11

Contingency Planning Emergency Response and Safety

OBJECTIVES

The study of this chapter will enable you to:

1. Discuss the role of contingency planning in emergency response, crisis management (also commonly referred to as Incident Management which will be used interchangeable throughout this chapter) and business recovery and resumption.
2. Discuss why safety is an aspect of many security programs.

Introduction

No facility protection program is complete without clear, well-defined policies, and programs confronting the possible threat of fire or any other natural or human-made disaster. While planning for such contingencies is the responsibility of top management, in most situations the task of carrying out emergency response falls specifically on the security management team; specifically those resources dedicated to incident management response now considered boutique specialty in many multinational companies. This is primarily due to the essence of the security mission—that is, to observe and report. In the best of all possible worlds the responsibility is a shared responsibility among security, fire, and safety departments. Regardless of the functional placement of responsibility, security, fire, and safety personnel must work together when they are confronted with preparing for and responding to disasters.

According to a 2006 IOMA Safety & Security Reports briefing, 39% of US companies lack a basic crisis plan and 56% have not conducted crisis drills or simulation in the last year. Follow up research in 2017 reveals not much has changed regarding general readiness for many companies. In fact, some companies consider crisis planning and drill exercise a bit of a nuisance and do so at their own peril. Under an amendment to a 9/11 bill passed by the House, the Department of Homeland Security and the American National Standards Institute established a set of "best practices" for disaster preparedness. This includes a certification process to verify compliance [1].

According to Dr. Dennis F. Sigwart, Emeritus Professor, Western Illinois University, current and future security professionals should be aware of the absolute necessity of disaster planning and preparedness as a viable component of the many facets (fire, earthquake, explosions, flooding, and so forth) of which they will have to perform as a practitioner. Those assigned disaster preparedness tasks must continually play the "what happens if"

Introduction to Security. DOI: https://doi.org/10.1016/B978-0-12-805310-2.00011-1

game [2]. Said another way, drill scenario and testing is akin to being a player on a practice field. Practice often makes perfect, builds confidence and comradery among players and streamlines the incident management response process. Drill scenario testing on a frequent basis cannot be overemphasized enough. Firesafety (discussed in Chapter 12, Fire Prevention and Protection), and emergency (contingency) planning is designed to anticipate what might happen to endanger people, physical assets, and information (thus causing damage and interruption to normal business) and to take the necessary preventive measures and make provision—through the use of appropriate hardware and/or personnel response—for prompt and effective action when an emergency does occur. While the emphasis in this chapter (as in most actual practice) is on physical safeguards, it is important to emphasize the human aspect. Disastrous losses often occur not from the failure or absence of physical safeguards, but from human error—the failure to close a fire door, to maintain existing protection systems in good working condition, to inspect or to report hazards, and, at the management level, to ensure through continuous employee education and training that the organization remains prepared at any time for any emergency. The Occupational Safety and Health Administration (OSHA), National Fire Protection Association (NFPA), and Life Safety Codes dictate certain safety requirements for all businesses.

Contingency Planning

The Association of Contingency Planners (ACP), which is an association dedicated to the evolution of business continuity, describes contingency planning in the following way: “Business continuity planning integrates knowledge from related disciplines such as information technology, emergency response, and crisis communications to create a strategy that ensures a business will remain resilient in the face of adversity.” [3]

The purpose of contingency planning is simple. Essentially, contingency planners work to prepare their business, organization, or institution to be better able to mitigate any disruption to normal business activities. As an example, if a natural occurrence (e.g., hurricane, fire, or earthquake) disrupts normal business activities, having plans in place for responding to and recovering from such an occurrence will allow for a faster resumption of business, thus reducing the amount of time the business is disrupted.

For our purposes, we will discuss contingency planning in the construct of four major components: emergency response, crisis management, business recovery, and business resumption. The fundamental elements of each component and the need for an effective integrated contingency planning process will be addressed. Furthermore, categories and types of crises, along with basic preparation and awareness needs, will be discussed. You will note that emergency response, crisis management, business recovery, and business resumption processes have much in common (e.g., communications requirements); however, each is handled as a standalone process.

Security and the Contingency Planning Process

The traditional role of security in the contingency planning process has been to develop emergency evacuation plans for the business and to respond to emergency or crisis situations. Acting as the eyes and ears for an organization, business, or facility and maintaining a 24 hours a day, 7 days a week presence, the security organization is best positioned to respond to an emergency and manage a crisis through the concept of C3: command, communication, and control. As crises escalate, they are best managed by a multidisciplined team.

Due to the ever-ready posture of many security organizations and the increased emphasis on emergency preparedness and contingency planning following the tragic events of September 11, 2001, in New York City, Arlington County Virginia, and Pennsylvania, many security departments have expanded their contingency planning capabilities to include the following components: emergency response, crisis management, business recovery, and business resumption.

Depending upon the scope of the effort, a contingency planning program can take into consideration many activities, events, conditions, and processes. Depending upon the size and complexity of a business the process of contingency planning can be quite extensive. Planning for a contingency generally means assessing and understanding all aspects of the business, particularly the business critical processes and supporting information systems. To do this effectively requires the participation of many people from different disciplines, including management, employees, suppliers, and sometimes even customers. It may also include representatives from external organizations such as representatives of an insurance underwriter or the local fire departments.

Having a variety of knowledgeable people involved from different functional disciplines calls for establishing common parameters. To be effective, everyone involved must have a common understanding of the elements and objectives of the contingency planning program and all must have a common understanding of the process. The first consideration in establishing common parameters is to develop a set of common definitions of terms. When discussing any aspect of contingency planning it is essential that all parties have a common understanding of what is being discussed. Just what does someone mean when he or she refers to the incident management, business recovery, or any other elements of the contingency planning process?

Below are a set of contingency planning terms defined in such a way as to be useful for any organization in establishing a common baseline, points of reference, and common jargon for the end to end contingency planning process. Definition of terms must be part of the organization's formal or institutionalized contingency planning process to ensure continuity of planning and success in achieving common preparedness objectives.

- *Business continuity*: Minimizing business interruption or disruption caused by different contingencies—that is, keeping the business up and running efficiently. Business continuity plans encompass actions related to how an organization prepares for, manages, recovers, and ultimately resumes business after a disruption.

- *Business recovery*: Refers to the short-term (less than 60 days) restoration activities that return the business to a minimum acceptable level of operation or production following a work disruption. Commonly used interchangeably with the term *disaster recovery*.
- *Business resumption*: The long-term (more than 60 days) process of restoration activities after an emergency or disaster that return the organization to its preincident condition. (Keep in mind that restoration to the exact preincident condition may not be necessary or even desirable. However, making this determination may not be possible without proper planning or going through the actual resumption process.)
- *Contingency*: An event that is possible but uncertain in terms of its occurrence or that is likely to happen as an adjunct to other events. Contingencies interrupt normal business activities. In some cases the disruption is minor, while in other situations the disruption can be catastrophic.
- *Contingency planning*: The process of planning for response, recovery and resumption activities for the infrastructure, critical processes, and other elements of an organization based upon encountering different contingencies.
- *Crisis and incident management*: The process of managing events of a crisis to a condition of stability and ultimate recovery. This is proactively accomplished by local, regional, corporate, and executive incident management response teams working hand in hand to successfully manage the incident. The “step up” or “step down” process is a key element of the incident response process. Let us take, for example, local flooding in a foreign country where the infrastructure cannot handle large amounts of rain from a typhoon. When conditions deteriorate “locally,” one would “step up”, and C3 the incident from the “regional” level. However, this does not preclude the local, regional, corporate, and executive incident management teams from activing simultaneously.
- *Critical processes*: Activities performed by functions, departments, or elements within a business or organization that, if significantly disrupted due to an incident, emergency, or disaster, would have an adverse impact on organizational operations, revenue generation ability, production, and/or distribution schedules, contractual commitments, or legal obligations.
- *Emergency response*: The act of reporting and responding to any emergency or major disruption of the business organization’s operations.
- *The Situation Watch Protocol*: Chasing not pacing the world of incidents is not an optimal strategy for a company. Hence the birth of the Situation Watch protocol. This protocol demands that incidents are proactively monitored and communicated to key business partners when there is a potential-tangential or direct impact on a company that may need to be incident managed. In fact, most incidents are predictable. For example, if a company is housed within the pacific ring of fire it is easy to understand that there will be earthquakes followed by a potential tsunami. Take, for example, Superstorm Sandy in 2012 which caused severe flooding along the eastern seaboard of the United States. It first began as a tropical wave in the Caribbean then formed into a tropical storm easily

monitored and easily communicated. That in a nutshell is the Situation Watch protocol in action. More specifically, proactively monitoring and communicating a potential incident from its inception. In this case, monitoring, tracking, communicating, and then proactively responding to Superstorm Sandy before it is at a Company's door step.

Contingency Planning Program

The purpose for contingency planning is to better enable a business or organization to mitigate disruption to the enterprise. Should disruptions occur, and they do all too often, the enterprise must be able to resume normal business activities as quickly as possible. The inability to restore normal operations will have an adverse economic impact on the enterprise. The extent of the impact will correspond to the extent of the disruption or damage. If the damage is severe and the mitigation of such damage has not been properly planned for, the effect could be catastrophic, even to the extent of failure of the business.

Essentially, contingencies fall into three categories:

1. Those that impact the business infrastructure (fire, severe weather, and earthquakes: see the definition of hazards further in this section) causing physical damage.
2. Those that impact people, such as accidents, seasonal illnesses (influenza), epidemics, or pandemics causing harm to employees, rendering them unavailable to work.
3. Those that impact the reputation of the business (such as a product defect leading to a recall), causing resources to be diverted from normal operations to recovery and/or restoration. Each contingency has the potential to disrupt normal business operations to some degree. A minor building fire may disrupt operations in a limited way for only a couple of days, whereas a major fire may destroy an entire factory, completely stopping operations for an extended period.

Contingency planning is a continuous process. It is not something that can be done once and put away only to be retrieved when needed. It is a continuous process requiring periodic updates and revisions as appropriate to, and consistent with, changing business conditions. It also involves implementing and maintaining awareness and training elements. Those personnel with contingency planning responsibilities require periodic familiarization with plans and processes and training on new techniques and methods. The process of contingency planning should be designed to achieve the following:

- Secure and protect people. In the event of a crisis, people must be protected (employees, visitors, customers, and suppliers).
- Secure the continuity of the core elements of the business (the infrastructure and critical processes) and minimize disruptions to the business.
- Secure and protect all information systems that include or affect supplier connections and customer relationships.

Throughout the remaining sections of this chapter, elements of the contingency planning process and program (Fig. 11.1) are presented and explained.

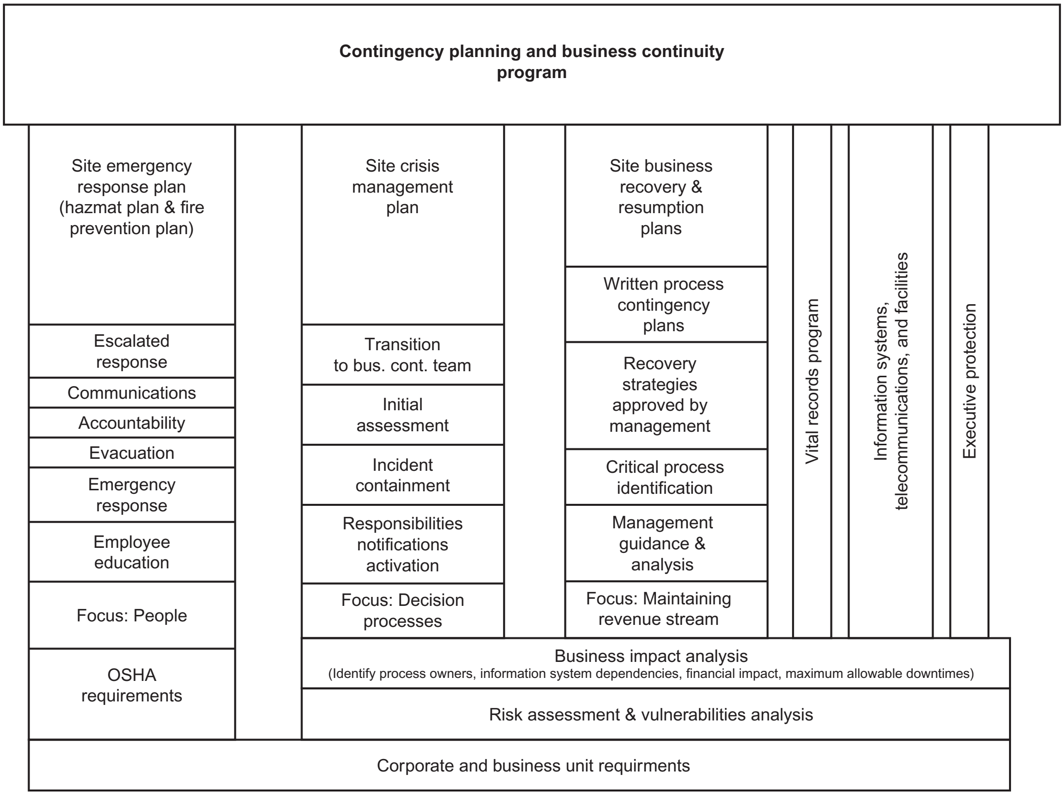
Contingency planning and business continuity program
Site emergency response plan (hazmat plan & fire prevention plan)
Escalated response
Communications
Accountability
Evacuation
Emergency response
Employee education
Focus: People
OSHA requirements
Site crisis management plan
Transition to bus. cont. team
Initial assessment
Incident containment
Responsibilities notifications activation
Focus: Decision processes
Site business recovery & resumption plans
Written process contingency plans
Recovery strategies approved by management
Critical process identification
Management guidance & analysis
Focus: Maintaining revenue stream
Vital records program
Information systems, telecommunications, and facilities
Executive protection
Business impact analysis
(Identify process owners, information system dependencies, financial impact, maximum allowable downtimes)
Risk assessment & vulnerabilities analysis
Corporate and business unit requirments

FIGURE 11.1 Elements of a business continuity planning program.

Contingency Plans

Contingency plans formally establish the processes and procedures to protect employees, core business elements, critical processes, information systems and the environment in the event of an emergency, business disruption, or disaster. These plans should be developed and designed to consider specific categories and types of emergencies and disasters and address the mitigation, preparedness, and response actions to be taken by employees, management, and the organizations charged with specific response and recovery tasks. These plans should contain basic guidance, direction, responsibilities, and administrative information and must include the following elements:

- *Assumptions*: Basic assumptions need to be developed in order to establish contingency planning ground rules. As a baseline for planning, it is best to use several possible “worst-case” scenarios relative to time of event, type of event, available resources, building/ facility occupancy, evacuation of personnel, personnel stranded on site, and environmental factors such as weather conditions and temperature. Furthermore, consideration should be given to establishing response parameters for emergency events. Define (for your enterprise) what constitutes a minor emergency, a major emergency, and a disaster.

- *Risk assessment and vulnerability analysis*: Identify known and apparent vulnerabilities and risks associated with the type of business and geographic location of the enterprise. An assessment of risk and vulnerabilities should be made prior to developing or upgrading contingency plans. All planning will be accomplished in accordance with a thorough understanding of actual and potential risks and vulnerabilities. For example, in a petroleum refining facility, contingency plans for petroleum spillage, contamination, and fires must be considered. Furthermore, if located in an earthquake zone, planning must address associated hazards. The risk assessment and vulnerability analysis must also include an assessment of enterprise—critical relationships. That means involving suppliers and customers in the contingency planning process. If a critical supplier or many key suppliers are not also prepared for various potential contingencies, their inability to recover will adversely impact your enterprise.
- *Types of hazards*: Planning for each and every type of hazard is not practical, nor desirable. Grouping them into similar or like categories will allow for planning to address categories of hazards which can easily be categorized as natural occurrences, health/pandemic, infrastructure, and social, civil or political disruption. Since many hazards have similar consequences and result in like damages, it is best to plan for them in categories. The following is a list of common hazards: Medical Emergencies; Fires; Bomb Threats; High Winds; Power Interruptions; Floods; Hurricanes; Snow/Ice Storms/Blizzards; Hazardous Materials Issues; Aircraft Crashes; Civil Disorders; Earthquakes; Terrorist Threats/Activities; Workplace Violence; Explosions; and Tornados.
- *Critical process identification*: Critical processes must be ranked in accordance of criticality and importance to the productivity and survivability of the enterprise. Process of recovery must be focused on those critical processes that, when resumed, will restore operations to a minimal acceptable level. In essence, these processes are identified to be the first processes restored in the event of a major interruption to business operations. Failure to restore them presents the greatest possibility of damage or loss to the enterprise and could lead to the loss of a competitive edge, market share, or even the viability of the enterprise.
- *Business impact analysis*: A business impact analysis must be accomplished to accurately determine the financial and operational impact that could result from an interruption of enterprise operations. Moreover, all critical interdependencies, those processes or activities critical processes are dependent upon, must be assessed to determine the extent to which they must be part of the contingency planning process.
- *Emergency response*: All participants in the emergency response process, particularly emergency responders, must understand their role. Expectations and responsibilities of emergency response personnel must be well defined and documented. Guidance for all employees on how to react in the event of an emergency and what their individual and

collective responsibilities are must be documented and shared. Organizational responsibilities must also be established, to include the development of department-level emergency plans, generally for mid-size and large organizations. Events such as building evacuation and roll-call assembly need to be well defined so, in the event of an actual emergency, there is no confusion or uncertainty as to what must be accomplished.

- *Incident management or crisis management*: As an incident escalates, a crisis management team (CMT) should assume responsibility for managing the crisis. If the crisis is international or global in nature, it is important that the incident response process is fluid to address it. For example, activing a local or regional team and stepping up or stepping down as necessary as was discussed in a prior section of this chapter. How this process works and who has what responsibilities must be clearly stated in the contingency plans. In the event of an actual emergency, some unqualified people will attempt to manage the incident or participate in crisis management; however, they should not have any role in this process unless they were previously identified and trained as part of the CMT. Without established and well-defined incident management protocols and procedures, confusion is likely to erupt. It must be clear at all times who is the designated incident commander and his or her back up if necessary with C3 for the incident. Essentially, incident management, and crisis management personnel must be trained and must understand their responsibilities including decision-making authority in the teeth of a crisis real time. Without this authority, the timely response to an incident gets booged down in the bureaucratic quagmire which could jeopardize employee safety and well-being. Lastly and where here practical, back-up supporting personnel should be identified and trained in the event that primary personnel are not available.
- *Incident/event analysis*: After an event occurs and the situation is stable, an analysis of what occurred and why should be conducted to determine the immediate extent of damage and the potential for subsequent additional damage.
- *Business resumption planning*: The process of planning to facilitate recovery of designated critical processes and the resumption of business in the event of an interruption to the business should be performed in two parts. The first part focuses on business recovery in the short term while the other part focuses on business restoration in the long term. This process will also include establishment of priorities for restoration of critical processes, infrastructure, and information systems.
- *Post-event evaluation*: An assessment of preceding events to determine what went well, what did not go so well, and what improvements to existing plans need to be made must also be part of the process. Learning from real events is an unfortunate opportunity. There is no better way to learn how to handle an emergency than to actually handle one. The evaluation or after action report should always be documented to serve as an organization's memory of the event in order to proactively address improvements in the incident response process.

Emergency Response

When an emergency occurs, and unfortunately emergencies occur at even the most prepared businesses, being able to effectively respond is critical. *Respond* in this context means to call up the necessary incident response team regardless of the time of day or weekend and even holiday. As such accessibility of responding incident management team decision makers are paramount. The type and nature of emergencies that can occur vary widely. From a medical emergency in which an employee becomes injured or sick, to a natural or person-made disaster causing extensive damage to buildings and equipment, being prepared to respond will usually lessen the damage or impact of the event. Preparedness takes many forms. Being prepared to respond to a medical emergency is different from being prepared to respond to a natural disaster. The medical emergency may only require applying first aid to a victim or it may require the assistance and services of medical professionals. A natural disaster may require support from emergency medical services along with law enforcement, fire departments, search and rescue operations, and hazardous material crews.

When planning for emergencies, types of emergencies should be grouped into like categories so that planning is accomplished for only categories of emergencies, as opposed to each and every possible emergency occurrence. This strategy recognizes the similarities of different types of emergencies and is efficient in terms of creating fewer and flexible plans.

The purpose of preparing an emergency response plan is to document the planning accomplished in preparation for an emergency. This documentation provides the ground rules for emergency response activities. It also provides a reference for all who need to know how the process works. The plan will identify general and specific responsibilities for emergency response personnel and for all employees, both management and nonmanagement. Having a plan in place will assist emergency response personnel in their effort to return the business to normal operations. However, it is important to remember that the plan should be easily accessible, streamlined, and ready for action. A plan too burdensome in the number of pages and instructions will only serve to hamper the incident management response process.

- *Reporting emergencies*: Employees must know how, and to whom, emergencies should be reported. If handling an emergency is beyond the internal capability of an organization, additional external assistance can be sought. For example, a seriously ill employee may require immediate medical attention. If paramedic capabilities exist within the company then the in-house paramedic should be the first respondent. If the situation calls for more sophisticated expertise and capabilities, external emergency medical services can be called for.
- *Communications and warning systems during an emergency*:
  - *Fire alarm systems*: These systems are generally the most widely used. Linked to a variety of sensor detectors and manual pull stations, fire alarms do just that: sound an alarm. These systems are sufficiently unique in sound and volume as to clearly

indicate the need for building and facility evacuation. Employees must be conditioned to respond immediately.

- *Public address systems*: These systems can be used to augment the fire alarm system. Announcements can be made alerting employees to the danger of fire. Announcements alerting employees to other types of dangers can also be made. Public address systems are particularly useful during emergencies when a building or facility evacuation is just the opposite of what is needed. For example, in the event of a chemical discharge or other environmental hazard, it may be necessary to keep people inside the facility and shut down all air movement systems, thus preventing employees from exposure to hazardous airborne substances. Since employees are conditioned to evacuate a building or facility when a fire alarm is sounded, they can be conditioned to wait and listen for specific instructions provided over a public address system. New to the market in 2017 are Internet Protocol (IP)-based public address systems. Public not in the traditional sense but rather internet sense in that the address protocol works integrally with your desk phone and smartphone and will "chase you down" by communicating to multiple devices.
- *Emergency Response Team (ERT) Leads*: The use of employees to augment the emergency notification system has much value. Specially selected and trained employees can be given responsibility to act during an emergency to spread the word to evacuate a building or facility during an emergency. Assigning each a specific area of responsibility, the ERT Leads ensures complete coverage of the building or facility. Communications between floor ERT Leads and emergency response personnel or a security emergency operations center can be easily established. ERT Leads can be alerted by IP technology solutions radio, smartphone, or other means in the event of an emergency and be instructed to react to the specific situation. ERT Leads can and should be empowered and trained to react on their own in the event they recognize danger. Authority should be provided to ERT Leads to evacuate a building or facility based upon their judgment and assessment of an emergency situation. In the event of a complete communications failure, it may be necessary to empower them to dispatch people to a safe environment.
- *Response to emergencies:* Since security officers are located throughout the facility and operate on different shifts, they are usually the first to respond as often times they are the eyes and ears to an event unfolding or one that just occurred. Being on the front lines, the security officer can assess the situation and make a determination if additional assistance is necessary. In some cases, they may not be able to make an assessment and may require support from others. For example, in the event of a hazardous chemical spill, it will be necessary to have an expert in environmental and safety issues on the scene to make the assessment. It may even be necessary for a hazardous materials (HAZMAT) crew to respond to handle the event. Clean up of a chemical spill should only be done by skilled and certified personnel. Another example may be the unfortunate death of an employee in the workplace. This will require the security officer to make immediate notification to OSHA as well as

cordoning off the scene and directing law enforcement to the scene. In rare cases, it may require the preservation of evidence and stand by for the corner to clear to the body. Clearly, defining who has what response capabilities and responsibilities will impact the effectiveness of any response. Without a doubt, capable and training security officers are a key ingredient to the efficient handling of the incident management response process.

- *Department-specific emergency plans*: It is best to have one emergency response plan for each company facility. These plans should be incorporated into a master plan and provide a common framework. A key subelement of an emergency plan is the individual departments' emergency plans. Those plans must specifically identify the following information:
  - Common and unique responsibilities in the event of an emergency to include:
    - A roster of department employees
    - Emergency contact/notification roster (not all emergencies occur during working hours so it may be necessary to reach people at home)
  - Identify floor wardens
  - Evacuation routes, procedures, and assembly areas
  - Roll-call instructions
  - Procedures for evacuation of people requiring assistance
  - People identified as members of a search-and-rescue team
  - Additional manager- or employee-specific responsibilities
- *Incident management*: Personnel trained in handling emergencies should manage the incident at the scene. If the incident escalates to a crisis, a company CMT should be convened to manage the crisis. The senior emergency response person, when at the scene, should manage the incident with the assistance of specialists as appropriate.
- *Evacuation and assembly*: A critical objective during any emergency is employee safety. In the event it is necessary to evacuate a building or facility, having an established and orderly process is essential. Once a warning system sounds the notice to evacuate, employees must be aware of preestablished procedures for quick evacuation, including primary and alternate evacuation routes and where they should assemble. Maps or diagrams with this information should be included in the plan and posted throughout the work area. A floor warden or an employee with the assignment to facilitate evacuation should make a sweep of the area prior to their own evacuation to ensure all personnel have exited the building or facility. Once in the predetermined assembly area, a roll call must be taken. Primary, secondary, and tertiary responsibilities should be assigned to ensure someone is available to take roll call and report the results to security. If someone did not evacuate the facility, a search-and-rescue team or other emergency personnel may be required to reenter the facility and provide assistance.
- *Emergency evacuation drills*: The efficient and complete evacuation of personnel from a building or facility in the event of an emergency is such an important event that periodic drills should be conducted to reinforce the process and its importance. At least annually, each building or facility should undergo an evacuation drill where employees respond to

a warning and completely evacuate the building or facility. This may be required by law in some states or jurisdictions. Lastly, a roll call should be conducted and results reported to security and senior management.

- *Search and rescue*: In the event of serious damage such as a fire or collapse of building, it may be necessary to search and account for employees. Search and rescue is the responsibility of responding emergency personnel who have proper protective equipment such as the fire department persons not trained in search-and-rescue techniques or who do not have proper equipment should not enter hazardous areas and conduct searches. Heavy lifting should always be left to the professionals such as properly trained search and rescue teams and fire department personnel. Heavy lifting in this context means security personnel should not supplant the proven experience of responding agencies and do it themselves without the proper training. This can cause critical delays in response and could even jeopardize lives. At its core, the job of the security officer is to observe and report.
- *Return to work*: The process for returning to work after a crisis should also be included in the emergency plan. After any incident where employees are required to leave their work area and evacuate a building or facility, a process for having them return to work is necessary. For example, in the event of a false fire alarm where employees have evacuated a building, a means of communicating to them an all-clear, safe to return to work signal, is needed. This can be accomplished in many ways. Public address announcements can be made or security personnel can go to assembly areas, directing employees to return to work the good old fashion way by use of a bull horn. As appropriate, other methods may also be employed such as IP-based communication systems. In the event there is actual damage and employees cannot return to work, a process should be established identifying who makes the decision to send employees home—most likely Human Resources—as well as how that is communicated to them and how they are kept apprised of event updates. For example, if a building was severely damaged due to fire and cannot be occupied for several days, posting daily direction and guidance for employees on the company website or on an emergency toll-free phone line will allow employees to call each day for specific instructions. For this to be effective, employees must know this process, must know the phone number to call or website to access and, as with all other processes, this one must be updated regularly. Extended remote work authorization can also be of great assistance to a company keeping it operating efficiently while longer term infrastructure needs are addressed. This type of remote work authorization especially works well where natural occurrences most happen such as severe snow storms, hurricanes (when evacuation is not necessary), and typhoons. In some instances, keeping employees at home working remote while there is civil, social, and political unrest can save lives by keeping employees off the roads or away from the office.
- *After action*: When any incident occurs that necessitates evacuation or results in injuries, major damage, or presents the possibility of major business interruption, an after action report must be prepared. The primary focus is twofold:

- Document the events, circumstances, and chronology.
- Prepare a lessons-learned review. Include key personnel involved in responding to and managing the emergency so as to assess what occurred and how it could have been better handled.

Crisis or Incident Management

Emergencies, contingencies, business interruptions, and other unplanned events happen. Sometimes the event itself is a crisis, such as a fire burning a building or facility. In other cases, an incident not responded to or managed properly at the scene may turn into a crisis. For example, failing to respond promptly to that small fire may allow for it to turn into a large fire.

Incident management is the process of managing events of a crisis to a condition of stability. Emergency response personnel at the scene of an incident manage the incident. If the incident escalates, becoming a crisis, it is then necessary to have a different group take charge. Ideally, a CMT, consisting of experienced personnel from multiple disciplines, would come together to manage the incidents that develop beyond the capability and decision authority of emergency response personnel. Essentially, the CMT manages the crisis to closure.

After emergency response planning, crisis management planning is the next step in the continuum of the contingency planning process. A crisis management plan should address the following activities and concerns:

- *Crisis management teams*: Managing a crisis can't be left to emergency personnel only. When an incident escalates into a crisis, the situation becomes more complex, affecting different aspects of the business if not the entire business and requiring different skills to manage it. Employees with a broad understanding of the enterprise and its mission, goals, and objectives are much better suited to manage a crisis than those with a more narrow perspective of the business. Ideally, a CMT is like an integrated process team. Skilled professionals representing different disciplines come together on a short-term basis to work on a specific issue or tasking. In the case of CMTs, the task is to serve as a deliberative body to plan and prepare for a crisis and, when a crisis occurs, manage that crisis so as to mitigate damage or its impact. CMTs should include members with expertise in the following areas: security, human resources, site management, safety and environmental and safety services, business management and communications.
- *Disaster operations*: In the event of a crisis or disaster, it is to be expected that some personnel may not be able to immediately leave the site. For example, following an earthquake the surrounding area may not be safe for travel. Employees may have no choice but to seek shelter at the workplace for hours or days. Furthermore, emergency personnel may be needed on site for an extended period to assist in recovery operations. Being prepared to deal with this or similar scenarios is essential. Preparation will include ensuring sufficient supplies are on hand to meet the needs of a reasonable number of

stranded or support personnel. It is necessary to ensure that sufficient food, water, medical supplies and emergency sanitation, and shelter facilities are available. All of these items can be acquired and placed in a long-term storage condition, providing they are regularly checked for serviceability, spoilage, and maintained within the expected shelf life. During a crisis, much uncertainty exists. Consequently, it will be necessary to communicate to employees, keeping them as up to date as possible about the situation and events and providing guidance concerning their safety and work expectations. During a crisis, employees are naturally anxious. Prompt and clear communications can help reduce this anxiety and keep employees informed. Communication may need to extend beyond the duration of a crisis into an undefined subsequent period. Using the previously referred to emergency contact and notification number, or company Web site, can be very effective. Messages can be updated regularly as needed so the information is current. Also, information broadcast on local news radio stations can reach a large population of employees. At the point in time where an incident escalates into a crisis, the CMTs become involved, managing the crisis to closure. At some point during a crisis, a deescalation of events will occur and eventually the crisis will terminate. If the impact or damage from the crisis is significant, the CMT will commence with restoration activities. These activities may be led by the CMT or passed on to a business continuity team. How this can work will be discussed further in the next section.

- *Media relations*: During a crisis, it is possible that the local, national, or even international media will become interested in events. For example, large industrial fires always draw the attention of local media. Natural disasters also draw much media attention. Even isolated events such as incidents of workplace violence can draw significant media attention. It is therefore important to have a media relations plan. The company media representative should be part of the company CMT. Since there is always a degree of unpredictability during a crisis, it is best that all CMT members understand how to deal with the media and be prepared should they be thrust into such a situation.
- *Damage assessment*: During a crisis, emergency personnel will make ongoing damage assessments, reporting status back to the CMT. These assessments are useful in determining actions to be taken next. However, these assessments are situational and due to the circumstances and nature of a crisis, do not have the luxury of thoroughness. The true extent of damage is not determined until after the crisis has terminated and a complete building, facility or site assessment can be made. Immediately following a crisis, a damage assessment for infrastructure safety and functionality must be made. Without this, a return-to-work decision cannot be made. The damage assessment is also the starting point for all restoration and resumption activities.
- *Business continuity team*: Earlier reference was made to the transition of responsibility from a CMT to a business continuity team. This is an important step in the effort to resume business. While the CMT's focus is on managing through the crisis, the business continuity team's focus is recovery and resumption. The role of a business continuity team will be discussed further in the next section.

Business Continuity

Earlier in this chapter, we defined business continuity as the effort to minimize business interruption or disruption caused by different contingencies. When contingencies occur, business recovery and resumption needs to happen as rapidly as possible. In essence, business must continue. Business disruptions can be costly and even catastrophic. Customers, shareholders and stakeholders demand the business remain viable. Preparation to deal with contingencies is a critical component of keeping the business going and maintaining the viability of the enterprise.

Business continuity is a two-stage process. Business recovery is the first stage. Business resumption is the second. The recovery effort is the process of getting the business up and running again but only in a minimal acceptable condition. It is not a recovery to a preevent condition, but rather a recovery to produce product, make deliveries to customers and accomplish the basic activities to keep the business going.

The business resumption stage is the effort to recover from a contingency and resume business in a preevent condition. This is not to say that all critical processes and other processes will be exactly the same as they were preevent. Resumption planning may call for new or modified processes. The intent is to resume business operations to a level similar to the preevent operations level, but not necessarily exactly the same.

A business continuity team should be established to provide oversight of the development of business resumption plans. Representation from each of the major business functions should be part of this team. Manufacturing, business management, finance, engineering, information technology, human resources, legal and others major areas, and disciplines within the business, depending upon the nature of the business, need to participate. Business resumption teams lead the effort and planning process to ensure the business is prepared to recover from contingencies and resume full business operations. In some cases it may be necessary to have a major supplier or customer participate as a member of this team. Business recovery and resumption planning have common elements. The difference is the stage of recovery and the time necessary to get there. Following are common elements of the processes for business recovery and resumption:

- *Business impact analysis of critical processes and information systems*: The most fundamental aspect of recovery and resumption planning is conducting a business impact analysis of critical processes. Critical processes must first be identified. Knowing what they are and having the business continuity team agree to their criticality will allow for proper planning and prioritization. Failure to properly identify critical processes may lead to wasted time, effort, and money. Even worse, noncritical processes may be given priority over critical processes, leading to further delays in recovery and causing the unnecessary expenditure of resources. It is not uncommon for organizations to identify their processes as critical, where upon further examination they are determined not to be critical. Process owners have a tendency to believe all of their processes are critical. This is precisely why it is necessary to have the business continuity team make this assessment. When developing recovery and resumption plans, the following areas must be considered and addressed:

- *Define critical processes*: Each major business area, function and discipline should provide to the business continuity team a listing of all critical processes. The business continuity team should then review these processes for criticality and prioritize them, creating an official critical process list. Planning for recovery of the critical processes is the primary concern. Noncritical processes should be recovered and resumed after the critical processes. Resource and time limitations do not allow for resumption of all processes at the same time. Processes critical to the business must have top priority. Any processes determined not to be critical should be planned for during the later stages of the resumption effort.
- *Critical process interdependencies*: As part of the critical process assessment, particular emphasis must be placed on information systems and process interdependencies. For example, an information system in and of itself may not be determined by its process owner to be critical. However, if it supports a critical process and that critical process can't be completely restored without the information system, then that information system itself becomes critical. Examining processes as part of a system is essential in the assessment of criticality. Interdependencies need to be identified in order to properly assess criticality to the business. Other interdependencies may exist in the form of relationships with organizations outside of the enterprise. These too must be considered. Different methodologies can be used to estimate potential impact a contingency or disaster may have on a critical process. When considering the criticality of a process, the financial effect, operational effect and any less tangible or quantifiable concerns, such as customer satisfaction, must be addressed.
- *Resources*: Critical process recovery requires an assessment of resources. Planning for process restoration means considering what resources may no longer be available and will need to be acquired or obtained to get the critical process up and functional again. What type of facilities will be needed and where? Will additional hardware, software, or equipment be required? Will people capable of managing and working the processes be available? Will there be effective means of communications? If not, what must be done to provide a minimum capability of communications until full communications can be restored? These are some of the resource issues and questions the team must grapple with.
- *Mitigation strategies:* For those processes identified as critical, preevent actions can be taken to help mitigate the impact, both operationally and financially, of interruptions to the business. When developing contingency plans for critical processes, strategies will become apparent that may be implemented prior to an event that will lessen the impact of an event if and when it occurs. A cost/benefit analysis may be required to assess the feasibility of implementing a preevent action and if the analysis shows it to be an effective action, it should be taken. For example, an old building not built to current building codes may be vulnerable to damage from an earthquake. If that building supports a critical process, it may be more cost effective to retrofit the

building with the necessary structural supports and bring it into compliance with current standards than to risk severe damage in the event of an earthquake, rendering a critical process inoperative.

- *Vital records*: The ability to recover vital records is critical to the recovery and restoration process. Having a vital records protection and management program will enable the recovery of essential information during a contingency.
- *Customers and suppliers*: The importance of considering input, participation, and impact to customers and suppliers cannot be overstated. Any business continuity planning must take into consideration customer and supplier relationships. Moreover, it is important to work with your suppliers and providers of goods and services to ensure they too have contingency plans in place. In the event a supplier supports one or more of your critical processes, a disruption to their business will impact your business operations.
- *Communications*: Communicating during the recovery and resumption process can be just as important as communications during other phases of a contingency. Employees who may have been affected by the events of a crisis or disaster need to be kept abreast of developments affecting them and their employment. Customers and suppliers need to understand the progress made toward resumption of business, as it may have a serious impact on their operations. Even the external worlds of stakeholders and shareholders have an interest in these events.
- *Lessons learned*: There is an old adage that lightning doesn't strike twice in the same place. If only that were certain and true, and applicable to the critical processes of a business. However, it is not. Therefore, much can be learned from each phase of managing and recovering from a contingency. Documenting the process of recovery and restoration will help in identifying the things learned, both good and bad, and will go a long way toward helping to deal with other crises when they occur.

Business Recovery

The previous section addressed areas and issues common to resumption and recovery aspects of the total contingency planning process. This section will discuss areas specific to recovery and the short-term process of resuming normal business operations.

Recovery plans focus on getting the business up and running—in essence, the actions that need to be taken within the first 30–60 days to restore critical processes and resume operations. These should be the most critical processes focused on infrastructure, product delivery, and keeping damage or loss to an absolute minimum. As difficult as it may be, people need to be part of this equation. For example, should a natural disaster occur, causing severe damage to a building or facility, there is a good chance that some key employees may have experienced something similar. Some may be preoccupied with their own issues of recovery and restoration and may not be able to support the company. Generally, you can expect this to be limited to a few, but it could be a critical few. Part of the critical process planning should take this into consideration and identify alternatives.

Vital records recovery is very much part of the recovery process. Being able to access off-site records storage, hard copy, and electronic, is critical to expediently moving this process forward. Many companies use outsource providers to handle, store and, retrieve their vital records. This process allows for separate storage, away from company facilities, and reduces the possibility of damage or destruction to these records. There are many capable and reliable companies throughout the world who perform vital records handling, storage, and recovery.

Business Resumption

Issues and areas of focus and concern that are common with recovery and resumption were addressed earlier. This section discusses areas specific to resumption and the long-term process of resuming normal business. Long-term priorities are addressed in business resumption plans with the intention of restoring operations to a preevent condition. Restoration to a preevent condition does not necessarily mean that all is the same or equal to the conditions prior to contingency occurrence, crisis, or disaster. During the process of recovery and restoration it may be learned or discovered that the implementation of a critical process or other processes can be accomplished differently, in the sense that improvements can make the process more efficient and more cost effective. Consequently, changes can and should be made. Furthermore, it may be learned that some processes can be eliminated altogether. Recovery and resumption in many ways are similar to a reengineering process. Process owners are usually the best source for ideas and as they participate in resumption they may develop new approaches and methods to implement and execute their process.

If the process is simple, changes can be implemented quickly with little or no additional review from management or the business continuity team. If the process is complex, affecting, or dependent on other processes, a cost-benefit analysis is warranted to accurately assess the impact of any proposed changes.

Pandemics

Defined, “a pandemic is a global disease outbreak.” (end-note WebMD). This has driven governments and private organizations to take mitigating steps to address the pandemic threat. Pandemic preparedness continues to receive much attention most recently the middle east respiratory syndrome (MERS), the H5N1 Avian Flu and the H1N1 Swine Flu viruses remain active in various parts of the world, with the H5N1 being active mostly in Asia [4]. Pandemics are not new, having been with us since humankind’s earliest time. They don’t occur frequently but when they do, the effects can be devastating. The last devastating pandemic occurred in 1918, when the Spanish flu affected more than 30% of the population, killing between 50 and 100 million people worldwide and disrupting the normal lives of societies around the globe [5].

Planning for a pandemic requires an emphasis on people. The focus is on planning to keep employees, and their families, healthy and in the workplace where they can be productive. Pandemics affect people, not infrastructure, although without people operating an infrastructure is at best difficult, and may be nearly impossible. Consider running the air transportation infrastructure without people. With a 30% reduction in the number of air traffic controllers, pilots and maintenance personnel, would this system work effectively, or would it even work at all? How would your business be affected if air transportation was limited or shut down for operating for 30 days?

The Center for Disease Control and Prevention (CDC) has created a Pandemic Severity Index to assist local and state governments in assessing the severity of a viral outbreak. The level will help officials determine the extent of school closure, quarantines, and work-from-home assignments.

- Category 1 involves less than 90,000 deaths and would not require school closures.
- Category 2 and 3 would recommend school closures and limiting personal contact for up to one month.
- Category 4 or 5 would potentially involve over 1.8 million deaths, school closures of up to 3 months and limits on public events [6].

Summary

Within this chapter, the authors have attempted to provide the reader with a framework for understanding the complexities of contingency planning and the development of contingency plans. A particular point we attempt to make lies with the importance of planning for categories of contingencies. It is a daunting task to attempt to plan for each and every possible contingency. However, contingencies can be grouped into categories and planned for accordingly. This allows for consistency in preparedness and best utilization of resources. Types of contingencies develop and change over time as societies and organizations change and progress. Prior to the 20th century, nuclear contamination was not a concern, but today countries with nuclear power generation capabilities have in place extensive contingency plans that are regularly tested. More common hazards such as severe weather and other natural events have caused enough damage to drive organizations to better preparedness. State and local governments along with private enterprises in states like California and Mississippi spend large sums of money to prepare to mitigate the effects of earthquakes and flooding.

Contingency planning may not have been a traditional security process, but in today's global business environment the security organization is assuming a much greater role and responsibility for its implementation. Even prior to the events of September 11, 2001, many organizations were becoming more conscious of the need to have contingency plans. A complete contingency planning program has three major elements:

1. Emergency response
2. Crisis management
3. Business continuity: business recovery and business resumption

Emergency response activities involve responding to an incident, crisis, or disaster and managing that incident at the scene. Should an incident escalate to the crisis or disaster stage, a CMT should take over managing the crisis to its conclusion. If the crisis or disaster does cause damage to a company building, facility, or operation, the CMT should hand over to a business continuity team the responsibility of recovery and resumption. After a disaster, it is critical that the business recovers and resumes normal (preevent) operations as soon as possible. Customers, shareholders, and stakeholders expect nothing less. Executive management has the obligation to ensure contingency planning is properly considered and addressed within their company. The consequences of not planning for contingencies can be catastrophic, with numerous liability issues

■ ■ Critical Thinking ■

Can a business be successful without having contingency plans?

Review Questions

1. What are the key elements of any contingency plan?
2. What should be the role of security in developing a contingency plan?

References

[1] R. Block, Pushing disaster preparedness the lieberman way, Wall St J Online 02/09/2007 and ANAB Accreditation for Private Sector Preparedness Voluntary Certification. <www.anab.org/accreditation/preparedness.aspx>, (download 6.17.12).

[2] D.F. Sigwart, Disaster planning considerations for the security/safety professional: a historical interface, in: J. Chuvala, R. Fischer (Eds.) (Eds.), Suggested Preparation for Careers in Security/Loss Prevention, Kendall/Hunt, Dubuque, IA, 1999.

[3] <www.acp-international.com/> For contact information mail to: chairman@acp-international.com.

[4] http://www.flu.gov/individualfamily/about/h5n1/#what.

[5] http://en.wikipedia.org/wiki/Spanish_flu.

[6] T. Pugh, Rating system develop to gauge pandemics, Houst Chron. (February 2, 2007) A10.