

Basic Safety & Security Checkpoints For Public & Commercial Buildings

These checkpoints are intended to help in the development of safety and security programs, which should include:

- *Contingency plans,*
- *Emergency evacuation plans,*
- *Building inspection checklists, and a*
- *Safety and security committee.*

Some issues deal with content and others with process, but all are directed toward avoiding oversights and obstructions in the development of effective safety and security programs.

Loss identification and management “action points”

> Identify risks:

Survey facilities and review the current safety and security process. Make use of resources from federal agencies such as FEMA (the Federal Emergency Management Agency) via their web sites, publications, and telephone help lines. Communication with local fire and law enforcement agencies is essential. Also helpful are professional associations and organizations. Talk to your insurance agent. If possible, make use of certified professionals in your inspections and reviews. Communication with all these organizations will assist in the identification and mitigation of risks.

> Analyze the risks your organization or building face. To analyze risk:

1. Develop a list of negative events that could occur to your organization / facility. Loss can result from natural disasters such as tornadoes and flash floods, man-made environmental disasters, terrorism, domestic violence, and criminal activity including fraud and theft.
2. Estimate/appraise the degree of risk associated with each recognized event.
3. Assign a weight or value to each event based on potential loss of life, property, intellectual property/information, etc.
4. Assign to each event the likelihood of occurrence. This probability value should be based on the experiences of your organization, community, and other similar organizations. Add to this the potential value or weight of any new factors affecting your industry or organization type, your community, similar types of facilities, etc.
5. Rank your risks. Rate and order potential events according to their combined value of potential loss and likelihood of occurrence.
6. Create a plan and process to address these risks.

> Informed decision making:

Allow an adequate amount of time for informed decision-making. Time is necessary to coordinate with all appropriate outside agencies such as local fire and law enforcement agencies, as well as other organizations within the facility/building and other organizations in your community as needed. Internal people critical in the decision-making process are those who can secure funding, develop and set policies, and

administer the safety and security processes that are, or need to be, developed.

> Policies & procedures:

Develop a structured policy and corresponding sets of procedures for each potential loss. To help ensure success, seek the acceptance of those targeted for protection, as well as those who provide the policy/procedure's funding and administration.

The protection of lives will be the first priority. As to property, intellectual property and data are likely to be important commodities. Contingency plans, to ensure business resumption, are also necessary. Off-site, back-up data storage (including the current week's employee contact list), and to a lesser degree back-up facilities, are key elements of your contingency plans.

Some recommend that data be mirrored live in at least two locations or backed up on tape and remotely stored; the goal is order, accessibility and protection for proprietary data (see *Time Magazine*, October 2001, Page Y11). According to *Time*, "40% of businesses that are hit by disasters such as earthquakes and fires close within two years." An alternative for some companies will be the use of optical-character-reading scanners to produce digital archives of documents that can be stored on CD-ROMS.

> Take action:

Correct current conditions and improve procedures to mitigate losses. Measures can be active or passive. The five basic loss management techniques are:

1. Avoidance (*lowering corporate and public profiles, limiting travel perceived as risky or of marginal value and substituting video and web-based conferencing, decentralizing operations, and removing a threatened object from a vulnerable location*)
2. Reduction (*broadening employee background checks to include both criminal and motor vehicle records; some countries other than the United States offer multinational companies who employ foreign nationals access to their government's intelligence indexes*)
3. Spreading (*includes delaying strategies -- such as the installation of barriers, locks, and alarm systems, procedural controls that reduce the opportunity for a loss, and security guard check-in; and pooling of isolated data storage devices/systems*)
4. Transference (*purchasing insurance such as property-casualty coverage and life insurance for workers. Better planning could include coverage of the loss of a CEO as well as business interruption coverage for not just lost profit but also overhead. One product gaining popularity is "violent acts" insurance; it provides benefits for employees as well as anyone who is on company property during an attack. Another transference practice is to pass the costs of associated loss on to customers.*)
5. Acceptance (*accept or retain the risk*)

> Ensure continued financing:

Maintain an annual budget for safety and security. In general, it is easier to obtain resources to correct or upgrade current property, facilities and procedures immediately

following a loss. If no major loss has occurred in recent history, it is common to encounter little interest and support, and fewer resources, to allocate to the prevention of future losses.

It can be difficult to maintain adequate budgets for facilities and safety/security procedures when losses don't occur and/or technological improvements, rather than wear, drive new purchases. One expense that is especially important to budget for is information storage. It is estimated that the volume of digital information (transaction data, e-mail, video images) that companies collect and store doubles every year. Conduct periodic reviews of all insurance policies to ensure adequate coverage.

Integrating people into the emergency process

An organization's members need to proceed through a series of steps to personally integrate and adopt the organization's safety and security programs and procedures and to become reliable, functioning units of the group.

The adoption process will likely include:

1. Awareness of the emergency plan's "process":

At work, individuals should become aware of the organization's program and how it operates (its process) through new employee orientations.

For the public, audio announcements can be made regarding emergency procedures in place (perhaps directing people to signage which identifies shelters or emergency evacuation procedures). These announcements can be delivered via television and radio broadcasts. When these announcements are made via public address systems in government buildings, malls, bus/train stations, etc., reminders of the process can be inserted in regular operational announcements.

Radio and television announcements are frequently used to notify employees of short-term changes in a local emergency process. One example would be a request to drivers involved in "fender-benders" during a snowstorm to go to the nearest police station to report the event instead of pulling off the road.

2. Education:

Employees are often given a pamphlet or shown a video to provide an overview of an employer's (or the building or facility's) safety and security policy and procedures. However, each employee's participation in emergency drills is essential. Employees should practice emergency evacuation procedures every six months or so; there should also be practice drills for other relevant disasters such as earthquakes, tornadoes, major chemical spills, etc. If there is high turnover, more frequent drills should be conducted and/or individual participation should be scheduled, monitored and recorded.

Public safety and security programs/process are often first learned in school, as with the civil defense notification system and fire evacuation drills. Education in other life safety skills including procedures for personnel safety in natural disasters (flash floods, earthquakes), water safety, violence avoidance, etc. are strongly encouraged.

A variety of national and local government agencies, such as FEMA, deliver public safety/security announcements and reminders through the national and local media -- newspapers, radio and television.

Essential elements of safety and security education are:

- Familiarity with, and understanding of, different audible and visual signals, signs, and alarms (fire, tornado, containment breach, etc.)
- Awareness of the alarm objectives (seek shelter, evacuate the facility, etc.)
- Knowledge of the warning system process:
 - alarm systems may be silent or audible
 - alarms may notify only occupants, or only individuals off-site, or individuals both on- and off-site
- Knowledge of whom, if anyone off-site, is notified by alarms
- Repeated practice of recommended procedures

3. Cultural adoption

* Modeling

Programs, plans, and processes can be technically correct and still fail because a key group of people, such as parents or senior management, did not personally adopt the procedures.

There should be no “them” and “me/us” when it comes to safety and security procedures. Some characterize this issue with the phrase “walk the walk.” Others would say failures occur when the procedures are not integrated into the organization’s culture. Every employee should participate equally in drills. If there is an ID program in place, all employees should wear or display their ID tags. Consider training every employee in the use of fire extinguishers, first aid and CPR.

Senior management serve as role models. What they do or don’t do signals the importance, and therefore acceptance and adoption, of safety/security procedures in families and organizations.

* Open involvement

In addition to (role) modeling, keeping involvement and participation open to everyone in the development and/or maintenance of safety/security procedures is important. Employee involvement can assist in the adoption of safety and security procedures. While maintaining open employee involvement opportunities, it is still important that involvement is managed to the degree that a variety of people representing different groups within the organization or facility actively participate. This type of diversity can help identify and head off potential roadblocks to success.

Maintaining diverse employee involvement can help identify, during the planning and review processes, current procedures, norms, and/or political/social/cultural issues that could derail well-intended rules and procedures. Would senior management know if equipment noise is likely to block out audible alarms? Who would know that sight lines to visual alarms are blocked at certain workstations after new machinery is installed? Are planners familiar with what is considered normal behavior regarding outside delivery service drivers and visitors including vendors, family members, and customers? How are temporary employees integrated into the process? What arrangements are made for the physically challenged and those who do not read or speak English?

To further maximize the involvement of diverse members, educate them. It is essential that committee participants, inspectors, reviewers, and others understand the rationale

for rules and procedures. Incomplete knowledge can lead to incorrect assumptions, with disastrous results. To encourage procedure/rule compliance, who could be more effective than an informed peer who can explain its rationale? *(Example: If propped-open stairwell fire doors are a chronic problem, perhaps it is not generally understood that doors into stairwells marked for fire evacuation must be kept closed to help keep fire out and to prevent drafts in the stairwell that can feed a fire, help spread it, and thereby make the stairwell unusable as an exit route.)* When the objective or desired outcome of a rule or procedure is understood and accepted, compliance is likely to increase.

To help develop and maintain a functioning safety/security committee, secure:

- Member representation from maintenance, operations, administration including finance, and unions
- Member representation from all social and cultural groups
- Ongoing, mandated technical education of committee members
- Peer-enforcement of model safety and security behaviors
- Senior management's positive recognition of and involvement in the committee
- Use of maximum terms of office to keep the committee fresh
- Objectives and tasks that are mandated, scheduled, useful, and relevant
- Public recognition of the committee's success

Unscheduled review windows

Safety and security plans and procedures should be reviewed on a scheduled, periodic basis. Administrators can also tag specific types of events for an automatic safety/security review (and possible adjustment to procedures). Here are some examples of events that could generate automatic review windows:

- > Increased publicity/public awareness (*major litigation, merger*)
- > Use of facilities for a new/additional function (*adding on-site child care center*)
- > Opening the use of meeting rooms or auditoriums to outside/community groups
- > Contracting for new services or services with a new supplier (*employee/customer shuttle vans, carpet cleaners, indoor plant maintenance, equipment repairs, etc.*)
- > Changing types of chemicals used (and stored) in manufacturing, servicing, and/or cleaning processes
- > Installation of new types of emergency doors, elevator controls, emergency lighting, windows, phone system, etc.

Contact: Jan Sutkus sutkusj@nsc.org
Educational Resources Division
National Safety Council

October 2001