ☐ Triangular bandage, 6
- ☐ Eye-injury kit (ophthalmic ointment, eye pad, and eye-wipes)
- ☐ Latex gloves, 1 box
- ☐ 4X4 inch gauze pads, 1 box
- ☐ Adhesive tape, 7.5cm x 4.6cm, 4 rolls
- ☐ Sanitary pads (to stop bleeding), 1 box
- ☐ Adhesive bandages, assorted sizes, 1 box
- ☐ Butterfly bandages, 1 box
- ☐ Elastic bandage, 2" x 3," 2 boxes
- ☐ Elastic bandage, 2" x 4," 2 boxes
- ☐ Abdominal pads, 2
- ☐ Burn Bandages, 4
- ☐ Eye pads, 8

HELPFUL TIP

Most local American Red Cross Chapters offer free or low-cost training classes in Standard First Aid and CPR/Automated External Defibrillation (AED) training. They will even arrange sessions on-site so that your entire staff can be prepared.

- ☐ Sterile gauze pad, 2" x 2," 6 boxes
- ☐ Sterile gauze pad, 4" x 4," 6 boxes
- ☐ Bandage gauze (cling strip 3"), 4 rolls
- ☐ Thermometer
- ☐ Motion sickness pills, 1 bottle
- ☐ Hydrogen peroxide 3% (plastic bottle), 32 ounce
- ☐ Ammonia inhalant, 1 small box
- ☐ Liquid soap (individual packets), 2 boxes

Individual First Aid Kit

- ☐ Latex gloves
- ☐ Disposable resuscitation face shield
- ☐ Antiseptic solution
- ☐ Aspirin
- ☐ Bee sting kit (epinephrine pills and injection kit)
- ☐ Tweezers
- ☐ Sunscreen
- ☐ Alcohol wipes
- ☐ Band-aids (various, including triangular, butterfly, knuckle, and fingertip)
- ☐ Field compresses
- ☐ Eye-injury kit (ophthalmic ointment, eye pad, and eye-wipe)

SPECIAL EVENTS

Dov Black's head was spinning. Marcia Fairmont, the chair of the East Cupcake Jewish Heritage Fair was telling him about all of her plans for their first fair.

"We'll attract thousands of people. We'll use every inch of this campus. We'll have klezmer music across the street in the high school and carts with Israeli food everywhere. There'll be dozens of vendors. The governor will open the program and someone on our committee knows that new, controversial author on the best seller lists, and can get her to speak, and we'll wind up the day with fireworks. Times-a-wasting! We should get to work," Marcia said.

Dov, the CEO of the East Cupcake Jewish Federation, was excited too. A well-run fair will bring in lots of new people and raise the federation's profile.

"But what headaches," he thought, "what about security, what if someone gets food poisoning from eating falafel?" "How do I plan for all this?"

Special events offer special challenges. There are books written about running special events and this manual can not offer comprehensive guidance. However, some of the issues clearly intersect with emergency planning. You should be thinking about:

Managing risk

- Should your organization be doing this event? Do the benefits outweigh the risks and effort?
- How can you reduce your risk? Do you have the capacity to adequately plan for safety concerns?
- How can you share your risk? Should you hire an events planner? What other vendors should you contract with? Are they insured? Is your insurance coverage adequate?

Insurance

Special events are often beyond the normal scope of your normal activities and may require special insurance arrangements. Activities such as serving liquor or a boat ride are outside the parameters of many standard insurance policies. Contact your insurance broker early in the special event planning process to learn whether the event is covered under your existing policy, or if additional coverage is needed.

Your general liability policy also might not apply if the magnitude of risk is much larger than anticipated in the application for insurance. Special events can fall into this category.

Additional insurance coverage can be obtained through a special events policy or by increasing your general liability policy or obtaining a specific endorsement to it. Your agent or broker should be able to advise you about the alternatives.

Protection strategies

While your day-to-day security might be tight, special events create special security problems. The first step is to gauge how the event changes your organization's security profile. Events that are publicly advertised are more likely to attract security problems than those that are advertised internally. Governmental officials or controversial speakers could attract problems. Your security planning should take note of these factors. Consult with your local police and make adequate preparations.

- Your security staff might routinely require id's from all staff and guests. They know your "regulars". How will you screen people before admission to your event? Do you need metal detectors and/or search bags? If so make sure that you have enough equipment and personnel to quickly handle the crowd.
- Review your evacuation and lockdown plans in light of the special event. Your facilities might be filled to capacity. If you are using an outside facility make sure that you and your staff know the procedures for that site. Hold special drills or tabletop exercises to anticipate potential problems.
- People want to feel safe at your event. Make sure that you have trained, visible, identifiable (e.g., uniforms, blazers, t-shirts, sashes) security personnel stationed at key places before, during and after your event.
- Develop a "lost child" procedure and make sure that your security staff are fully prepared to respond to parents and children.
- Your higher profile can attract threats. Review your bomb threat procedure and make any changes that are necessary. Consult with your local law enforcement officials and ascertain if any other agencies will have jurisdiction at your event (e.g., the Secret Service takes precedence at events involving the President and visiting Heads of State or Heads of Government).
- Thieves take advantage of special events, especially if cash is involved. Minimize your exposure by planning to safely move cash to a secure area throughout the event. Lock areas that will not be used during the event.
- Major events often require construction and equipment placement the night before the event. Make sure that your security plan stations personnel to guard open equipment.

Crowd and traffic control

Scholars in crowd control note that crowds can develop a personality of their own. As an event manager you want to be able to control that. For example, a panicky crowd is dangerous to all concerned.

You should control entry to your facilities and plan for the contingency that too many people might show up. If you are using tickets, make sure that you don't sell or give away more tickets than there are seats. Even airlines plan for no-shows, but you must have a way to accurately predict them. Allowing too many people into an event is dangerous.

People counterfeit tickets for rock concerts and have been known to counterfeit tickets for certain speakers. In today's world of scanners and color copiers it's not difficult. If you are relying on tickets to control entry make sure that they are copy resistant.

- What is the capacity of facilities used for the special event? Are you likely to exceed the capacity?
- What kind of equipment do you need for crowd control? For example, ropes and ribbons can be used to keep people in line or out of areas that should be kept clear. Signs and announcements over PA systems or bullhorns can help to direct the crowds.
- How many staff or volunteers should be assigned to direct crowds? Do you need ushers or marshals (at a rally)? What kind of directions and training should they receive? How should they communicate to the central office?
- Have you developed open corridors (both outside for emergency vehicles and inside) so that emergency responders can easily reach injured individuals?
- Have you adequately planned for parking?
- Will the local police help with traffic control?

Disturbances

Unfortunately, some people may try to use your hard work to make their point. If you have a prominent or controversial speaker or deal with certain issues there may be demonstrators or hecklers. You should plan for them.

If you can control entry into your event the demonstrators can be kept outside. Police can set up a "demonstration area" that will allow the demonstrators their constitutional rights, yet keep them from directly interfering with your event.

Once demonstrators are “inside” you may need to have them removed. You should consult with your local police before the event and learn about their policy and develop your own within their guidelines. Under what circumstances should people be removed? Will the police remove someone who is disrupting the event or do they expect your security guards to do so? Does someone have to make a formal complaint? Do you have a designated person who will work with police?

Accidents

- Do you have personnel who are trained on how to handle accidents and what to do next?
- Are the first aid facilities conspicuous and readily available?
- Do you have a formal accident reporting procedure (e.g., incident report, pictures, what level of accident should be reported to insurers)?
- Are appropriate supplies (e.g., first aid kit(s), incident reports, disposable camera) available?
- If you are using outside personnel, are they adequately insured?

Working with governmental agencies

Government regulations can restrict the sale of food and liquor, the use of amplified equipment, fireworks or a host of other special event activities. Make sure that you obtain all of the necessary licenses and permits.

If you are using a public area you might need to work with your local parks department. Everyone should be coordinating with their local police (and possibly fire) authorities.

Animals

Animals are often a welcome attraction at special events. However, check local requirements, obtain the proper permits and make provisions for appropriate holding areas, handlers, sanitation, etc.

Vendors

Vendors are often an important component of special events. They can provide the food or other special goods. Often they subsidize the event by paying for space and/or sharing a percentage of their sales.

It is your responsibility to check whether your vendors have the appropriate licenses and permits for their activity (e.g., those running your falafel stand might be required to have food handling permits). You should speak to your attorney about the type of contract vendors should sign. Should they have to prove insurance coverage? Should you be an “additional named insured” (see [Insurance Considerations](#), P. 102). What if a vendor sells a faulty product or a guest burns themselves on a stove, how are you protected?

PERSONS WITH DISABILITIES

People with disabilities often need more time than others to make necessary preparations in an emergency. The needs of older people often are similar to those of persons with disabilities. Your evacuation plan should identify those with disabilities and provide for their needs. Federal disability discrimination laws (see <http://www.eeoc.gov/facts/evacuation.html>) do not prevent employers from obtaining and appropriately using information on disabled individuals necessary for a comprehensive emergency evacuation plan.

Some specific considerations are:

- Because disaster warnings are often given by audible means such as sirens and radio announcements, people who are deaf or hard of hearing may not receive early disaster warnings and emergency instructions. Be their source of emergency information.
- Some people who are blind or visually-impaired, especially older people, may be extremely reluctant to leave familiar surroundings when the request for evacuation comes from a stranger.
- Special evacuation plans are required for high rise buildings.
- A guide dog could become confused or disoriented in a disaster. People who are blind or partially sighted may have to depend on others to lead them, as well as their dog, to safety during a disaster.
- People with impaired mobility are often concerned about being dropped when being lifted or carried. Find out the proper way to transfer or move someone in a wheelchair and what exit routes from buildings are best.
- Some people with mental retardation may be unable to understand the emergency and could become disoriented or confused about the proper way to react.
- Many respiratory illnesses can be aggravated by stress. Plan to have oxygen and respiratory equipment available.
- People with epilepsy, Parkinson's disease and other conditions often have very individualized medication regimens that cannot be inter-

rupted without serious consequences. Some may be unable to communicate this information in an emergency.

For more information see specific guides on evacuating persons with disabilities:

<http://www.access-board.gov/evac.htm>

<http://www.redcross.org/services/disaster/beprepared/disability.pdf>

<http://www.fema.gov/rrr/assistf.shtm>

<http://www.oes.ca.gov/Operational/OESHome.nsf/LevelTwoWithNav?OpenForm&Key=Plans+and+Publications>

<http://www.nod.org/pdffiles/epi2002.pdf>

<http://www.usfa.fema.gov/downloads/pdf/publications/FA-154.pdf>

STAFF AND CLIENTELE DURING AND AFTER CRISES

Clearly, disasters are, by definition, traumatic events and have a psychological dimension. Emergency planners should be prepared to appropriately respond. The federal government has resources available for different types of populations at: <http://www.hhs.gov/disasters/index.shtml>.

Dealing with employees

As a general rule, employers are responsible for the safety and welfare of their workers. During disasters many of your employees have two roles: victims and for many, responders. Employees who are members of your response teams will be responsible for their fellow workers and perform unfamiliar tasks while worrying about their own safety and wondering about the safety of their loved ones.

There couldn't be a better recipe for rampant stress? Your emergency plan should do whatever possible to minimize stress. Your goal is to empower employees so that they know that they can take care of themselves and their families. People can and do function effectively in spite of being afraid – even when they are afraid.

Remember training and drills

The more familiar and automatic a situation is to an employee the less traumatic it will be. If your employees have gone through a variety of exercises and drills (see [Drills and Exercises](#), pp 40 ff.) they will be both mentally prepared for emergencies and be well trained to do their assigned tasks.

Help them help themselves

Your employees are human. More often than not, when the earthquake or tornado strikes a teacher's first thought might not be about caring for her students, but worrying if her own children are all right.

As an employer it is to your advantage to help your workforce make emergency preparations for themselves and for others. Do they have a Go Kit at work and at home (see pp. 146 ff.). Do they have an emergency communication plan for their families (e.g., who to call, where to meet, etc.).

³⁰ Bradley D. Stein, MD, MPH, collected these recommendations. He is Assistant Professor of Child Psychiatry at the University of Southern California and the National Institute of Mental Health Faculty Scholar at the RAND/UCLA Health Services Research Center and leads a project at the Rand Corporation on the impact of terrorism on schools.

There are many wonderful household preparation guides, including information found at www.ready.gov and http://www.nyc.gov/html/oem/html/readynewyork/ready_guide.html. Most local red cross chapters offer classes at worksites or nonprofits. Offer your employees training. Give them one less thing to worry about.

Plan to shelter

Are you ready if a disaster strikes and your employees can't go home? Do you have food, water and blankets in case of emergency? Have you worked out an emergency overnight housing plan with employees who work nearby? Do you know if the medical condition of any employees would significantly worsen if they did not have access to their medication for 4, 8, 12 or 24 hours? Have you reminded such employees to have extra dosages in the event of an emergency?

Longer term needs

Stress symptoms are normal and prevalent in the aftermath of a disaster. Be alert. Work with your local mental health agencies to help you to identify symptoms and to provide programs that build resiliency and adaptive coping.

Students²⁶

There are a number of different guidelines available for talking with children in general—some are better than others. The better ones normally hit the following points:

1. Find out the child's perspective of what is happening by asking them. Listen and answer questions briefly, honestly and calmly in a way that's appropriate for the child's age.
2. Children want to know that they are safe—it's not something that we can honestly promise them. But what we can tell them is all the things that people are doing to keep them safe.
3. Let them know they are cared for and loved and not alone.
4. Make an extra effort to try to maintain daily routines.
5. It's probably OK to let children know that you are a little afraid—children are smart, they are going to know that anyway. Parents can serve as a role model for kids, showing them how one can be appropriately afraid, yet still be courageous and go on with one's life.

6. Constructive actions and positive coping help.
7. Don't pretend that there isn't anything going on—kids are smarter than that.
8. Be aware that children at different ages are going to have very different concerns. Teens are often forgotten because they seem OK and people are focused on younger children. Conversations with them will be very different from conversations with elementary school-aged children.

Post-disaster interventions

Disasters have taught us about the necessity of follow-up crisis counseling services. The purpose of the crisis counseling program is to help relieve any grieving, stress or mental health problems caused or aggravated by the disaster or its aftermath. There are often short-term services funded by governmental agencies.

Mental health experts say that disaster-related stress may surface days or even months following the event, and affects children as well as adults. Parents can find ways to assist their children in handling stress associated with the events on the FEMA for Kids web site, at www.fema.gov/kids.

Stress is a natural reaction. The most common symptoms of stress include irritability, anger, fatigue, loss of appetite, sleeplessness, nightmares, sadness, depression, headaches, nausea, hyperactivity, lack of concentration, and increased alcohol and drug abuse. Your disaster planning should identify an agency that you can turn to in the event of problems with students, clients, employees and volunteers.

Logically, your local Jewish mental health agency should take the lead in providing such services, in coordination with the Red Cross and governmental agencies.

PREPARING YOUR BUILDING FOR AIRBORNE CHEMICAL, BIOLOGICAL OR RADIOLOGICAL ATTACKS

According to intelligence sources, the possibility that terrorists may use chemical, biological, or radiological (CBR) materials may increase over the next decade. However, CBR incidents can be triggered by an industrial accident or a chemical spill caused by a vehicular collision.

No matter what the cause, you must be prepared to respond quickly and appropriately should a CBR incident occur. Some good basic guidelines to aid your decision process are available from the National Defense University at http://www.ndu.edu/ctnsp/wmd_tipsheet.htm. Another resource can be found at <http://www.rand.org/publications/MR/MR1731.2/>.

Security and facility managers need reliable information relative to how they can modify their buildings to decrease the likelihood or effects of a CBR incident and respond quickly and appropriately should a CBR incident occur. These managers should be prepared in advance to insure that effective decisions are made in the midst of a CBR incident.

There are several short-term actions that can be implemented immediately to help limit exposure to an incident. Getting to know your building may be the simplest way to protect it and can best be handled by conducting a walk-through inspection, including but not limited to HVAC, fire protection and life-safety systems. Here is a list of the items to consider during your walk through:²⁶

- What filtration systems are in place? What are their efficiencies?
- Is all HVAC equipment properly connected and controlled? Are equipment access doors and panels in place and appropriately sealed?
- Are all dampers (outdoor air, return air, bypass, fire and smoke) functioning? Check to see how well they seal when closed.
- How does the heating, ventilating, and air conditioning (HVAC) system respond to manual fire alarm, fire detection, or fire-suppression device activation?
- Are all supply and return ducts completely connected to their grilles and registers?
- Are the variable air volume boxes functioning?

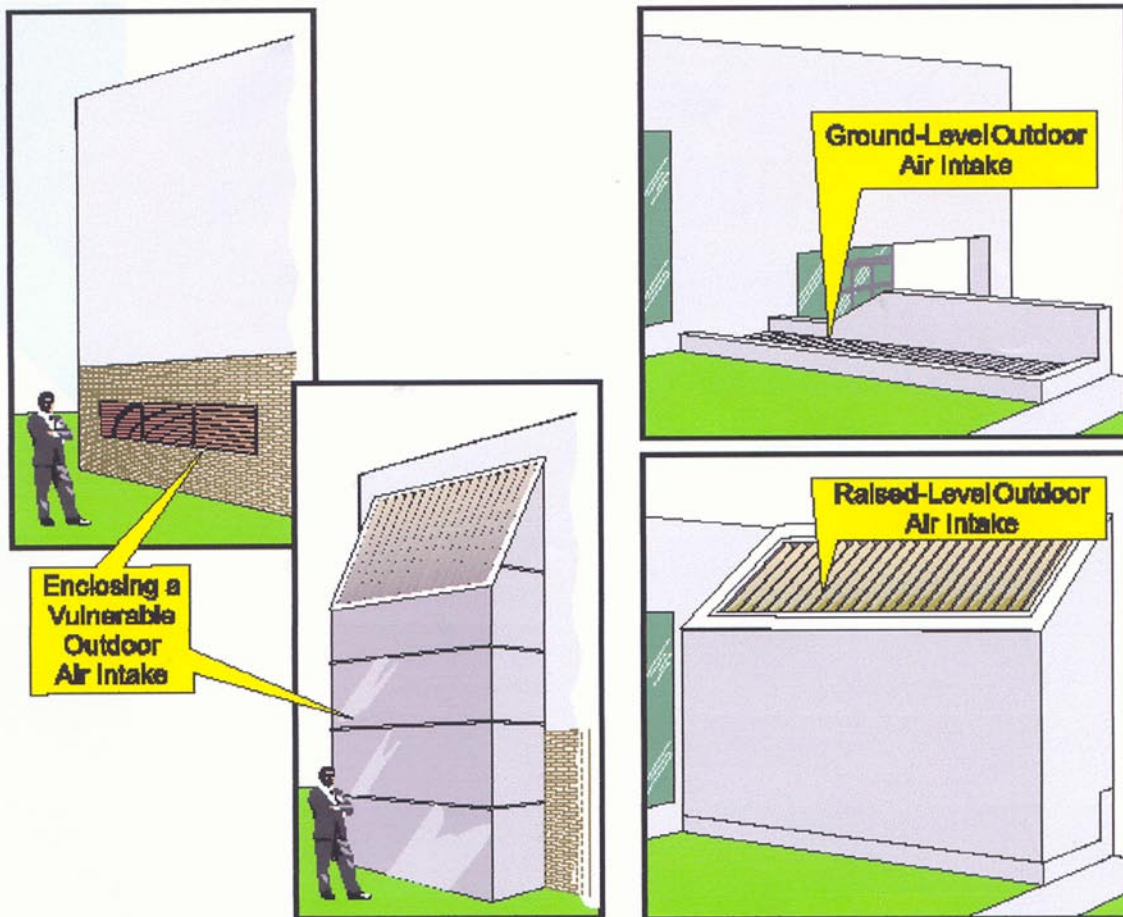
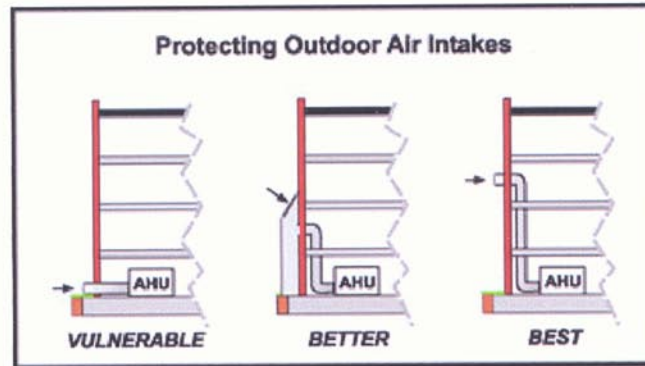
²⁶ Most of this section is adapted from *A Guide for Protecting Building Environments from Chemical, Biological or Radiological Attacks*, New York City Police Department, Counter-terrorism Unit, 2002.

- How is the HVAC system controlled? How quickly does it respond?
- How is the building zoned? Where are the air handlers for each zone? Is the system designed for smoke control?
- How does air flow through the building? What are the pressure relationships between zones? Which building entry ways are positively or negatively pressurized? Is the building connected to other buildings by tunnels or passageways?
- Are utility chases and penetrations, elevator shafts and fire stairs significant airflow pathways?
- Where are the various system shut-offs. How do you prevent your heating or cooling system from using outside air?
- Is there obvious air infiltration? Is it localized?
- Does the system provide adequate ventilation given the building's current occupancy and functions?
- Where are the outdoor air louvers? Are they easily accessible?
- Are they or other mechanical equipment accessible to the public?
- Do adjacent structures or landscaping allow access to the building roof?

Preventing access to a targeted facility requires physical security of the entry, storage, roof and mechanical areas, as well as securing access to the outdoor air intakes of the building's HVAC system. The physical security needs of each building should be assessed, as the threat of a CBR attack will vary considerably from building to building. For example, the threat to a large corporate headquarters may be considered greater than the threat to a small retail establishment. Some physical security measures, such as locking doors to mechanical rooms, are low-cost and will not inconvenience the users of the building. By first assessing the vulnerabilities of the building, security managers can better address physical security in an effective manner. While the identification and resolution of building vulnerabilities will be specific to each building, some security actions are applicable to many building types. These include:

Preventing access to outdoor air intakes

The illustrations on the following page show several short-term goals that can limit the exposure to a CBR incident. This is accomplished by elevating the outdoor intakes including an open buffer zone between the public areas and the intake louvers. The key element to the design of the enclosures should be that any device would “roll off” the enclosure.



Other Considerations

- *Preventing public access to mechanical areas.* This can be strictly controlled by keyed locks, key cards or similar security measures.
- *Preventing public access to building roofs.* Fencing or other barriers should restrict access from adjacent roofs.
- *Securing air-return grilles.* Relocate air-return grilles to inaccessible, yet observable locations; increase security presence (human or CCTV) and direct public access away from air-return grilles.
- *Restricting access to building operation systems by outside personnel.* Building staff members should escort these individuals throughout their service visit and should visually inspect their work before final acceptance of the service.
- *Restricting access to building information.* Release only to authorized personnel.
- *Developing secure procedures.* Keep a logbook to record who enters mechanical areas and the roof and when. The logbook should record all repair personnel and visitors to these areas. These individuals should be escorted at all times.

Rapid response, such as shutting down an HVAC system, may also involve closing various dampers, especially those controlling the flow of outdoor air in the event of an exterior CBR release. Building managers must ensure that all personnel are aware of the proper procedure for conducting an emergency shutdown of the HVAC system. The procedure should be kept in the “[Red Binder](#)” (P. 147).

In addition to physical security needs, managers should maintain an information folder easily accessible to emergency responders. The folder should contain fundamental building information, possible CBR threat scenarios and the associated responses and procedures for communicating instructions to building and emergency personnel. The folder should be comprehensive, thus enabling responders to make well-informed decisions.

First Responders Information Folder

Contents of the folders should include the following information:

- Building Name
- Location
- Description, physical layout, emergency exits, etc.
- List of occupants (corporate names, types of business, affiliations, emergency contact information)
- Are industrial hazards stored at the location? If yes, what and

where?

- Day/ night population
- Type of area surrounding site (residential, business, theater)
- Photos
- Location of HVAC system, controls and all fresh air intakes
- Evacuation routes
- Past-threat history
- Elevator locations
- Key dates or anniversaries
- Resident activities that may be targeted by activists
- Symbolic value of location
- Vulnerabilities of the building
- Emergency shut-off locations, alarm codes and locations.

Reducing a building's vulnerability to a CBR incident requires a comprehensive approach that must include periodic staff training, particularly those with specific life-safety responsibilities. Holding regularly scheduled practice events, similar to common fire drills, increase the likelihood for success in an actual event.

Decisions concerning which protective measures to implement should be based upon the threat profile and a security assessment of the building and its occupants. While physical security is the first line of defense, other issues must also be addressed. Preventing possible terrorist access to outdoor air intakes and mechanical rooms and developing CBR-contingent emergency response plans should be addressed as soon as possible. While it is not possible to completely eliminate the risk of a CBR incident, several measures can be taken to reduce the likelihood and consequences of such an incident.

Many of the recommendations presented herein can be implemented reasonably quickly and cost-effectively. Security managers should assess a building by looking first at those items that are most vulnerable and can be addressed easily. Additional measures should be implemented as feasible. The goal is to make your building an unattractive target for a CBR incident and to maximize occupant protection in the event that such an incident occurs.

DEALING WITH THE MEDIA DURING CRISES

Initial Steps

Have an established relationship with the police and other emergency responders. Let them know what your emergency plans are.²⁷

Have a designated spokesperson who can respond to an incident at your organization. He/She should be trained in how to effectively handle the media in a crisis and know the essential message points that the organization wants to make and which questions should not be answered.

Your plan should include methods to inform key stakeholders (e.g., parents, students, board members, volunteers, clients) in a timely manner—before they hear about a crisis in the media.

Bear in mind: your interests during a crisis are different from the media's. They want to gather as much information as possible. At times, some media outlets stress sensational elements of a crisis. Your goal is to accurately and appropriately inform your staff and clientele of the situation before they hear about it on the news. To do so, you must work closely with the on-the-scene emergency commanders.

REMEMBER

- *Choose a single spokesperson.*
- *Coordinate with emergency personnel.*
- *Convey information as quickly as possible.*
- *Your credibility is your most important asset.*

During a Crisis

The spokesperson should consult with the appropriate professional or lay leaders and emergency commanders before speaking to the media and work closely with clientele coordinators to ensure that everyone receives a consistent message.

If you make a determination that a threat is to be taken seriously or an incident occurs, activate your crisis plan. Once police notification and the appropriate life-safety actions (e.g., evacuation) are completed:

- Assume media will be notified because they monitor police radios.
- Only the designated spokesperson should speak with the media.

²⁷ Prepared in association with Howard J. Rubenstein Associates. There is an extensive literature on emergency risk communication. A good place to find more information is: http://www.cdc.gov/communication/emergency/erc_overview.htm.

- Have a staging area where parents can pick up those evacuated from the building. Try to find a building nearby that emergency personnel can secure and declare “off-limits” to the media.
- Tell parents they should not speak to the media, even when the media is persistent.
- There is no need to release any names to the media until families are told.
- When you speak to parents, do not tell them anything you will not be comfortable saying to the press. Your statements will always get to the media.
- Let police be the main spokespeople to the media. They will have more information about the crisis and will not wish to release information that would compromise an investigation.
- Try to do your press conference with police.

Key Message Points

- The safety of children and employees is of paramount concern to you.
- No one was hurt (or injuries were limited).
- Your organization was prepared and implemented your emergency plans, which were formulated in consultation with the emergency responders.
- You have a mechanism to respond and assess threats and you made the decision (along with the police) to close the institution.

Incident-Dependent Message Points

These will vary depending on incident, but some general points are:

- You will need to determine your history of threats and make a decision on what information you want to release. For example, “this is the first threat the school has ever received.” Take guidance from police on what you release to the public. Check with police before you give out the specific nature of any threat.
- Express sadness when appropriate.
- Note your thoughts and prayers for injured when appropriate.

- Comment on violence in society or terrorism when appropriate. Take care not to draw conclusions beyond the evidence at hand.
- Thank the police and other emergency responders.
- Thank your staff.
- Discuss heroic behavior on the part of a child, staff or police, when appropriate.

DATA AND DOCUMENT PRESERVATION

The warnings were ominous. Hurricane Pam was on the way and it was going to be a big one. East Cupcake was directly in its track. The staff at the East Cupcake Jewish Federation knew that they had to make all sorts of plans.

It was worse than anyone had imagined. The effects of the storm surge and the wind added misery and destruction to the flooding. The leadership and staff of the East Cupcake Jewish Federation were fine but they knew they had to start to get back to business.

Fortunately, the Upper Cupcake regional office was unscathed. It even had phones, internet service and power. The East Cupcake staff could work out of a conference room there. They set up a command post, brought in their laptops and cell phones and were ready to get to work.

But where were their computer records? Their staff had faithfully made tape backups and stored them in a fireproof room at the federation office. Now the tapes were floating alongside the computers in the federation office. All of their documents . . . all of their lists . . . all of their donor records. Maybe they could be recovered but no one could get to them soon.

Document backup strategies

So what do you do if your documents are destroyed? Often disasters create the necessity to show people various documents. They should be readily available. Otherwise, the job of finding necessary documents is added to your recovery burden.

In case of emergency, you should know that some documents (e.g., deeds or articles of incorporation) are filed as public records. Others are prepared by professionals such as lawyers and accountants. You should ask to keep a full set of your backup corporate documents in their offices. Make sure that they have a current set in their office files, rather than a less-accessible warehouse.

Some records are already in computer form (e.g., you prepared your bylaws or board minutes using your word processor), or can be scanned into the computer. Such records are backed up if your computer backup system is sound.

Corporate records

Examples of corporate records that should be backed up are articles of

incorporation, bylaws, deeds, leases, insurance policies and corporate minutes.

IRS and other tax data

Examples of such documents that should be backed up are: your IRS recognition letter, state sales tax forms and charities registrations. Most IRS 990 forms can be downloaded from www.guidestar.org. New documents can be obtained from the issuing authorities, but that takes time and effort.

Sometimes this time and effort can slow down recovery efforts. For example, an organization exempt from sales tax would not have to pay sales tax on the construction materials used in rebuilding and repair. However, contractors and vendors might insist on the proper certificate before starting work. A call to state tax authorities would probably yield new documentation, but that phone call would have to compete with the thousand other details that come up during recovery.

Financial and Pledges

Some documents are obvious, e.g. your certified audits (which are usually kept by your accountant). But you have all kinds of financial records. In case of disaster can you reconstruct your accounts payable and receivable? Rest assured, your creditors will have records of their bills to you, but do you trust that the new bills will be accurate?

Pledges are another concern. If major pledges are merely recorded in the computer records without the underlying documentation, you might get into a dispute with an estate in the event that the donor has died. It's a good idea to review your files with disaster planning in mind. What pieces of paper would you need in the aftermath of a disaster? How can you safeguard them?

Data ²⁷

All data should be backed up regularly. You should decide on a policy regarding the frequency of backups (e.g., daily or weekly, incremental or full), based on data criticality and the frequency that new information is intro-

²⁷ Much of this information is selected from NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, June 2002. This publication has many details not included in this manual. The Guide is available from <http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>.

duced. When you think about data backup policies you should consider:

- Where will you store the backed up data?
- How often will you back up?
- How often will you reuse your backup?
- How will you get the data off-site?

Data may be backed up on magnetic disk, tape or optical disks such as compact disks (CDs).

Making daily backups can be inconvenient. However, if your systems are not backed up more often you risk losing any files or changes made in the interim. Your backup system should be automatic, with the ability to make unattended backups.²⁸

Most often, backups are made on a daily basis. Some people reuse the tapes the following week, keeping the “FRIDAY” tape as a weekly archive. Your method should be based on how often your data changes and how important it is for the files and databases to be exactly right in the aftermath of a system failure.²⁹

Networks vs. workstations

Today, many network servers are available with sophisticated backup capabilities, including RAIDs (Redundant Arrays of Independent Disks) that allow several hard disks in the server to mirror one another. Ideally, there should always be a functional copy of your data, even if one hard drive fails. When critical files are kept on a server it is efficient to invest in such sophisticated equipment.

Many people think that “everything” is backed up. Unfortunately, software on each individual computer has to be instructed to save to the network rather than the local hard drive. If your E-mail, word processor or spreadsheet program only saves to your “C” drive, your work will not be automatically backed up. When you install new programs, make sure that you modify the “file save” defaults so that your work will be automatically saved on your server.

Backup systems can be placed on individual work stations (computers). If each computer is to be backed up, each individual is responsible for off-site

DON'T FORGET YOUR EMAIL

Unless you have your own mail server most people only have copies of their email on their own computer. If their hard drive crashes many valuable documents (emails and attachments) can disappear.

You can regularly backup your email onto your server or automatically or you can get a free email account (e.g. Hotmail or Gmail) and set your email account to automatically forward a copy of your email to the off-site account.

²⁸ Unattended can be a relative term. Someone should switch the backup medium regularly if you choose a non-internet off site backup.

²⁹ Unfortunately, there can be errors in a backup. It's critical that your backup program verifies that the backup program has done its job and that someone checks the backup log to see which files were not backed up.

backups themselves.

Many organizations use a fireproof safe to store their backup media.

Off site storage

It is good business practice to store backed-up data off-site. Small organizations wishing to minimize off-site storage costs can simply designate a reliable employee to take the daily backup home each night.

Many organizations now use internet-based electronic tape vaulting. Your data will either be constantly mirrored (i.e., data on the second site will be a mirror image of the first.) at your vendor's facility or your backup will be copied to that site on a regular basis. There are often fees for set up, installation, ongoing maintenance, customer support and usage (time, quantity and frequency). One rule of thumb is that a T1 connection is preferable if you are going to back up more than 2 GB of data and a cable/DSL line is acceptable if your backups are smaller than that.

Commercial data storage facilities are specially designed to archive media and protect data from threatening elements. If using off-site storage, data is backed up at the organization's facility and then labeled, packed and transported to the storage facility. If the data is required for recovery or testing purposes, the organization contacts the storage facility requesting specific data to be transported to the organization or to an alternate facility.

Alternate sites

Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. Thus, the plan must include a strategy to recover and perform system operations at an alternate facility for an extended period. This site is usually associated with your alternate command center.

These alternate sites may be owned and operated by the organization (internal recovery), or commercial sites may be available under contract. The alternate site might not have enough computers for everyone in your office. Your emergency plan should designate how to "scale back"—who gets access to the available resources and who should share.

Two or more organizations with similar or identical IT configurations and backup technologies may enter a formal agreement to serve as alternate sites for each other or enter into a joint contract for an alternate site. This type of site is set up via a reciprocal agreement or memorandum of understanding (MOU, see [Mutual Aid and Assistance](#), P. 111).

OFF-SITE BACKUPS

As hard disks get cheaper and broadband more prevalent there are many firms that offer relatively inexpensive off-site backup.

Special software can be installed on your server to automatically track every file that is created and/or changed in designated directories (e.g., those containing your documents and databases).

The software then copies compressed versions of those files to an off-site location. The backups can be readily restored to another computer.

Internet access

What happens if your internet provider goes out? In most cases, you can still use your modem to get dial-up internet access and set up your computer network to use internet connection sharing so that several people can use the same connection. You should maintain a dial-up account for such eventualities.

Remote access

Telecommuting has made it possible for many individuals to work from home. There are many safe and secure methods of gaining access to a corporate computer network. A local emergency might block access to your site, but leave your equipment running. If that's the case, you can use your remote access. When your computers are down, but your network is mirrored off-site, you will easily have access to your files.

Anti-virus protection

In this era of E-mail and internet connectivity, most computer disasters are caused by computer viruses and worms. Each computer must have anti-virus software that is kept up-to-date with current virus definitions, and someone must be responsible to monitor and install product security patches.

Program backups

You might have your data and still not be able to use it if you don't have the appropriate programs on your alternate site computer (or if your current computer is damaged). Make copies of your program disks and store them off site so that you don't have to get copies in case of emergency.

Recovery documentation

There should be a central, hard-copy file that includes a record of the up-to-date passwords and vendor contact information in case your primary computer staff person is not available.

GUIDELINES FOR HIRING A SECURITY CONTRACTOR

Security Consciousness

The potential for anti-Semitic incidents, or even terrorist attacks increases during times of high visibility and activity by the Jewish community. The reality today is that a large number—if not the overwhelming majority—of Jewish institutions consider and often hire security contractors for a special event or on a regular basis. Institutional leaders should have the necessary tools and information to make informed choices.



Indicators of Potential Exposure

Initially, it is of critical importance to determine if increased security measures are necessary. If an institution has experienced any of the following threats, it may wish to explore hiring a security contractor:

- Written or verbal threats
- Hate-based graffiti
- Theft or unexplainable losses
- Appearance of mysterious packages
- Local crime patterns

If recent crimes in your area suggest an increased risk or if there is a sense of insecurity in your organization, a security contractor may create an increased sense of security.

In general, security decisions should be made in consultation with you local police.

Guidelines for Using Security Contractors

Once a decision is made that your institution has immediate or long-term security needs, it should be determined whether limited or complex security requirements are necessary. ADL strongly recommends that each institution undertake security as a long-term, on-going process.

Since 1913, the Anti-Defamation League has worked “to stop the defamation of the Jewish people and to secure justice and fair treatment to all citizens alike.” Now one of the nation’s premier civil rights/human relations agencies, ADL fights anti-Semitism and all forms of bigotry, defends democratic ideals and protects civil rights for all. As part of ADL’s effort to protect the safety and well being of the Jewish community, the League continues to provide the Jewish community with tools and training to effectively create secure environments.

Statement of Work

During holidays or special events where security guards may be required on a short-term basis, institutions should obtain competitive bids as soon as possible. It is essential to check with local law enforcement and other community agencies for recommendations. Further, the institution should define the security contractor's scope of work. All of the following criteria should be met:

- A concise statement describing the security tasks to be performed, including the number of days and hours that security is needed. This information should be clearly outlined with the Security Contractor before security staff is assigned to the site.
- A detailed set of general and particular special instructions. The importance of these instructions cannot be overstated. The institution should not rely on the security contractor to provide them. These instructions should be discussed with and agreed upon between the decision-makers of the institution and the security firm.
- Assignment of one person who will be the security guard's contact, and will greet the security guard upon arrival to ensure that the security guard understands his/her role, and among other requirements, has a neat appearance and proper attitude.

Security Guards

First impressions are important in determining how the security guard will perform. It is important to remember that the security guard is present to deter and detect unusual or suspicious activity as well as to safeguard property and people. To someone assessing whether your institution is a "hard" or "soft" target, a perception of security is as important as actual security. Your entire security plan, including your guards, should project both.

Key points

When hiring a security guard, discuss with him/her the rules of conduct that will enhance effectiveness. For example, no smoking, practical joking, fraternizing, etc. Good supervision is essential, e.g., Assess the security guard during the shift for alertness.

Security guards are often the first people your clients see. They should project an air of professionalism while maintaining the welcoming atmosphere your clients have come to expect.

Scope of work

Your security guards should have the information necessary to do his/her job. Explain the scope of work and provide in writing concise expectations

as soon as the security guard is hired. Some issues include:

- Institutional contact and how to immediately reach him/her.
- Requirements of the assignment.
- Purpose of security during the prescribed times.
- Layout of the facility.
- Facility security and/or fire regulations.
- Any particularly vulnerable areas.
- Locations of telephones, fire-fighting equipment, fire alarms, emergency exits, etc.
- Location of stairways and doors.
- In the event of an emergency (fire, suspicious package, bomb threat, etc.), clear operational guidelines.

Criteria for Security Contractor Selection

As soon as the need for a security firm has been determined on an immediate or long-term basis, a security contractor should be selected. Selecting a company that has valid, current state licenses is essential. To determine the reputation of a security contractor, it is advisable to investigate any history of complaints about the prospective security contractor reported to the state licensing authority. You should be certain that a company is reliable and in good standing.

Some of the criteria that should be considered are:

Insurance

After a security contractor's license has been established, scrutinize the insurance coverage the security contractor provides. The following criteria should be met prior to hiring a security contractor:

- The contractor provides and maintains adequate insurance coverage for your situation.
- Your risk manager (insurance agent) approves of the contractor's coverage.
- Contractor's Broad Form General Liability Insurance covers a minimum of \$1 million per incident and \$3 million total. The higher the coverage the better.
- Workers Compensation Insurance is at statutory minimums.
- Vehicles utilized by the security contractor have adequate Automobile Liability Insurance coverage
- Security contractor's insurance covers sexual harassment through their Professional Liability coverage.

- Liability coverage for special equipment provided (golf carts, computer equipment, watch clocks, etc.).
- Contractor's insurance carriers name your organization as "Additional Insured" on their liability insurance policies. If so, is there an extra charge for this?
- Your insurance advisor does not object to any of the policy "Exclusions."

These criteria are important in determining whether a security contractor's insurance coverage is sufficient to meet your needs. A security contractor must both provide security and be properly insured.

Reputation

A security contractor's reputation should be examined to insure the company has maintained a trustworthy and dependable reputation. To determine the quality of past work, ascertain whether there has been a recent history of valid or successful lawsuits against the contractor filed by clients or employees. This can be learned at your local courthouse. Consider three main factors when researching a company's history:

Negligence

Determining possible history involving negligence by the contractors is important. By reviewing liability insurance claims history, your organization should be provided insurance "Loss Experience" or "Loss Runs" by the contractor upon your request. Your lawyer can explain the report and advise you on the significance of each case and report.

Workers Compensation Claims

Review their listing of worker compensation claims to determine the possibility of patterns of carelessness or inadequate employee safety practices. This report is available from the security contractor and your insurance agent can advise you of the significance of each claim.

Experience

Although not essential, the security contractor should have recently provided similar security service. It is recommended to hire a security contractor that has recent experience similar to the needs of your institution.

Proposal Characteristics

Carefully analyze the proposal submitted by a security agency. The proposal should address the specific security needs at your site and demonstrate that the security contractor has carefully reviewed your needs, giving them full

consideration in the proposal. The following are key points that the security contractor should enumerate in a proposal for your institution:

Training

The proposal should describe the security-related education and training levels of personnel to be assigned at your institution. Security contractors that provide additional education and training are more likely to divulge this information.

Staffing

Staffing may be regular, rotating or temporary and it is important to know beforehand which personnel you will be dealing with. A permanent staff assignment is always best if it can be obtained. However, security contractors often have difficulty maintaining regular staff as a result of odd shifts, frequently consisting of less than eight hours. You should research the security contractor's history of staff stability and determine excessive turnover or poor relationships with employees. The contractor should also obtain your approval before transferring personnel from your site. To this end, the contractor's needs at other sites should not take precedence over security needs at your site.

Description of Supervision

Does the proposal describe the exact nature of supervision to be provided? Contractors should be willing to explain clearly how they will monitor and control the quality of security services.

Documentation

In selecting the best quality contractor, the proposal should describe the frequency of reports and documentation (daily officer activity logs, incident reports, crime reports, officer time sheets, other special reports, etc.). Consistent and thorough written communication is an important output of contract security services and is the only management control mechanism you have over security services and costs.

Instructions to Security Guard

Carefully analyze whether the proposal includes sample Post Orders or Standard Operating Procedures Manual. This document describes all aspects of job performance at your site, including security guard grooming and decorum, sets the standard of security services and provides the basis of guard discipline. Ultimately, this document becomes the main basis of legal defense in the event of litigation. The contractor should provide a document that is comprehensive and clear both to you and the security guards.

Emergency Procedures

The contractor's proposal should describe how his/her guards will function under various emergency conditions. Your contractor's emergency procedures should mesh smoothly with your agency's. The proposal should demonstrate an understanding and coherent approach to a wide variety of non-standard, unusual or crisis situations. Does the contractor have the ability to assist the on-site guard in the event of an emergency?

Equipment Issues

If the security guard is expected to patrol your institution when it is closed (holidays, overnight, etc.), he/she should be equipped with a cellular phone enabling contact with emergency services if needed. It is important for you to ask what other equipment is standard issue and/or the guard is certified to use. For example, will the guard carry a baton? Pepper spray? Handcuffs, etc.?

Extra Services

Determine if there are any special "value added" services proposed. The best contractors proudly propose unusual features of their firm's services such as private investigations, extensive employee background checks, useful liaisons with local law enforcement agencies, new state-of-the-art technology applications and specialized reports.

References

References help find quality and reputable security contractors. Client references give invaluable insight as to the reliability and performance of a security contractor and highlight areas of possible improvement. To secure the most qualified and experienced security firm, the following criteria should be met:

- Clients verify a contractor's history of relevant experience.
- Past clients' references verify a contractor's history of responsiveness.
- References indicate contractor's employee-turnover rate is lower than or equal to that of industry norms.

Costs

Hiring a security contractor is also dependent upon cost. Prospective security contractors should address the following issues:

- How frequently will contractor bill for services rendered? Weekly?

Bi-weekly? Other? Is this convenient for you?

- Will it be a flat monthly rate, a uniform hourly rate for all employees or a unique hourly rate for each individual employee? Generally, paying a unique hourly rate for each guard provides clients with the most economy.
- Contractor discloses wages to be paid to guards assigned to your site. A good contractor should be willing to discuss openly all cost drivers and the fee or profit margins it expects to earn for the services to be provided.
- Contractor's periodic invoices list wages and bill rates for each guard. Invoice detail provides a good audit trail and shows contractor professionalism.
- How will guard pay increases be handled? Inadequate or stagnant wages are a frequent cause of staff turnover. Wage increases should be proposed in advance by the contractor, based on officer incentive and merit, reflected logically in billing rate adjustment and mutually agreed upon by the contractor and client before implementation.
- Will any additional charges be made for uniforms, equipment, supplies, etc.? Again, these should be proposed, justified, logical and mutually agreed upon.
- Is the total estimated average monthly cost within your budget?

As a rule of thumb, your monthly budget can be calculated using the following formula as a guide:

Estimated average hourly wage rate for security guards in your area	\$7
Estimated average monthly hours per security guard	x173
Estimated number of guards at your institution	x2
Estimated cost for security personnel	\$2422
Estimated markup factor	x1.65
Estimated total monthly cost to your institution	\$3996

The monthly costs to depreciate and maintain necessary security equipment such as patrol vehicles and/or radios should also be reflected in the above budget configuration.

Contract

The security contract ensures the contractor will meet your needs. There are numerous questions and criteria that a security contract should specifically address that indicate the security firm is responsible and dependable.

These serve as guidelines to refer to and are enumerated below:

- Does the contractor indemnify you for all security-related liability for which the contractor is responsible? In cases where partial liability is determined by a court of law, does the agreement clearly specify how such indemnifications shall be applied?
- Does the contractor provide sufficient supervision to ensure adequate quality control?
- At contract time will there be a price increase? How much? Why?
- Do you retain the right to terminate the agreement at any time and for any reason? Is this right mutual?
- Is the amount of notice required for contract termination reasonable? Thirty days is the usual standard.
- Does your agency have the right to have a specific contractor's employee removed from your premises?
- Is the agreement sufficiently flexible to meet your needs?
- Does it assure fairness to the contractor and adequate control to the client?

Management

You and the security contractor must share an understanding of the reasons generating the contract. As such, discussion issues should include the following:

- Discuss your desires with management from the outset, allowing the security contractor to communicate with janitors, landscapers and maintenance personnel to create an integrated security team.
- Discuss terms of supervision with the contractor in addition to the contractor supervising your security personnel with both field and management staff. This ensures that the security personnel know, understand and comply with your site's written policy manual. If a security guard performs below par, it is important to know that the individual will be counseled, disciplined and replaced by the contractor as needed.

Once the security guards are in place, you will need to monitor them to ensure that they meet high professional standards, project a professional and alert demeanor, and respond effectively to security-related concerns. It should be required that all that written materials from the security guard

(logs, reports, etc.) be clear, complete and usable.

Deciding What Kind of Security Should Be Hired

It is important to know that hiring a security contractor, whether limited or extensive, armed or unarmed, is a serious business and not to be taken lightly.

Different kinds of security guards are appropriate for different situations. The most important issue is whether you would like security at your site to be provided by a uniformed or plainclothes guard. Depending upon your security goals, hire a contractor who will provide service that fits your needs.

- The main goal of a uniformed security guard is deterrence.
- The main goal for hiring a plainclothes security guard is apprehension.

After deciding what kind of security to hire, you must determine whether the security guard should be armed or unarmed. There are many costs and benefits to be considered when choosing an armed versus unarmed security guard. The following should clarify in what manner security should be provided:

Armed Security Guards

It is important to determine if hiring armed security guards meets your institution's expectations for security.

- Realize that armed guards may utilize deadly force.
- Determine the training qualifications the security guards have with firearms.
- Determine the contractor's shoot policy and the use of weapons with regard to deadly force
- Keep in mind moral questions when hiring an armed security guard. You should also determine whether the members of your institution will accept an armed guard on the premises. Please note that special care should be taken if your institution serves many young people. Schools should be particularly concerned with the message an armed guard conveys to students, parents and staff.
- Consider the cost effectiveness of an armed guard. They are much more expensive than unarmed security, due to licensing and training requirements.
- Decide whether the presence of a weapon may escalate the possible

use of force and violence that otherwise may not occur.

Unarmed Security Guards

- Use of deadly force is not an issue.
- Unarmed security guards often provide the same deterrent as armed guards without the risk of deadly force.
- The protection afforded by unarmed guards is less expensive and incurs less liability and insurance.

CRITERIA FOR SECURITY CONTRACTOR SELECTION CHECKLIST

When the need for a security firm has been determined on an immediate or long-term basis, a security contractor should be selected. The following checklist has been developed to assist you in this process:

Institution Name	
Security Contractor Name	

	Requested	Received	Accepted
Insurance			
Reputation			
Negligence			
Workers Compensation Claims			
Experience			
Proposal			
References			
Costs			
Contract			
Management			
Security Guards			

EMERGENCY PROCEDURES FOR SABBATH AND RELIGIOUS HOLIDAYS

While it's always a challenge to properly respond to a crisis, your planning can be further complicated by the restrictions connected to Sabbath and Holidays. In general, rabbinical authorities permit any steps directly contributing to lifesaving. However, the specific delineations of lifesaving activities are best left to the appropriate, local rabbinical authorities¹.

As always, if your facility is open on the Sabbath or Religious Holidays then your emergency plan should reflect the contingency that a crisis could occur during those periods. Which activities should be cancelled in the event of an impending storm? How would you contact emergency personnel, even if a client becomes ill? Could you use a bullhorn or walkie-talkie if necessary? Do you have easy access to phones, or have they been locked up for the holiday?

For an example of some of the considerations relating to a hurricane, see <http://www.ou.org/resources/hurricanehalacha.htm>.

¹ Obviously, some streams of Judaism maintain no such restrictions.

HOUSES OF WORSHIP & HIGH HOLIDAYS

More people attend High Holiday services than any other synagogue event. At the same time that congregations around the world are busy planning meaningful services, they are faced with the additional burden of ensuring that congregants are as safe as possible.

In these uncertain times people appreciate security measures rather than resent them. Since some of these measures have *halachic* implications, they should only be implemented after appropriate consultation with your rabbi. The following are recommendations regarding issues that should be considered during your holiday or special event planning process:

Police Liaison

One of the most important components of your security planning is coordination with local police authorities. Notify your local commander or community affairs officer of your schedule of meetings and all religious services (including *selichot* and *tashlich*). Your local commander can best determine what resources should be made available for security, crowd control and traffic control purposes.

Tickets

Many institutions require High Holiday tickets as a matter of course. In the current environment High Holiday tickets can be an important component of a security plan. Institutions should assume that those in possession of legitimate tickets should be admitted to services. How secure is your High Holiday ticket? Do you give blocks of tickets to third parties (e.g., Hillels) for distribution? Could it be counterfeited on easily obtained card stock or on a color copier?

If tickets are to play a role in your security plan, those receiving tickets should be pre-screened. There is an obvious hierarchy to those attending High Holiday services: long-term members, long-term casuals (who regularly attend only on the holidays) and new casuals. Your concerns should be commensurate with the congregant's place on the hierarchy, i.e., you usually worry more about the people you don't know than the people you do know.

New casual attendees require the greatest scrutiny. If someone calls to purchase tickets their identity should be confirmed. Are they in the phone book? Did they pay by check or credit card? Is their name and address printed on their checks? Be suspicious of anyone who insists on paying in cash.

Training

As plans are developed, staff and volunteers should be informed and trained to carry them out. Specific concerns include screening and monitoring congregants, evacuation procedures, etc. Written policies and procedures are the easiest to carry out effectively.

Communication

Use newsletters and flyers to inform your congregants about visible changes in security and any changes in policy, e.g., advising congregants to carry fewer bags, that weapons will not be allowed, etc. Attendees tend to feel reassured if they know that security concerns are being addressed.

Emergency Communication

How will you communicate in case of emergency? Does the staff have walk-talkies or cell phones? Are there “panic buttons” at key locations that signal a central alarm company that there is an emergency?

Vendors

Be prepared to look gift horses in the mouth! Be suspicious of vendors offering prices that are too good to be true. How well do you know your caterer, baker, florist, security or janitorial supplies dealers? Known purveyors are less likely to be abusing their relationship to gain illicit entry to your building. If you are going to make a change be sure to ask for and to check references.

Crowd Control/Access

The general rule is that no person should be admitted to any Jewish facility unidentified and this holds true of synagogues on the High Holidays and during special events. Wherever possible, tickets should be required. Tickets are, simply put, a sign that the holder of the ticket has been previously identified.

Those checking tickets can be assisted by long-term members or staff who can personally identify congregants. Synagogue leaders should discuss whether security concerns outweigh the wish to be welcoming. When security concerns are high, only those specifically identified by ticket or by a known person should be admitted to your services. Develop a policy about handling people without tickets. If you don’t want to require tickets, do you have an alternative method of identifying congregants? Should you prepare signs to inform your congregants of any changes in policies? Do you have a way of immediately notifying the police if you need assistance?

Disposable Cameras

It's a good idea to keep a disposable camera handy in case you see something suspicious or if a suspicious person approaches your facility. The mere fact that a picture is being taken could prove to be a deterrent.

Searching People and Bags

Determine your policies ahead of time. Should everyone be searched or should you "profile" those wishing to enter? Should you use metal detectors?

What happens if your searchers find something? E.g., what if someone is carrying a gun or other weapon? As a private institution you have the absolute right to establish criteria for entrance to your facility. If you decide that no one with a weapon, except law enforcement personnel, should be allowed onto your premises you may legally bar anyone with a weapon from entering. You may wish to notify people in a flyer and/or to prominently post such a policy. Note: holding a weapon for someone (even in a locked box) may expose your institution and staff to criminal or legal liability. Your policy should be set in advance, be consistent and be reviewed by legal counsel.

Evacuation Planning

In the event of a threat or an actual emergency it may be necessary to evacuate the building. If a threat is received it should immediately be reported to the police.

Each congregation should have an evacuation plan. The plan should explicitly:

- *Determine lines of authority.* Who makes the determination to evacuate the building? One person must be in charge. How will the decision be communicated?
- *Map out logistics.* If your sanctuary has several exits plan which rows or sections should use each exit—ahead of time. How will you notify each of the services or classes meeting in your building that an evacuation has been ordered? Prepare the evacuation announcements with explicit directions, in writing, and have the appropriate announcement available on the bimah and other convenient locations in case it is necessary to order an evacuation.
- *Have family assembly areas.* Since many synagogues have several, simultaneous services any announcement should include provisions to reunite families. For example, parents should know that they can meet their children at a specific location outside rather than adding to the chaos by trying to find them inside the building.

- *Identify mutual support agreements with neighboring institutions or facilities.* An evacuation could be necessary during inclement weather. By pre-arranging an agreement with a neighboring facility you can instruct your congregants to relocate to a specific site should an emergency occur.

Security Guards

While police departments in the region will give extra attention to synagogues during the holidays (Remember: notify your local police precinct of the times of all services.), it is rare that police will be stationed inside the building. Many synagogues hire extra staff at this time. While anyone in a uniform provides some benefit of deterrence, the most effective guards are those with adequate training and supervision (Note: Some states and provinces require all security guards to be licensed). If you choose to use an outside security company make sure to request and to check references.

Many people ask whether they should hire armed guards. Experts believe that the most important qualification of a guard is his/her training. Putting a weapon in the hands of a poorly trained individual can be more dangerous in an emergency than not having an armed person. Alternatively, many security companies employ off-duty and retired police and corrections officers. Their training is a distinct advantage.

GLOSSARY OF TERMS

This manual uses many terms. The following glossary is courtesy of Claire B. Rubin of Claire B. Rubin & Associates, who maintains <http://www.disaster-central.com>, a web site devoted to providing timely, quality digital resources in the fields of emergency management, risk management, and homeland security. Dr. Rubin credits the sources of her definitions in parentheses.

Accident: A disruption that physically affects a system as a whole. (Pauchant and Mitroff)

Crisis:

1. A crucial turning point in the course of anything, an unstable condition in which an abrupt or decisive change is impending.
2. A major, unpredictable event that has potentially negative results. The event and its aftermath may significantly damage an organization and its employees, products, services, financial condition, and reputation. (Barton)
3. A crisis, like an accident, is a disruption that physically affects a system as a whole and also threatens the priority goals of an organization, and challenges the traditional behaviors and values shared in an organization. (Pauchant and Mitroff)

Disaster:

1. An occurrence inflicting widespread destruction and distress.
2. A situation that is disruptive and harmful; is of high magnitude; is sudden, acute and demands a timely response; and is outside the organization's typical operating framework.
3. Any occurrence which causes damage, ecological disruption, loss of human life, deterioration of health and health services on a scale sufficient to warrant an extraordinary response from outside the affected community. (World Health Organization)
4. An event concentrated in time and space, in which a society, or a relatively self-sufficient subdivision of a society, undergoes severe danger and incurs such losses to its members and physical appurtenances that the social structure is disrupted and the fulfillment of all or some of the essential functions of the society is prevented. (Fritz)

Emergency: An unexpected event, which places life and/or property in danger and requires an immediate response through the use of routine community (or organizational) resources and procedures. (Drabek, *Social Dimensions of Disaster*)

Exposure: To be placed without protection in the area affected by the hazard.

Hazard: An event or physical condition that has the potential to cause fatalities, injuries, property damage, infrastructure damage, agricultural loss, damage to the environment, interruption of business, or other types of harm or loss. (FEMA, 1997) FEMA also defined a hazard as “a source of potential danger or adverse condition.” (FEMA, 2001)

Hazard Profile: A description of the physical characteristics of hazards and a determination of various descriptors, including magnitude, duration, frequency, probability and extent. (These descriptions may be recorded and displayed as maps.) FEMA. 2001.

Homeland Security: A concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.”(*The National Strategy for Homeland Security*, July 2002)

Incident: A disruption of a component, a unit or a subsystem of a larger system. (Pauchant and Mitroff)

Terrorism:

1. Any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments. (*National Strategy for Homeland Security*, 2002)
2. The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (FBI)

Cyber-terrorism: An act perpetrated through computers that results in violence, death, and/or destruction, and creates terror for the purpose of coercing a government to change its policies. (National Infrastructure Protection Center)

Bioterrorism: the overt or covert dispensing of disease pathogens by individuals, groups or governments for the explicit purpose of causing death or disease in humans, animals or plants. Biological terrorism agents include both living microorganisms (bacteria, protozoa, viruses, and fungi) and toxins (chemical) produced by microorganisms, plants or animals.

Vulnerability:

1. Susceptibility to a physical injury or attack.
2. In the context of this manual, vulnerability refers to the susceptibility to hazards. (*American Heritage College Dictionary*, 3rd edition.)
3. Describes how exposed or susceptible to damage an asset is. Vulner-

ability depends on an asset's construction, contents and the economic value of its functions. Like indirect damages, the vulnerability of one element of the community is often related to the vulnerability of another. (FEMA, 2001)

Vulnerability Assessment: The extent of injury and damage that may result from a hazard event of a given intensity in an area. The vulnerability assessment should address impacts of hazard events on existing and future conditions.

Weapon of Mass Destruction: Any weapon or device that is intended, or has the capability to cause death or serious bodily injury to a significant number of people through the release, dissemination or impact of (a) a toxic or poisonous chemical or their precursors; (b) a disease organism; or (c) radiation or radioactivity. (50 U.S.C. 2302)

Risk Assessment:

1. The exposure to the chance of loss
2. The assessment of the severity and probability of a loss.
3. The combination of the probability of an event occurring and the significance of the consequence (impact) of the event occurring. [Risk = Probability x Impact]

Vulnerability Analysis: The determination of the possible hazards that may cause harm.

Risk Analysis: The determination of the likelihood of an event occurring (its probability) and the consequences of its occurrence (its impact) for the purpose of comparing possible risks and making risk management decisions.

Risk Assessment: The combination of vulnerability analysis and risk analysis. The determination and presentation (usually in quantitative form) of potential hazards, the likelihood and the extent of harm that may result from such hazards.

Risk Management: The process of intervening to reduce risk, the making of public and private decisions regarding protective policies and actions that reduce the threat to life, property, and the environment posed by hazards.

Risk Communication: The exchange of information, concerns, perceptions, and preferences within an organization—and/or between an organization and its external environment—tying together the functions of risk assessment and risk management.

Business Area Impact Analysis: A systematic method of determining the cost of risk by identifying the impact of business or service disruptions which allows targeting operations and processes require recovery planning. (Moore, *Disaster Resource Guide: How to Plan for Enterprise-Wide Business and Service Continuity*)

Stakeholders: An individual, group or organization impacted by the decisions and actions of an organization. Stakeholders provide input to vulnerability/risk assessment, risk management decisions and business area impact analysis.

Catastrophe: An event in which a society incurs, or is threatened to incur, such losses to persons and or/property that the entire society is affected and extraordinary resources and skills are required, some of which must come from other nations. (Drabek)

Emergency Management

Emergency Management consists of the expert systems that manage people and resources in order to address major disasters.

Four Phases of Comprehensive Emergency Management (as used by FEMA):

Mitigation: Activities aimed at eliminating or reducing the occurrence of a disaster and reducing the effects of unavoidable disasters.

Preparedness: Activities taken to help save lives and minimize damage by preparing people to respond appropriately when an emergency is imminent. Preparedness includes planning to respond when an emergency or disaster occurs and working to increase resources available to respond effectively.

Response: Activities occurring during or immediately following a disaster designed to provide emergency assistance to the victims of the event, reduce the likelihood of secondary damage and to expedite recovery operations.

Recovery: Activities taken to return systems to normal or better condition. Short-term recovery returns vital life support systems to minimum operating standards. Long-term recovery may go on for years until the entire disaster area is completely redeveloped either as it was in the past, or for entirely new purposes that are less disaster-prone.

Contingency Planning: Planning for an organization's reaction to incidents or emergencies to ensure the protection of life, safety, health, and the environment, to limit and contain damage to facilities and equipment, to stabilize operational service and public image impacts of an event, and to manage communications about the event. Plans include:

Emergency Planning: Disaster and Crisis Response Systems for Jewish Organizations

- Emergency response plan
- Incident management plan
- Crisis communications plan, and
- Crisis management team plan.

Prevention: The positioning of those measures and activities that will lessen the possibility or the impact of an adverse incident occurring in an organization. The primary goals and objectives of prevention are to protect an organization's assets and to manage risk. (Moore) Prevention is a term commonly used in the context of private sector crisis management and is analogous to the term mitigation used in the public sector emergency management context.

Response: The reaction to an incident or emergency to assess the damage or impact and to ascertain the level of containment and control activity required. In addition to addressing matters of life safety, response also addresses the policies, procedures and actions to be followed in the event of an emergency. (Moore)

Resumption: The process of planning for and/or implementing the resumption of mission-critical business operations immediately following an interruption or disaster.

Recovery: The process of planning for and/or implementing expanded operations to address the less time-sensitive, post-disaster business operations. (Moore)

Restoration: The process of planning for and/or implementing procedures for the repair or relocation of the primary site and its contents, and for the restoration of normal operations at the primary site. (Moore)

Expanded to include consideration and implementation of necessary changes designed to improve preparedness for and mitigate the impact of future emergencies.

Continuity: The processes and procedures employed to ensure the timely and orderly resumption of a company's business cycle. (Includes all of the processes/plans/actions contained in the above definitions from risk assessment through restoration).

AUTHORS

Marcia R. Eisenberg

Since 1986, Marcia Eisenberg has served as the Director of the Jewish Legal Assistance Program (JLAP) and General Counsel to the Jewish Community Relations Council of New York (JCRC). She is a 1972 graduate of Barnard College and a 1978 graduate of Columbia University School of Law. Ms. Eisenberg has spent most of her legal career specializing in New York nonprofit and religious corporation law. Before coming to JCRC she served as the founding executive director of the Nonprofit Coordinating Committee of New York.

JLAP annually provides hundreds of Jewish communal and religious organizations with legal advice and services either directly or through the assistance of pro bono attorneys. Services provided by JLAP include: acting as a house counsel to many organizations, involvement in major lawsuits and the promotion of formal and informal legal education for lay and legal audiences. In addition, Ms. Eisenberg is a national resource for Jewish organizations on legal strategies to combat Hebrew-Christian missionaries. She is an expert in New York City real property and water exemptions as well as the Jewish community's liaison to New York governmental agencies charged with protecting Jewish communal assets.

Timothy J. Flannery

Timothy J. Flannery owns a consulting business that concentrates on fire safety training for municipal and industrial organizations. He has over twenty-seven years of experience in the fire protection field. He has been an adjunct professor at John Jay College of Criminal Justice for over six years. He is also the Online Course Coordinator for the Fire Science Division at John Jay. His experience includes fifteen years at a municipal fire department in northern New Jersey, seven years as a fire-training instructor and supervisor at a northern New Jersey fire training academy, three years as director of a county fire academy located in central New Jersey and as a member of the consulting faculty at Thomas Edison State College in New Jersey. Mr. Flannery has done extensive teaching throughout New Jersey for the New Jersey Division of Fire Safety and holds certifications as fire instructor and fire inspector in New Jersey.

He has authored various articles on fire training and safety for several nationally published fire service related magazines. He has been involved in

the development and implementation of fire safety training standards in New Jersey as a member of the New Jersey State Fire Commission's Training and Education Advisory Council.

Mr. Flannery holds a Master of Science degree in Protection Management from John Jay College of Criminal Justice/CUNY and a Bachelor of Science degree in Fire Service Administration from Empire State College/SUNY.

Jeannine Goff

Jeannine Goff recently earned a Master's degree in Criminal Justice at John Jay College. She also holds a Master's degree in Psychology from New York University, and a B.A. in Psychology from the University of Pennsylvania.

Jeannine worked for fifteen years in marketing, primarily in the entertainment and online industries. Deciding it was time for a career change, she enrolled at John Jay College of Criminal Justice and gained experience in the fields of criminal justice and security by working in a variety of positions at the College with John Jay faculty members. At the Criminal Justice Center, she participated in a large-scale study of the Delaware State Police department, evaluating racial and gender issues and measuring job satisfaction with the work environment and the promotion process. She helped produce the *Urban Hazards Forum*, a catastrophic events management conference jointly sponsored by FEMA and John Jay. Jeannine also worked at John Jay College's new Center on Terrorism and Public Safety on a variety of projects.

Norman Groner

Norman Groner recently joined the faculty at John Jay College's Department of Protection Management as an Associate Professor. He has worked in the human factors field for 25 years, much of it in the area of cognitive factors related to fire safety and emergency planning. After earning master's and doctoral degrees in general psychology from the University of Washington, he worked for the National Bureau of Standards where he developed a method for calculating the difficulty of evacuating board and care facilities, later included as an optional method in the NFPA Life Safety Code for establishing required levels of fire safety requirements.

Among other activities, Dr. Groner has investigated human behavior during fires, conducted post-earthquake studies of organizational responses, analyzed the feasibility of using building refuge areas and fire safe elevator technologies, and worked on various code writing committees and task

forces. Most recently, Dr. Groner has coordinated the World Trade Center Evacuation Study Initiative, an *ad hoc* group of researchers, practitioners and advocates who came together out of concern over the repeated failures to improve our knowledge of building evacuation as a crucial, emergency mitigation measure. Dr. Groner's current research interests center on extending human-factors methodologies to better support people during the chaotic events that characterize building emergencies.

Dr. Groner developed much of the rationale for this manual and helped to make it as "user-friendly as possible.

Lawrence Kobilinsky

Dr. Lawrence Kobilinsky has been at John Jay College since September 1975 when he joined the interdisciplinary forensic science department as its forensic biologist. He received his B.S. and M.A. degrees from City College of City University of New York in 1969 and 1971 respectively and his Ph.D. degree from the City University of New York at the Mt. Sinai School of Medicine, in the department of Biochemistry. After receiving his doctorate he was a postdoctoral fellow at the Sloan-Kettering Institute in New York City. While there he became a research associate and eventually a visiting investigator.

At John Jay College he is a full Professor and serves as Associate Provost. He is a member of the doctoral faculty in biochemistry at the Graduate Center of the City University of New York. He has served as a consultant to CBS and other network news programs on issues related to forensic science. He also served as an advisor to the U.S. State Department regarding forensic science laboratories in the Ukraine.

He serves on the boards of the New York Microscopical Society as well as the Eastern Analytical Symposium. He is a member of 18 professional organizations.

As an internationally renowned forensic scientist Dr. Kobilinsky has served as advisor to criminalistics laboratories in several countries including Mexico, China and Brazil. He is a Diplomate of the American College of Forensic Examiners and is a Board Certified Forensic Examiner. He has received numerous grants for both research projects and institutional development projects and has received numerous honors including the Federal Law Enforcement Officers "Civilian Award." He has published extensively on the subject of forensic DNA analysis and has made many presentations at regional, national and international meetings.

Robert J. Loudon

Robert J. Loudon, Ph.D. is the Director of the Criminal Justice Center and Security Management Institute at John Jay College of Criminal Justice/CUNY. He teaches as an adjunct faculty member in the sociology department, the department of law, police science and criminal justice administration and the graduate program of the department of public management. He has lectured throughout the U. S. and internationally before groups in Canada, Russia and Ireland and at the International Law Enforcement Academy in Budapest, Hungary. Dr. Loudon accepted his position at John Jay in 1987 upon his retirement as a Detective Lieutenant in the New York City Police Department.

During his twenty-one-year police career he was involved in a variety of patrol, administrative, training and investigative activities. In 1981 he assumed the role of Commanding Officer, Hostage Negotiating Team and Chief Hostage Negotiator. He was also a supervisor in the Kidnap Task Force. He was designated Commander of Detective Squad in 1983. He is a member of the Honor Legion of the New York City Police Department as well as the Honor Legion of the Police Departments of the State of New Jersey.

In 1993 he was appointed by the US Department of Justice and the US Department of the Treasury, along with nine other international experts, to provide recommendations on how federal law enforcement should handle complex hostage/barricade situations such as the stand-off that occurred near Waco, Texas, between February 28 and April 19, 1993.

Dr. Loudon earned a bachelor of business administration degree from Baruch College and a master of arts degree in criminal justice from John Jay College of Criminal Justice. He then received a M. Phil and his Ph.D. degrees from the Graduate School and University Center of the City University of New York. Dr. Loudon is the founder of the proverbial village of East Cupcake.

David M. Pollock

DAVID M. POLLOCK is the associate executive director of the Jewish Community Relations Council of New York (JCRC), the central coordinating and resource body for over 60 major Jewish organizations in the metropolitan New York area.

As the director of government relations, Mr. Pollock articulates Jewish communal concerns regarding community relations issues to federal, state

and city officials. He is the liaison for the Jewish community with law enforcement officials and active in the development of intergroup relations strategies for the Jewish community.

At the JCRC, Mr. Pollock has played a key role in the development and operation of programs to stop the theft of Torah scrolls, increase the number of Jewish voters and provide pro bono legal services to Jewish organizations.

Mr. Pollock did his undergraduate work at Columbia University and the Jewish Theological Seminary and his graduate work at Columbia's School of Social Work and School of Business. He has published articles on many subjects of interest to the Jewish community and is co-author (with Seymour Siegel) of *The Jewish Dietary Laws* and has lectured on a variety of topics at several institutions of higher learning, including Harvard University, Catholic University, Columbia University, and New York University.

Mr. Pollock is the principal author and project manager of this manual.