1. **Identification of Workplace Hazard**

   One cause of workplace injuries not due to work performed for the employer is physical violence by a criminal intruder, disturbed customer or disgruntled employee or associate of an employee. Hazards resulting from an act of crime are by far the more prevalent and dangerous situation. Given the need for many offices and commercial establishments to be open to the public and to be located in virtually all communities, their appearance of affluence and vulnerability is attractive to those who are predisposed to crime. However, disgruntled ex-employees and individuals with personal problems with an employee may pose an equal hazard.

   To prevent acts of violence, the employer must train employees to cooperate fully with all physical and administrative security measures available. These include access controls as well as emergency response and evacuation procedures in the event of an incident.

   In addition, employees should know how to recognize potentially dangerous or threatening situations and promptly report these to management. Examples include:

   (1) Suspicious conduct by any person with no legitimate relationship to employer's operations.

   (2) Violations of security systems by employees or others.

   (3) Agitated or disgruntled customers who threaten employees.

   (4) Agitated or disgruntled employees or ex-employees who threaten employees.

   (5) Knowledge that a relative or associate of an employee has threatened to commit a violent act.

   Given the increase in frequency of violent incidents in workplaces, and the general mandate of the Injury and Illness Prevention Standard to prevent all workplace injuries, Cal/OSHA requires employers with a recognizable workplace violence hazard to take action to prevent future incidents.

2. **Management and Trainer Information**

   Due to the increasing prevalence of violence as a cause of injuries in workplaces, Cal/OSHA has issued Guidance for Workplace Security and a Model Injury and Illness Prevention Program for Workplace Security.

   This guidance emphasizes Cal/OSHA's position that violence should be prevented by employers like any other safety hazards.

   To begin to analyze the potential for workplace violence and to design a prevention program, employers need to consider the type of violent workplace events which can reasonably be anticipated. Incident recognition and preventive measures listed in the following table are based on Cal/OSHA's classification scheme.

   **Type of Violent Event(s)**

   Type I events are cases in which the hazardous agent, or person committing the act, has no legitimate relationship to the workplace and usually enters to commit a robbery or other criminal act.
Appropriate Preventative Measures

(1) Establish safety measures to make employees aware of how to avoid violent situations and enhance personal protection.

(2) Provide physical barriers to access and alarm systems.

Type II events are cases where the hazardous agent is the recipient of services provided at the affected workplace, for example, the assailant is a current or former customer.

Appropriate Preventative Measures

(1) Provide control of physical access through workplace design.

(2) Provide alarm systems.

(3) Train employees on safety procedures to enhance personal protection.

(4) Train employees to recognize hostile situations and how to diffuse such incidents.

Type III events are cases where the hazardous agent has an employment-related involvement with the workplace, for example, the agent is a current or former employee, a relative or friend of an employee or has a dispute with an employee.

Appropriate Preventative Measures

(1) Physical barriers and most other preventative actions are ineffective because the assailant usually is known and welcome.

(2) Improved employer-employee communications to ward off hostile relations between the employer and employee or to encourage employees to confide in their employer concerning threats to their safety.

Depending on their location and clientele, employers will most often encounter Type I and Type II violent events, although Type III events are possible. In any event, to establish an appropriate prevention program, an analysis of potential threats should be conducted by the person responsible for the injury and illness prevention program (or security if the employer has established this position). This analysis should consider factors such as the incident experience of the workplace, local crime statistics, and industry trends. The resulting analysis will assist in identifying appropriate security countermeasures which will prevent future incidents. Measures that are suitable for most workplaces (with type of event indicated in parentheses) include the following:

Physical Safety Measures

(1) An access management system should be used during all business and non-business hours to limit access to only those persons having a legitimate need to enter the facility or certain interior areas of the facility. Customer access should be controlled and limited to only those areas designed to provide customer service. The access management system should be a combination of electronic card access, video cameras and burglar alarms (Type I and Type II).
In facilities where state-of-the-art electronic security systems are not warranted, access management should be established through the use of a traditional lock and key control program and should be rekeyed annually (Type I and Type II).

Wherever possible, a physical barrier between the customer and service provider should be established. Design of the barrier may vary from a service counter to bulletproof glass enclosure depending on the nature and severity of the threat (Type I and II).

Customer service areas should be open and easily viewed. Objects or displays that restrict view or allow for concealment should be removed. Valuable items such as computers, customer records and goods should not be accessible from the customer service areas or visible through exterior windows. (Type I).

"Panic alarm" systems and "panic buttons" in strategic locations in the office are an additional security measure (Type I and Type II).

The building exterior including entrances, walkways and parking areas should be adequately illuminated (Type I).

Private security or guard agency may be retained to provide further security (Type I).

An armored car service should be used to transport valuables (Type I).

Procedural Security Measures

A formal access control policy should be established. This policy should define the objectives of the program, identify limited access areas, and define criteria for assigning authorization levels to employees, vendors and visitors (Type I and Type II).

Employees should be required to wear their identification cards and be instructed in the proper use of the cards. This should include formal policies against allowing persons to piggyback, loaning cards to others, and requirements for reporting lost or missing cards or keys (Type I and Type II).

Employees should never allow access to anyone not displaying an authorized access card. Persons attempting to gain access without authorization should be immediately reported (Type I and Type II).

A "zero tolerance" policy for any act of threat or harassment in the workplace should be established. Action plans to immediately respond to these acts should be adopted (Type III).

Employees need to be sensitive to and recognize threatening or hostile situations that may lead to violence (Type I and Type II).

Employees should report all threatening or hostile situations immediately to their supervisor or at a minimum to the nearest co-worker (Types I, Type II and Type III).

Employees should use a "buddy system," especially during off hours (Type I and Type II).

Access to inner office work areas should be controlled at all times. Customers should be allowed into such areas only with the expressed consent of an authorized employee. Visitors admitted to the inner office work areas should be escorted at all times (Type I, Type II, and Type III).
(9) Employees should be aware at all times of potential "escape routes" from whatever area they are working in (Type I, Type II, and Type III).
Employees should use "panic buttons" if equipped or other means of immediately summoning assistance in an emergency (Type I, Type II, and Type III).

Employees should look out windows or door viewers before exiting the building. This is critical for doors that exit into an alley or another location hidden from public view (Type I, Type II, and Type III).

Employees must not resist in the event of a robbery attempt. Money or any other item demanded should be surrendered immediately and other employees should try to separate themselves from the assailant (Type I).

The employer should minimize the amount of cash and other tangible assets kept on hand (Type I).

Actions the employer has implemented (selected from the above list to the extent applicable) should be incorporated as part of the employer's injury and illness prevention program.

3. Employee Safe Work Practices

Employees should be required to comply with the following safe work practices to the extent applicable:

1. Surrender money or any other items of value demanded by a threatening assailant.

2. Know how to call for emergency assistance from other employees, building security, or public officials.

3. Know how all alarm systems, security locks and panic buttons work and their locations, and use these devices as instructed.

4. Know how to evacuate from any area in the office, plant or other buildings.

5. Lock doors after regular business hours, even if not required during working hours. Never grant access to an unauthorized person even if you know them.

6. Wear your identification card or badge at all times and report missing or lost cards or keys immediately.

7. Never loan your access card or keys to anyone.

8. Report any unauthorized access or suspicious activity to your supervisor or person responsible for injury and illness prevention or security officer.

9. Avoid being alone in offices and other workplaces where intruders are a possibility. Follow the buddy system.

10. Always look outside before leaving during non-business hours. Use a well-lit route and park in a well-lit area.

11. Be sensitive to agitated customers, employees or other persons who may become violent. Report all such incidents to your supervisor, other employees and the person responsible for injury and illness prevention.
(12) Be attentive to co-workers and others who express concern about their personal safety. Attempt to learn about potentially violent intruders and discreetly report the concern.
4. **Items Subject to Periodic Scheduled Inspections**

The employer's periodic scheduled inspections should consider the following items during workplace inspections:

1. Is the workplace's access management fully functional with all systems in operation and coverage complete?
2. Are conventional door lock and other physical security measures operational and have the locks been rekeyed at a reasonable frequency?
3. Do current physical barriers and reception procedures prevent entrance into the workplace, unless authorized?
4. Is unauthorized entrance available at some other location; for example, the loading dock?
5. Do tests of panic alarms and communications systems indicate that they are operating as designed?
6. Is there any evidence of circumvention of security systems, blocking open of secure entries, employees loaning keys or cards?
7. Are employees following a buddy system during off-hours work?
8. Are entrance ways, hallways and parking areas well illuminated?
9. Is there excess cash present in publicly accessible areas of the workplace?
10. Is there an excess amount of valuable goods on display in publicly accessible areas or in windows?
11. Are any unauthorized persons present in the non-public areas of the workplace?