
Causes and Contributing Factors
Prevention Programs & Countermeasures
Model Policies & Program Checklists
Legal & Regulatory Changes
Current Research & Case Studies
Training Best Practices
Threat Assessment Tools
Latest Benchmark Data
New Risks & Prevention Strategies
2011 Report on Workplace Violence:
Complete Guide to Managing Today’s and Tomorrow’s Threats

Including ...

Causes and Contributing Factors
Prevention Programs and Countermeasures
Model Policies & Program Checklists
Legal & Regulatory Changes
Threat Assessment Tools
Current Research & Case Studies
Latest Benchmark Data
New Risks & Prevention Strategies
# 2011 Report on Workplace Violence: Complete Guide to Managing Today’s and Tomorrow’s Threats

## TABLE OF CONTENTS

### INTRODUCTION .......................................................... 7

### I. VIOLENCE PREVENTION PROGRAM ELEMENTS ............................................. 11
   A. Risk Assessment ................................................................. 11
   B. Program Development ......................................................... 24
   C. Policies .................................................................................. 30
   D. Background Screening .......................................................... 39
   E. Physical Security ................................................................. 47
   F. Training .................................................................................. 54
   G. Incident Management ............................................................ 66
   H. Crisis Response ................................................................. 76
   I. Partnering ............................................................................. 92

### II. CAUSES/COUNTERMEASURES ........................................................................ 97
   A. Criminal ............................................................................... 98
   B. Customers/ Clients ............................................................... 112
   C. Coworkers .......................................................................... 116
   D. Domestic Violence .............................................................. 123

### III. CONTRIBUTING FACTORS/MITIGATION ..................................................... 131
   A. Adverse Employment Actions ............................................... 131
   B. Organizational Culture ......................................................... 141
   C. Stress ................................................................................. 145
   D. Substance Abuse .................................................................. 148
   E. Online Communication ......................................................... 150
   F. Solitary Workers .................................................................. 153
   G. Open Environments ............................................................. 157
   H. Racial Conflict .................................................................... 162
   I. Suicide .................................................................................. 165
   J. Crowds ................................................................................ 166

### IV. LEGAL/REGULATORY CONSIDERATIONS .................................................. 171
   A. General Liability Prevention .................................................. 173
   B. Workplace Safety Regulations .............................................. 176
TABLE OF FIGURES

Figure 1. Number of Workplace Homicides, 1992-2008 .......................................................... 11
Figure 2. Incidence of Workplace Assaults vs. Total Lost Work Time Injuries and Illnesses Since 1999 ........................................................................................................... 12
Figure 3. Cause of Fatal Work Injuries, 2008 ........................................................................... 13
Figure 4. Change in Target of Business Robberies ................................................................. 13
Figure 5. Victims of Workplace Bullying .................................................................................. 14
Figure 6. Occupations With Greatest Number of Homicides, 2008 ........................................ 14
Figure 7. Number of Workplace Homicide Victims by Gender, 1997-2008 ............................ 15
Figure 8. Rate of Significant Incidents of Workplace Violence by Public Accessibility ........... 15
Figure 9. Use of Employee Perception Surveys About Security ............................................. 19
Figure 10. Organizations Using an Interdisciplinary Team to Address Workplace Violence Prevention Industry, 2010 ................................................................. 26
Figure 11. Organizations Lacking a Written Policy on Workplace Violence by Size and Type, 2010 ................................................................................................................. 30
Figure 12. Formal Workplace Weapons Policy by Size of Organization, 2006 ...................... 35
Figure 13. Discipline for Violations of Organization Weapons Policy, 2006 ........................... 36
Figure 14. Job Applicants With Criminal Record by Employer Industry, 2008 ..................... 39
Figure 15. Personality Testing of Prospective New Employees, 2010 ........................................ 40
Figure 16. Physical Security Measures in Private Industry Workplaces by Size of Company, 2006 ......................................................................................................................... 49
Figure 17. Annual Training on Workplace Violence Prevention to General Workforce, 2009 ................................................................................................................................. 54
Figure 18. Annual Training on Workplace Violence Prevention to General Workforce by Organization Size ........................................................................................................... 54
Figure 19. Annual Training on Workplace Violence Prevention to Managers/Supervisors ................................................................................................................................. 55
Figure 20. Annual Training on Workplace Violence Prevention to Managers/Supervisors by Size ....................................................................................................................... 55
Figure 21. Employee Training at Large Establishments on Workplace Violence Reporting Procedures by Industry, 2006 .................................................................................. 67
Figure 22. Prevalence of a Mass Notification System by Industry, 2010 ................................. 84
Figure 23. Establishments Experiencing Workplace Violence by Source of Violence, 2006 ................................................................................................................................. 98
Figure 24. Large Establishments Experiencing Criminal Workplace Violence by Industry, 2006 ..........................................................99
Figure 25. Large Establishments With Method for Identifying Clients/Customer With History of Violence, 2006 ..............................................113
Figure 26. Witness Perception of Organization’s Response to Reported Bullying ......118
Figure 27. Abusive Supervisor Behavior of Subordinates, Observed or Experienced...119
Figure 28. Victim Response to Workplace Bullying, 2007 .........................................119
Figure 29. Organizations Addressing Bullying In Workplace Violence Prevention Policy by Size and Type ..............................................121
Figure 30. Establishments Addressing Domestic Violence in Workplace Training by Size, 2006 ....................................................................124
Figure 31. Current IPV Victims Reporting Victimization at Work, 2009 ..................125
Figure 32. Victims That Disclose Intimate Partner Violence—Who They Tell, 2009 ....126
Figure 33. Where & When Domestic Violence Assaults in the Workplace Occur......127
Figure 34. Employees Reporting an Increase in Stress & Stress-Related Conditions, 2010 ............................................................................145
Figure 35. Substance Testing of Prospective New Hires, 2010 .................................148
Figure 36. Routine Scheduled Substance Testing of Existing Employees, 2010 ....149
Figure 37. Random Substance Testing of Existing Employees, 2010 ......................149
Figure 38. Organizations with a Policy of “For Cause” Substance Testing by Size, 2010 ..............................................................................149
Figure 39. Perpetrators of Cyberstalking by Relationship to Victim, 2004 ...............151
Figure 40. Locations of Assaults at Institutions of Higher Education (IHE) ..............159
Figure 41. Company Tracking of Costs Related to Incidents of Workplace Violence by Size of Company, 2006.......................................................201
Figure 42. Workplace Violence Costs Tracked by Large Companies, 2006 ..........201
Figure 43. Comparing the Cost of Violence Versus Prevention ...............................202
Figure 44. Health Effects Observed by Witnesses to Workplace Bullying, 2007 ......204
Figure 45. Result of Workplace Bullying, 2007 ..........................................................205
Workplace violence can be easily defined as violent acts, threats, and other intimidation or harassing behavior directed toward a person at work or on duty. Generally, an event of this nature will fall into one of four types of situations:

- **Criminal.** When the perpetrator has no legitimate relationship to the business or its employees and is usually committing a crime in conjunction with the violence (e.g., robbery, shoplifting, or trespassing).

- **Customer or client.** When the perpetrator has a legitimate relationship with the business and becomes violent while being served by the business (e.g., customers, clients, patients, students, inmates, or any other group to which the business provides services).

- **Coworker.** When the perpetrator is an employee of the business, past employee, or contractor who works as a temporary employee of the business and attacks or threatens another employee.

- **Domestic violence.** When the perpetrator, who has no legitimate relationship to the business but has a personal relationship with the intended victim—such as a family member, boyfriend, or wife—threatens or assaults the victim at the workplace.

Simply defining terms and setting out the scope of the threat belies the complexity of the challenge, however. Consider an issue that Starbucks finds itself facing. While going about its business of selling coffee, the company has found itself dragged into the national debate over gun rights.

Advocates of “open carry” singled out Starbucks locations to test the corporation’s policy toward those who carry firearms by visibly wearing guns into its establishments. Though most states allow it through concealed carry laws, establishments generally have the right
to restrict guns on their property by posting signs to notify customers they are not permitted. Starbucks said it faced a difficult choice: Ban guns from stores—and ask baristas to confront gun-toting customers—or ignore the objections of gun opponents who object to sipping frappuccinos next to a guy with a gun on his hip.

In March 2010, the company issued a statement. “We have examined this issue through the lens of partner (employee) and customer safety. Were we to adopt a policy different from local laws allowing open carry, we would be forced to require our partners to ask law abiding customers to leave our stores, putting our partners in an unfair and potentially unsafe position.”

The decision could not have been an easy one for Starbucks to make. Back in 1997, an employee of a store located on an upscale stretch of Wisconsin Avenue in Washington, D.C., arrived to a gruesome scene. The three-person crew from the night before had been shot and killed in an apparent robbery attempt.

Starbucks referenced its history with workplace violence in its statement regarding the gun controversy. “We are asking all interested parties to refrain from putting Starbucks or our partners into the middle of this divisive issue. As a company, we are extremely sensitive to the issue of gun violence in our society. Our Starbucks family knows all too well the dangers that exist when guns are used irresponsibly and illegally.”

The above example reflects the gray areas that arise as companies attempt to navigate what may seem like a black-and-white issue. There are many are others, like zero-tolerance (should a long-time employee really be terminated for a single threatening comment jokingly made?) and background check procedures (how far back into a worker’s history do you need to dig for possible violent acts? Three years? five? ten?).

Workplace violence has been atop the list of workplace worries for decades, but the issue is far from static. Threats, best practices, prevention tools, and the regulatory environment constantly evolve.

- New technology has significantly changed how companies can and should respond to an active-shooter incident, conduct background checks of workers, and secure controllable spaces.

- Lawmakers are raising the stakes for preventing workplace bullying with proposed legislation to expand harassment laws to cover all workers—not just those of a protected class.

- States are forcing employers to rewrite company policies, like businesses in Indiana, which since July have been prohibited from telling employees they can’t keep guns and ammo in their locked vehicles at work (joining 12 other states that have recently passed similar laws).

- New case studies show what works—and doesn’t—when trying to issue crisis alerts and respond to mass casualty events, and how to minimize workplace stressors that are precursors to violence.
INTRODUCTION

- The troubled economy has increased incidence of workplace suicides, shootings sparked by layoffs, and violent conflicts with shoplifters.

- Better security at traditional targets have forced criminals to turn to other businesses, putting a broader array of workers at commercial establishments at substantial risk of workplace robberies.

- Issues that increase job stress—a contributor to violence—have been increasing in many workplaces because of the troubled economy and layoffs (stressors include role ambiguity and a mismatch between knowledge/skills and one’s work role).

- Diversity and downsizing can be a volatile combination, and there are indications that even as society as a whole grows comfortable with the nation’s multiracial demography, it can be a spark for troubled individuals in an uncertain, competitive job market.

- New data show which types of violence companies too often ignore and how much they typically spend on violence prevention, and provide benchmarks on the training they conduct.

This report is designed to help organizations adapt to changes in the law; implement new tools, strategies, and knowledge; and incorporate lessons learned to strengthen existing violence prevention efforts. It also details the full range of fundamental elements that a violence prevention program must build upon to be a living, breathing part of the organization—one that ensures ongoing commitment and continuous improvement.

It provides guidance and describes best practices in all aspects of a comprehensive program: from policy wording and employee training to incident response and hazard control. The report can also help organizations that want to focus on or assess their handling of a single issue, such as including bullying within the violence prevention program, reducing assaults in parking areas, or enhancing the safety of employees who work alone.

- Section I describes the elements of a successful workplace violence prevention program, including baseline program elements, security and personnel strategies that can aid in preventing all forms of violence, and how to structure prevention to have an effective mechanism for reacting to fluctuations in risk and emerging threats.

- Section II examines each of the primary causes of workplace violence, identifies trends in each, and details recommendations for prevention.

- Section III describes factors that can make workplace violence more likely, alongside new advice for managing them and minimizing the threat they pose.

- Section IV examines legal issues, with a special focus on recent changes in the legal and regulatory environment and what it is on the horizon.

- Section V provides a closer look at the costs of workplace violence in order for companies to justify violence prevention initiatives, as well as advice for extracting maximum value from violence prevention efforts.
• Section VI includes model policies and program checklists that companies can use to develop or improve select aspects of a prevention program or audit the adequacy of their current efforts.

The latest data on workplace violence—as well as benchmarks on how companies are addressing it—are included throughout the report. This information is useful for navigating difficult questions regarding workplace violence, such as emerging threats that demand greater attention or how strictly to word a zero-tolerance policy. Comparative data also help to show a company how its response to different risks stacks up against other companies’—a critical question should a tragic incident cause a plaintiff’s attorney to take aim at a company’s prevention efforts.

Finally, the report includes dozens of “From the Field” sidebars. These boxes describe current research and case studies to reflect workplace violence in the “real world,” help firms transition from understanding the right thing to do to getting it done, and show the real consequences from program failures.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

There is no magic bullet in workplace violence prevention. To successfully combat violent acts, threats, hostile behavior, and other forms of workplace violence, organizations must fight on many fronts. An internal risk assessment will focus an organization’s intervention, but rarely will it point to a single strategy. More likely, a successful prevention plan will need to encompass improvements in many areas simultaneously.

A. Risk Assessment

By the most tragic measure—employee fatalities—violence has become a relatively less important issue of workplace safety. While the total number of annual workplace deaths due to other causes is a touch higher today than it was in 1992, the number of workplace homicides has been cut in half (see Figure 1). Additionally, workplace assaults comprise less than 4 percent of all lost work-time injuries and illnesses. However, these statistics paint a false picture of the position that violence prevention should have within the overall workplace safety program.

It’s true that the number of workplace homicides is way down and that assaults account for less lost work time than most all other injury and loss of life, but the data also paints a picture of a workplace culture that does not take the potential for violent acts seriously enough.

*Most recent year for which data is currently available
**Totals for 2001 exclude fatalities from the September 11 terrorist attacks.
(Source: Bureau of Labor Statistics)
illness categories—including repetitive motion injuries, falls, slips, and overexertion. But if companies focus on the raw numbers to guide their workplace safety priorities, they may be making a costly error.

One chief example of why this is so is that companies are making better progress against other causes of injuries. There has been a decline in both workplace assaults and total workplace injuries since 1992, but there has been a larger drop in injuries overall than for assaults due to violent incidents, according to data by the Bureau of Labor Statistics. While the rate of all injuries has dropped consistently at about 5 percent per year, the overall decline for injuries due to violent incidents has not been nearly as significant, and the rate has even gone up almost every other year, including 10 percent in 2006 (see Figure 2).

It’s clear from the data that gains made in the prevention of workplace injuries from other causes are the result of permanent safety improvements, such as safer equipment or safer work processes, while reductions in workplace assaults are alterable and subject to swings in the general crime environment and workplace hostilities. Additionally, workers’ compensation claims related to crime-related injuries typically cost

---

**Media Reports Distort the Risk Picture**

Recognizing that job type is the single greatest risk factor for suffering a violent act is not something that every organization does, according to researchers from the Southern California Injury Prevention Research Center at the UCLA School of Public Health.

From their study, researchers concluded that some companies focus too much on preventing rampage shootings at the expense of preventing attacks that workers suffer because of the jobs they perform. The finding that most workplace violence is actually linked to crime contradicts “the excess[ive] media attention that employee-on-employee events receive compared with other workplace violence types,” UCLA researchers concluded (Journal of Occupational and Environmental Medicine, 2003).

Despite the media attention they receive, rampage office shootings are rare and getting more so, while year-to-year data are far less encouraging for violent attacks as the result of robberies and other assaults related to workers’ jobs. Dr. Rosemary Erickson, a security consultant specializing in workplace violence and liability (Athena Research Corp.), says she sees the same mistake in her dealings with clients. Companies focus on staff-on-staff violence, even when such events represent a small fraction of violent incidents affecting their staff, she says. Rather than letting national trends or news reports guide them, companies need to analyze internal incident data and focus on their specific areas of risk.
much more than injuries of other types, and medical payments also tend to be higher when crime is the cause of the injury. (For more information on these costs, see Section V. Program Assessment.)

Workplace murders are indeed at their lowest level in more than a decade, but worker fatalities from assaults and violent acts remain the third leading cause of workplace fatalities (see Figure 3).

Of course, workplace violence encompasses a far wider range of events than homicide. Robberies and assaults are acts of workplace violence, and in many geographic areas and for certain types of businesses, the rate of these violent incidents are on the rise.

After years of being easy targets, businesses like convenience stores have improved their security. Thieves seem to have caught on and have increasingly been targeting other commercial houses (e.g., supermarkets, department stores, restaurants) in which deployment of standard security measures and cash management is far less certain and rewards are potentially higher. As a percentage of commercial robberies, these less stereotypical targets now comprise a greater share, while crime at gas and service stations and convenience stores has declined and robberies of banks are basically unchanged (see Figure 4).

The sagging economy is also a risk factor. Although the most recent statistics from the FBI showed a decline in robbery and burglary—confounding many experts who predicted a crime wave would accompany the recession—retailers have reported a surge in shoplifting. These crimes routinely put store associates and loss prevention personnel in confrontation with often-desperate individuals.

Verbal abuse, harassment, and lesser forms of intimidation are also types of workplace violence—and in this area the latest data are sounding a real alarm. There are an estimated 43,800 acts of harassment, bullying, and other threatening behavior in the workplace every day. According to the most recent large national survey on workplace bullying, 37 percent
of the U.S. workforce (an estimated 54 million Americans) report being bullied at work; an additional 12 percent witness it.

It is difficult to speak in any broad sense about whether the problem of workplace violence is getting better or worse. Some contributing causes of incidents are growing more troublesome, while progress has been made against others. Some types of violence are on the decline, but others are on the rise. What is increasingly clear, however, is the price companies pay for violence in the workplace. It is well understood that a workplace shooting will result in substantial legal bills and that the harm to reputation, brand, and employee morale may be incalculable, but there is increasing evidence that threats, intimidation, and other bullying behavior is a real drain on company productivity as well—making a robust workplace violence prevention program a bottom-line benefit to the organization.

**Employee risk**

A worker’s vocation is his or her single greatest risk factor for being killed while working. This fact is clearly represented by the list of jobs that comprise the highest percentage of workplace homicide victims (see Figure 6).

The link is underscored by data on the gender of victims.
Although women are almost always the victims of domestic violence shootings that occur in the workplace, men nonetheless comprise the majority of workplace homicide victims (see Figure 7). This reflects the fact that men still perform a majority of the most dangerous jobs, like police officer and taxi driver.

Of course, workplace violence prevention programs must take aim at other forms of violence as well, including physical assaults, threats, harassment, and intimidation. But here, too, employees who have contact with the public suffer a higher incidence of violence, facing potentially aggressive behavior from clients or customers.

A survey of 275 companies by IOMA/SDR found that organizations suffered one significant incident of workplace violence for every 613 employees in 2008. (A “significant incident” was defined for survey respondents as a high-level threat, physical assault, or similar event.) Workplaces that are closed or mostly closed to the public reported fewer incidents, while open environments, particularly retail and entertainment establishments, reported substantially higher rates of violence. Open facilities suffer one significant workplace violence incident annually for every 500 employees, according to the survey (see Figure 8).

**Organizational risk assessment**

Organizations need to be systematic in their own approach to workplace violence risk. By embracing formal risk assessment methodologies, organizations can prioritize and have confidence that solutions make sense within the larger context of mitigating operational risk.
Aggregate data are helpful to illustrate the scope of the issue and understand trends and general risk factors, but they are unable to indicate where any single organization needs to focus its efforts to reduce the risk of workplace violence. A company’s internal data and assessments—examining who, when, and why its own workers are exposed to potentially violent situations—should provide the basis for its violence prevention efforts.

To maximize security and safety benefits and be cost-effective, a violence prevention program needs to be implemented in light of a company’s threats and vulnerabilities. To identify appropriate interventions:

1. Companies should conduct a formal written workplace violence risk assessment to determine the level of risk for violence in the workplace. This entails reviewing specific procedures or operations that contribute to hazards and specific areas where hazards may develop.

2. Companies should conduct a written violence vulnerability assessment. They need to look at their current operations and security procedures to determine where they might be vulnerable to acts of violence.

The contents of this report provide the framework for conducting a workplace violence risk assessment. For example, later in Section II A, we provide a detailed examination of workplace assaults in parking areas and what can be done to prevent them. Employers should review their current security operations in light of those recommendations and factor in their specific level of risk (based on internal incident data and other facility-specific threat factors), to identify what needs to be done to reduce the risk of violence in parking areas.

To aid in conducting the assessment, it may be helpful to follow a general security risk assessment protocol. There are numerous risk-assessment methodologies available to security executives as well as tools to measure and assess different components of risk. ASIS International, the preeminent organization for security professionals in the United States, has created a seven-step process that establishes a methodology by which security risks at a specific location can be identified and communicated. Its “General Security Risk Assessment Guideline” is available for free download for members and for purchase for non-members from the association’s Web site (www.asisonline.org).

The Economy and Crime: Feelings Matter

It’s certainly logical: A tough economy equals more crime. But historical evidence complicates the picture. Crime waned during the Great Depression and grew as the economy began its rapid expansion in the 1960s. Certain categories of crime, including robbery, declined during the most recent recession.

Researchers recently took a novel approach to the issue by examining consumer sentiment and property crime. After all, the actual rate of unemployment or inflation may be less of a driver of behavior than how people feel about it (“The Impact of Economic Conditions on Robbery and Property Crime: The Role of Consumer Sentiment,” Richard Rosenfeld and Robert Fornango, Criminology, November 2007).

“We find that consumer sentiment had significant effects on robbery and property crime rates over the period that were largely independent of the effects of unemployment and economic growth,” said the authors. In short, how the public regards economic prospects is a good indicator of whether your company is more or less likely to be the victim of robbery or other crime in the months ahead.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

It is also important to place workplace violence within the context of overall security risk, so that it receives the correct amount of focus and resources. To help prioritize which threats are most critical, two members of the Steele Foundation—David Patterson, senior consultant, and COO Greg Pearson—believe there is value in using pair-wise comparisons as one part of a risk methodology. This strategy—of comparing different threats at different locations—can help security teams identify where workplace violence fits in the overall security risk picture and in which locations the risk is greatest. (For an example of pair-wise threat analysis, consult item N. Illustrative Pair-wise Threat Analysis in the Appendices.)

It is possible for a single individual to conduct the risk/vulnerability assessment, but for the analysis to be complete it must receive input on risk from many sources, including safety, HR, general staff, and the employee assistance program. Once completed, the individual or risk assessment team should pass the assessment to the workplace violence prevention team along with recommendations for intervention priorities.

Many activities are necessary for conducting a comprehensive assessment of workplace violence risk and vulnerability, including analyzing and tracking records; conducting screening surveys; and analyzing current workplace security. These are described below, separated into three sections—activities for looking at elements internal to the organization, external factors, and measuring.

Internal data

A company needs to systematically assess its internal operations and analyze past incidents to identify which employees are most at risk from violence and why. This assessment will indicate where the company’s risk is greatest and which violence prevention strategies are

FROM THE FIELD...

Study Shows Teen Workers Most Vulnerable to Violence at Work

Teenagers are at higher risk for suffering workplace violence. One reason is because they often work in retail, which suffers a higher rate of workplace violence than most industries. Additionally, their youth seems to contribute to their rate of victimization, according to results from a survey conducted by the Injury Prevention Research Center at the University of North Carolina-Chapel Hill (“Workplace Violence Against Adolescents in the United States,” Rauscher, K.J., American Journal of Industrial Medicine, May 2008).

Out of the 1,171 high school students (age 14 to 17) surveyed, 25 percent said they’ve been verbally threatened on the job, 10 percent said they’ve been physically attacked, and 10 percent have been sexually harassed. “Many working adolescents, most with only a few years’ work experience, have already suffered workplace violence. As youths are likely to be more vulnerable to its effects, developing workplace violence prevention strategies that target adolescent workers should be made a priority,” the study concluded. Supervisors—who are supposed to help protect teen workers from violence—are often the source of it (see below).

Source of Attack on Teenage Victims of Workplace Violence

<table>
<thead>
<tr>
<th>Source of Attack</th>
<th>Customer</th>
<th>Coworker</th>
<th>Supervisor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical attacks</td>
<td>31%</td>
<td>29%</td>
<td>18%</td>
</tr>
<tr>
<td>Verbal threats</td>
<td>55%</td>
<td>30%</td>
<td>27%</td>
</tr>
<tr>
<td>Sexual harassment</td>
<td>34%</td>
<td>45%</td>
<td>32%</td>
</tr>
</tbody>
</table>

(Source: American Journal of Industrial Medicine)
most appropriate for its operations. As part of that assessment, the risk assessment team should conduct the following activities:

- **Review records.** This activity should include reviewing security incident reports, medical and safety records, workers’ compensation, and insurance records (including the OSHA Log of Work-Related Injury and Illness [OSHA Form 300], if required to maintain). Instances of workplace violence indicated in these records will provide evidence of the frequency and severity of the problem.

- **Identify individuals at high risk.** Tabulate and analyze data to learn about high-risk departments, times of day, days of the week, and so on. Construct a risk profile for different persons. Are supervisors at greatest risk? In which departments? Who receives the most threats? Identify those situations where you have the most frequent or serious assaults in order to focus your interventions. For example, use your analysis to identify subgroups of employees, job classifications, facility locations, or job tasks that seem to be putting employees at particularly high risk for injuries from assaults.

- **Identify the risk factors of different buildings.** Do all your buildings have identical access control? If not, the risks for individuals inside them are different. Other controls may need to be put in place to address these differences.

- **Identify how procedures contribute to potential hazards.** Examine the policies and procedures in specific locations or among specific work groups and measure how they may contribute to potential violence. For example, if some departments have a pay-for-performance structure, does worker stress put those supervisors at increased risk? Wherever policies point to a potential problem, examine the records in those units or departments more closely and monitor them more frequently.

- **Examine related documents for insight.** In addition to reports that specifically detail violence or threats, insight into risks and vulnerabilities may be a part of other types of reports, such as safety committee meeting minutes and action items, records of hazard analyses, and records of employee training.

**Assuming You Know Your Risks Can Steer You Wrong**

Vito Capobianco, security chief at University of New Mexico Health Sciences Center, offers the following warning: Don’t assume that you know which departments are the most dangerous and which employees are at greatest risk.

After reviewing several years of violence data, Capobianco discovered that the bulk of his workplace violence incidents were occurring in the business office—not the emergency room (ER). In fact, the ER ranked third behind administration. Although ER employees were found to be at greatest risk of physical assault, the detailed record review uncovered other jobs and locations in which other incidents of workplace violence (such as bullying) were even more likely to occur.

Capobianco notes that if a company fails to identify areas where it faces the most risk from workplace violence, then it can not know if its prevention activities are targeting its biggest threats.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

Internal perceptions

Included in the workplace violence risk assessment should be an analysis of the general work environment and how employees treat each other, how management treats employees, and how supervisors treat subordinates. To gain insights into the general attitudes/perceptions in the workplace, risk assessments may utilize employee surveys, focus groups, or existing committees. Questions about workplace violence, the threats employees face, and how safe they feel at work can be included in perception surveys on security, something that nearly 60 percent of organizations do at least occasionally (see Figure 9). More than 40 percent of very large organizations survey all employees at least annually. Employee and supervisor perception surveys can be particularly helpful to a violence prevention team in several ways:

- **Gauging the perception of risk for comparison to actual risk.** Identify gaps by analyzing results of the employee survey in conjunction with data from the workplace violence incident reporting system.

- **Learning how risk perception differs among employees.** Examine the perception of risk by department, employee level, time of day, location, and so on. Which departments feel unsafe? When do employees feel vulnerable?

- **Focusing security awareness education on those issues that employees indicate are most important to them.** For example, if employees identify that working alone at night is their top security concern, you can focus employee training on that issue and aggressively promote security procedures that are designed to protect workers who stay after-hours.

- **Indicating what workplace violence policy issues you may need to review.** For example, an employee survey may indicate that workers lack an understanding of how or to whom to report an incident of workplace violence or a threat.

- **Measuring how well you are implementing different aspects of the workplace violence program.** Employee surveys can reveal which procedures go ignored.

- **Demonstrating the commitment of your organization to your employees’ welfare.** By surveying employees on workplace violence issues, an organization demonstrates to staff that it cares about protecting them.
• Advertising aspects of the workplace violence program of which employees may be unaware. For example, surveying employees to see if they’ve ever used a security escort to their car is a good way to alert or remind employees that you provide this service.

• Showing employees that you take workplace violence seriously. By surveying employees about whether they’ve ever suffered any type of abuse from other employees, you can help show that your company won’t tolerate such actions and will investigate reported cases.

• Enabling the corporate security department to compare the security operations of different business units. For example, responses might suggest employees at one business unit feel safer than at another, indicating where security efforts should be focused.

• Improving employee perceptions of risk, which could lead to service improvements and aid recruitment and retention. By proving that you take employees’ security concerns seriously enough to ask their opinion, employees often feel safer. Employees who feel safe in their work environment are more likely to stay with their current employer.

• Providing an objective indication of how successful the security department is at communicating with employees. For example, a survey can show that employees aren’t aware of certain policies or services, and that may indicate that the security department isn’t communicating well with workers.

• Providing a baseline so that the security department can measure future progress toward its goal of communicating better with employees. This can be a good metric to evaluate performance of the workplace violence prevention team.

High-Risk Workplaces Are High Risk Even in Low-Crime Areas

Although the level of community violence can impact workplace violence for many organizations, high-risk employers shouldn’t count on it.

It seems logical to think that employees of large hospitals in high crime areas suffer the most assaults. Indeed, it’s clear from a recent study that this is the perception many hospitals work under. Small hospitals in low crime areas less frequently require certification of security officers or have an in-house guard force and are less likely to have policies for reducing emergency room tensions and panic alarms in the emergency department.

However, of the four types of hospitals studied, small hospitals in low crime areas had the second highest rate of assault-related OSHA-recordable injuries among ED employees (0.66 per 100,000 staff hours). Furthermore, the median assault rate in small hospitals was two to five times higher in small hospitals than in large ones, according to the study’s lead author Jim Blando, Ph.D. The rate of assaults against ED staff was highest of all in small hospitals in high crime areas (1.1 assaults per 100,000 ED employee hours per year).

“Due to the highly stressful workplace characteristics of emergency departments, the risk of employee assault is universal among all hospital sizes in all types of communities,” according to Blando (“Emergency Department Security Programs, Community Crime, and Employee Assaults,” Journal of Emergency Medicine, January 2009).
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

- Empowering staff and soliciting their involvement in addressing goals of the corporate security department. Surveying employees about workplace violence can get them more involved in corporate security issues and help them understand their role in making the workplace safe for everyone.

External data

Internal data provide violence prevention teams with the most relevant statistical information from which to identify appropriate security interventions. But general data, such as area crime statistics or general workplace violence statistics, can also inform workplace violence teams about risk. For very small organizations, those with too little internal data from which to extract meaningful information, broader data can be especially useful in understanding the threat environment.

Benchmarking with like businesses and area organizations provides insight, as can area crime data from the FBI’s Uniform Crime Report (UCR). The UCR is “easily the most exhaustive and comprehensive and geographically comprehensive source of crime statistics for the U.S.,” according to authors Karim Vellani and Joel Nahoun (Applied Crime Analysis).

The UCR maintains data for eight primary crimes in two categories: violent crimes (murder, rape, robbery, and aggravated assault) and property crimes (burglary, larceny theft, motor vehicle theft, and arson). Within these categories, the UCR provides data on crime trends by:

- The nation as a whole.
- Geographic regions.
- Individual states.

Violence in the Community Affects Workplace Aggression

To test their hypothesis that an external environment of violence surrounding an organization relates to workplace aggression within that organization, researchers examined 250 geographically dispersed and operationally independent plants of a nationwide U.S. public service organization.

The conclusion: After controlling for variables, the study showed that the level of violence in the surrounding community does, in fact, predict workplace aggression at the organization (“The Impact of Community Violence and an Organization’s Procedural Justice Climate on Workplace Aggression,” University of Western Ontario, Academy of Management Journal).

“There is a tendency [by organizations] to treat cases of workplace aggression individually. Our finding … supports the notion that workplace aggression is a partial outgrowth of community-level violence. “It has practical implications for workplace interventions. The study concluded:

- Managers might be more successful in eliminating workplace aggression if they recognize “the necessity for strong actions” at the organizational unit level, such as rigorous company policies or unit-wide training.
- Organizations may need to engage in counter-cultural actions to offset the influence of external forces. Such counter-cultural actions might include the use of salient role models engaging in constructive behavior, symbolic management, and other mechanisms that reinforce positive organizational norms.
- Organizations should engage in community efforts to curb social problems such as violence.
• Metropolitan Statistical Areas (MSAs), for example, the Albuquerque, N.M., MSA includes figures for the city of Albuquerque and the surrounding counties of Bernalillo, Sandoval, and Valencia.
• Cities with 10,000 or more population.
• County (suburban counties and rural counties).
• Universities and colleges.

To use UCRs effectively, businesses should weigh data more heavily the more narrowly they apply to their facilities. For example, organizations should pay greater attention to county or city crime trends than state or MSA crime figures.

Another useful strategy is to use the UCR data in conjunction with Calls-for-Service (CFS) data from local police departments. CFS come in to law enforcement via a 911 call or other method, and include not just crimes, but other events such as suspicious activity, traffic accidents, and parking complaints. They are particularly helpful because they are specific to a certain location. As such, it is possible to get CFS data that will reflect security-related incidents and crime trends for a specific property (including your own), a neighboring building, or locations down the street that are in the same industry as yours.

Vellani and Nahoun rate CFS data more valuable than any other—except your own security incident reports—because no other data are as complete or detailed. Thus, security directors can use CFS to: (1) Approach security countermeasures holistically, such as considering reports of “suspicious persons” in addition to reports of crime; and (2) correlate crimes by their specific location, time, day of the week, and so on. CFS are generally available from local police departments at a reasonable cost, note the authors.

“In conjunction with the more concentrated CFS, the UCR allows for strong comparisons: property to city/county, property to state, and property to property,” note Vellani and Nahoun. All these comparisons are extremely useful for benchmarking your property and may lead to discovering what other properties are doing to reduce calls to the police that you may be overlooking. Vellani and Nahoun remind organizations, “When using the UCR...examine violent and property crimes separately.” Addressing trends in each type of crime is important, they assert, because each poses distinct concerns to management and thus requires different levels of response.

Emerging risks

A comprehensive risk and vulnerability assessment is critical for establishing suitable goals and objectives for a violence prevention program. It also provides a foundation for considering emerging threats. An organization that fully understands how protected its workplace is against violence can more easily determine if new trends alter its risk profile, and, if so, can react more quickly and with greater confidence.

Myriad events and economic factors can influence an organization’s level of risk. For example, employees who transport precious metals are now at greater risk of being robbed because prices have increased; a shooting at an educational institution can increase the risk
at other schools in the short term because of copycats; and the current economic downturn is increasing shoplifting, which can raise the risk to retail staff as they confront thieves.

Although individual news stories can’t provide—and may obscure—an accurate portrait of workplace violence, it’s important for workplace violence prevention teams to monitor media reports for early warning about events or trends that may need to be addressed. For example, news reports have noted an increase in the number of customers, frustrated at the surge in the price of gasoline, verbally abusing and even assaulting gas station attendants. Although based solely on anecdotes, this type of report can alert a violence prevention team that it might be a good time to send out a workplace violence reminder or take some other corrective action.

Other trends and workplace developments alter the risk for all employers. Some current issues to include in today’s risk assessments:

- Workplace suicides have been up by more than 25 percent in recent years—a reminder to companies that the threat needs to be included in the workplace violence prevention effort. Although a worker who is violent to others may result in more victims, an employee’s suicide at work can have a serious and long-lasting effect on employees’ psyches. Experts note that the act of carrying out a suicide at work is a clear indication of problems in the work environment, one that can portend other violent and disruptive behavior.

- A recent examination of the causes and effects of workplace violence and bullying concludes “racial discrimination continues to be an issue as the workplace becomes increasingly diverse with the inclusion of more ethnically dissimilar individuals.” It cites results from the National Victimization Project that discovered—of workplace bullying victims who were confident they knew the motivation behind their mistreatment—39 percent stated that racial bias was “the unequivocal catalyst.” (“Occupational Stressors and Antinormative Behavior,” Sameer Hinduja, Department of Criminology and Criminal Justice, Florida Atlantic University, Security Journal, 2007.)

- In combination with the sluggish economy, layoffs and firings may be more likely to trigger violence. Employees who face other economic stresses, such as a spouse who was also recently downsized or foreclosure on their home, are more likely to respond aggressively to the news.

- New mobile technology continues to fuel an increase in remote and field workers, which alters risk by placing workers outside of the controlled security environment of the traditional workplace. Company downsizing and the shuttering of facilities increases security risks faced by solitary or small groups of workers who remain at closed plants for cleanup and removal.

- Some employees returning from military deployment may have difficulty readjusting to the civilian workplace. Some 300,000 service members deployed to Iraq and Afghanistan are struggling with post-traumatic stress disorder or major depression, according to a study by the Rand Corporation. (“Invisible Wounds of War: Psychological and Cognitive Injuries, Their Consequences, and Services to Assist Recovery,” April 2008.)
H. Michael Peter, a clinical psychologist and retired military member in Binghamton, N.Y., says veterans or service members who are experiencing trouble coping might be more volatile and prone to outbursts at work. Some service members who work in a civilian environment “have tremendous contempt for civilians because they don’t appear to work very hard,” Peter says. “If they see slacking, they end up with emotional reactions to their coworkers. That kind of thing is going to happen a lot for young men and women coming back from Afghanistan and Iraq.”

B. Program Development

If your organization has done nothing to formally address the issue of workplace violence, it is not alone. In 2005, the U.S. Department of Labor’s Bureau of Labor Statistics conducted a “Survey of Workplace Violence Prevention” of 7.1 million private industry business establishments. What it found was shocking: “Over 70 percent of United States workplaces do not have a formal program or policy that addresses workplace violence.”

Often, when a company does address the issue, workplace violence prevention begins and ends with a workplace violence prevention policy. “Far fewer organizations, by a long stretch, have a well-developed program with a trained incident management team and a refined procedure for handling reports of threats and violence,” says attorney Rebecca Speer, principal of Speer Associates (www.workplacelaw.com), an employment law firm in San Francisco that specializes in workplace violence prevention.

Research shows that a comprehensive workplace violence prevention program is the most effective way to reduce risk, and the connections that this report reveals between the different causes and solutions of workplace violence should steer organizations toward adopting

**The Airborne Express Comprehensive Prevention Model**

Airborne Express has made violence prevention a corporate priority, but rather than a few specific security measures, the organization attributes its success to a seven-pronged approach. Airborne’s chairman and CEO explained it in an address on workplace violence to a Congressional subcommittee:

1. A strict zero-tolerance policy with regard to any act or threat of violence made by an employee, violations of which make the employee immediately subject to discipline, up to and including termination, regardless of that employee’s position or seniority within the company.

2. Background screening featuring a seven-year criminal background check; a 10-year previous employment check; a 10-year previous residency check; a five-year credit history check; and a three-year motor vehicle records check.

3. Drug testing at the time of hire and random drug and alcohol testing for those in safety-sensitive positions.

4. Physical security measures to enhance personal security, including guards, restricted entrances, bright lighting, key cards, alarms, and various types of surveillance systems.

5. A strict no-weapons policy.

6. A consistent termination policy.

7. A crisis-management program specifically designed to respond to any incident or threat of violence made by or against an employee.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

a holistic approach. A prevention program provides the necessary mechanism for addressing the many facets of violence prevention—from physical security to threat management to incident response—and it helps ensure that there is a well-coordinated response to risks and incidents across many organizational disciplines.

Speaking at the 2008 International Security Conference (West), security consultant Richard Sem suggested that hit-and-miss programs could pose a real danger. They provide a company with a false sense that it is addressing problems, while threats go unnoticed. He suggested, for a start, that companies might want to look at their handling of sexual harassment. Companies often have prevention programs targeting this specific threat that are more comprehensive. “Today, I often see workplaces with good sexual harassment programs and a real need to bring workplace violence up to the same level,” said Sem.

He says it is common for workers to know that—regardless of the culture—they can’t get away with making sexually inappropriate comments, but that in the same workplace, yelling or bullying behavior is tacitly tolerated. “The [violence prevention] program needs to have the same employee involvement, awareness, ownership, duty to report, and clear lines of reporting. And just like with sexual harassment, a supervisor needs to know that if an issue gets raised, it can’t be ignored.”

This report describes in detail aspects of violence prevention that a comprehensive program will incorporate. More generally, there are principle components to an effective program for preventing workplace violence:

- Management commitment and employee involvement.
- Risk and vulnerability assessment and worksite analysis.
- Implementation of measures for prevention, mitigation, and response.
- Staff training.
- Recordkeeping and program evaluation.

Team approach

When IOMA asked more than one dozen experts on workplace violence to identify the most frequent mistake that organizations make with respect to the prevention and handling of workplace violence, the error identified most often was the use of a single department or individual (or no one at all) to address the issue, rather than the use of an interdisciplinary team.

When a team addresses the issue of workplace violence, “You get perspectives that individuals or single departments won’t have,” says Stephen Doherty, a workplace violence consultant (Doherty Partners, LLC). Time and again, case studies of successful prevention programs show that an interdisciplinary team is the very best way to administer the many necessary elements that comprise an effective and comprehensive program to prevent workplace violence.
In October 2009, IOMA/SDR conducted a national survey on corporate security management, policy, and practices. Several questions focused on companies’ management of workplace violence, and the results suggest that interdisciplinary teams are not used often enough.

Overall, 42 percent of corporate security executives say their organization utilizes a team to plan and coordinate violence prevention activities. Professional business and financial firms most commonly use such teams, while only 25 percent of retail companies and 17 percent of entertainment facilities (e.g., casino, hotel, sports venue) have a cross-functional group managing the threat of workplace violence (see Figure 10). Large employers (with more than 5,000 employees) are more than twice as likely to have a workplace violence prevention team as smaller employers (with fewer than 1,000 workers)—54 percent to 25 percent.

(If a company chooses not to use a team or committee approach, the department charged with violence prevention must still work to ensure participation from all stakeholders, including both management and frontline employees, as well as implement the program activities described in this section.)

Team members. When addressing workplace violence through a team or committee, members will vary by the type and size of organization. Typically, however, representatives come from the following functional areas:

- Senior management.
- Union or employee representative(s).
- Human resources.
- Security.
- Health and safety.
- Legal.
- Finance.
- Operations.
- Employee assistance.
Subcommittees. In additional to establishing an interdisciplinary team to administer the program, IOMA research suggests that it is also useful to join representatives from different parts of the company to form security subcommittees focused on individual security challenges and solutions. For example, a subcommittee could examine parking area security or how to protect employees who work late.

These days, a subcommittee might need to assess the impact of budget cuts on workplace violence prevention activities and develop creative ways to improve violence prevention with fewer funds. A study conducted by IOMA Research found that 39 percent of organizations spent less on security in 2009 than they did in 2008.

IOMA research shows that companies that employ a subcommittee strategy are more likely to reduce security incidents. Given that most companies wait until security incidents have grown troublesome before forming specific security committees, we think it’s telling that companies using issue-specific committees report fewer incidents.

Departmental coordination. If an organization does not utilize an interdisciplinary team to implement the violence prevention program, it must focus on improving departmental coordination between those who manage workplace violence (typically the HR department) and those who have expertise in preventing it (the security department, security contract firm, or consultant).

They must work closely together to share information and expertise. For example, human resources is often in a better position to know about general behavior trends in the organization or whether (and where) conflict is a growing or shrinking concern. It must relay that information to the security department so that it can adjust physical safeguards appropriately and conduct monitoring in accordance with the current threat environment. In short, there must be an ongoing information exchange between those employees who know about “people problems” and those charged with implementing security controls to prevent those problems from becoming security events.

Also, because departing employees are often more forthcoming than existing employees about bullying and other problems they experienced or witnessed, human resources should inquire about workplace tension and conflict when conducting exit interviews. But a company

FROM THE FIELD...

HR Managers Feel Ill-Prepared to Handle Workplace Violence Duties

It is important for organizations to consider whether the individuals currently in charge of workplace violence prevention have the skills to do the job effectively.

The American Society of Safety Engineers (www.asse.org) asked human resources professionals whether they had felt “inadequately prepared” while dealing with a workplace violence issue in the past year—and more than half said they did. The problem is acute at large companies. Of HR managers in charge of the workplace violence function at firms with more than 5,000 workers, a whopping 65 percent said they felt inadequately prepared for things they faced.

Steve Millwee, former ASIS International president and president and CEO of SecurTest (www.securtest.com), a national crisis management and background screening firm, says he sees it all the time. “HR pros are scared to death,” he says.
can only transform that important information into a safer workplace if those in human resources relate what they learn in exit interviews to the security department.

In turn, a security department needs to extend to human resources its expertise to help them meet the security challenges of violence prevention. Assistance can come in many forms, such as providing support in terminations of a potentially violent employee or sharing professional contacts in the area of threat management and law enforcement. A security team might also conduct due diligence investigations to help the HR department select and screen vendors who perform preemployment background checks, and provide training to HR staff on how to conduct investigative interviews and recognize verbal cues and body language for signs of deception.

Additionally, it’s important to treat workplace violence within the context of worker safety and not just as a security or human resources issue, which ensures that incidents travel the same rigorous accident investigation process as an injury caused by, say, a malfunctioning machine. This results in the safety committee conducting a root-cause analysis for every event, rather than merely an annual workplace violence audit, and also improves the odds of controls being put in place that do not specifically address HR or security concerns. For example, an OSHA investigation in 2007 of a psychiatric facility found that unsecured items were posing a real threat to workers, including television equipment, chairs, and tables. Treating violence prevention as an occupational safety issue also helps it take its rightful place alongside other workplace safety-training topics.

Program activities

The workplace violence prevention team—or, in the absence of a team, the department in charge—is responsible for implementing elements of the workplace violence prevention program. A full description of those elements is indicated in the recommendations and action items described throughout this report. At a minimum, workplace violence prevention programs should:

1. Create, disseminate, and update as needed the organization’s policy on workplace violence and weapons in the workplace, and ensure it is disseminated to everyone who
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

needs to know about it (managers, supervisors, line workers, clients, contractors, temporary employees, visitors, etc.).

2. Develop and promote an incident reporting structure so employees (and others) have a mechanism for reporting incidents and threats of violence. The system should include a way for employees to give confidential information concerning threats or other dangers. A system for recording incidents should be developed to permit the assessment of risk and the tracking and trending of incidents.

3. Assess the current plan for maintaining security in the workplace and identify any additional opportunities to prevent and mitigate acts of violence. This includes conducting or contracting a written, extensive workplace violence risk and vulnerability assessment; concluding a job analysis to identify workers at highest risk of violence; coordinating with law enforcement; and identifying security technology and devices that can improve the safety of workers.

4. Prepare a threat management plan to outline the process the organization will follow in the wake of a threat, violent act, or behavior suggestive of a potential problem. Activities that need to be carried out include: designating personnel who will be on the threat management team, ensuring all persons assigned to the team receive appropriate training, developing a relationship with external threat specialists and law enforcement and coordinating with them as needed, developing a crisis response plan that details how the company will respond during and after a violent incident, and conducting tabletop exercises to practice handling an incident.

5. Assign responsibility and authority for the program to individuals or teams and provide them with the training, skills, and resources they need to implement the program. This includes necessary training for all members of the workplace violence prevention teams and the general employee population in accordance with their responsibilities and risk factors, such as providing appropriate personnel with conflict resolution training. This should include a mechanism for tracking employee and supervisor training to ensure refresher training is conducted on schedule.

6. Conduct periodic assessments of the workplace violence prevention program, its progress, deficiencies, and opportunities for improvement. Teams should meet at least twice a year to review incidents, analyze patterns, and develop solutions. Formal program reviews—to evaluate the success of the program against established performance measures and eliminate aspects of the program that are not working—should be conducted at least annually. The team should also adhere to a schedule for reporting to the CEO and executive management on the successes and challenges facing the workplace violence prevention team.

Workplace violence prevention teams (or the department in charge) also frequently perform the following functions:

- Gather workplace data to focus the organization’s violence prevention efforts.
- Conduct perception surveys of employees to identify attitudes and needs.
- Solicit help from local law enforcement, such as training presentations or crime assessments.
• Establish a liaison with experts who may need to be called upon to support the program, such as police agencies, expert legal counsel, and consultants in the area of threat management.

• Manage communications following incidents (media relations, internal communications, rumor control, contact with families of victims, and customers and suppliers, if necessary).

• Review security procedures in light of an incident.

• Make determinations about workers’ fitness for duty.

• Manage victim assistance in the wake of a crisis.

C. Policies

A written workplace violence policy, one that clearly defines a company’s definition and is communicated to employees, is one of the most basic elements of preventing workplace violence.

It has become commonplace for organizations that have dedicated security personnel to have a written policy covering workplace violence, according to an IOMA/SDR benchmark survey conducted at the end of 2009 of company security representatives. Overall, 96 percent of these organizations say they have a workplace violence policy. By comparison, in IOMA’s national security management survey conducted in 2001, 23 percent of companies reported not having a written workplace violence policy.

Still, the IOMA/SDR survey found that 4.4 percent of organizations with more than 5,000 employees and 5.4 percent of publicly traded corporations do not have a basic written policy in place (see Figure 11). Additionally, data from the U.S. Department of Labor—which surveyed U.S. establishments regardless of whether they have staff dedicated to safety and security—shows that most small companies do not have a written policy. Only 20 percent of businesses in the U.S. with 10 or less employees communicate a workplace violence policy (written or verbal) to workers.

How an organization defines “workplace violence” lies at the very heart of its response to the issue. Some companies limit their definition of workplace violence to

| Figure 11. Organizations Lacking a Written Policy on Workplace Violence by Size and Type, 2010 |
|---|---|
| **Number of employees** |  |
| Less than 1,000 | 5.5% |
| 1,001 to 5,000 | 1.5% |
| More than 5,000 | 4.4% |
| **Type of organization** |  |
| Non-governmental, not-for-profit | 6.1% |
| For profit, privately owned | 2.4% |
| Publicly traded | 5.4% |
| Government/Public service | 3.3% |
| Overall | 4.1% |

(Source: IOMA/SDR Survey on Corporate Security Management, Policy & Practices)
physical assaults, while others include direct threats, and still others consider generalized hostility to be a form of workplace violence.

Besides serving as the foundation for employee discipline (it’s hard to punish an employee when no policy exists for them to violate), organizations that possess a written policy are addressing workplace violence more effectively than those that don’t, according to IOMA research. Annual studies have shown that companies with a workplace violence policy are reducing their number of incidents faster than those without.

Written policies on workplace violence should be very specific and clearly worded, spell out the definition of workplace violence, specify unacceptable behaviors, and explain what can happen to employees who exhibit certain behaviors. “It also should outline what employees can do, where to go, and who to contact,” advises Mark Braverman, a consultant who works on workplace violence issues at the Braverman Group (www.bravermangroup.com). He added that a policy should also include language that reassures employees that it is safe to report information without fear of retaliation. Some additional recommendations:

- Provide a clear definition of the spectrum of workplace violence. Prohibiting “violence” or “threats” is not explicit enough. Companies should include definitions in their policy because employees will otherwise make distinctions on their own. For example, one employee may see shouting or throwing objects as a violent act while others may see it as “blowing off steam.”

- Identify and delineate in the policy employee responsibilities for reporting violations of company policy.

- Clearly outline the organization’s policy toward the possession of weapons on company property and while on company business off of company property.

- Provide awareness training to employees on the organization’s workplace violence policy. Periodically provide refresher training.

FROM THE FIELD...

Perceptions Vary on What Constitutes Workplace Violence

A clear and communicated workplace violence policy is critical for getting everyone on the same page about exactly what workplace violence is. Left on their own, workers have vastly different interpretations of it.

A study by Doherty Partners LLC is one of several to show that managers feel substantially safer than line workers, and that male workers and female workers often view identical incidents differently. Some examples:

- If a coworker has an argument with a spouse or family member at work, 77 percent of female workers perceive it as an act of workplace violence compared to 54 percent of men.

- If a client has an outburst, 44 percent of women but only 25 percent of men see it as workplace violence.

- If a coworker were to bring a weapon to work, 90 percent of women said they would think of it as workplace violence compared to 79 percent of men.

The results affirm how critical it is for an organization to educate employees on its definition of workplace violence and the range of incidents it wants employees to report.
• Review organizational policies relative to workplace violence annually (including weapons or other related policies) for relevancy and effectiveness, and to make changes as necessary.

Zero tolerance

Zero tolerance policies have emerged as a popular strategy to prevent workplace violence and take a logical approach to keeping workers safe from violence.

1. Develop and promote a very strict set of rules governing behavior.
2. Punish any deviation swiftly and severely.
3. Fearing punishment, workers will follow the rules.

Not everyone is a fan of so-called “zero tolerance” wording in corporate policies. Security consultant and author Joseph Kinney (Kinney Security), warns that companies can end up restricting their options and, in the wake of incident, having to choose between firing an employee or ignoring it altogether. He advises eschewing language that is too black and white so a company can have flexibility in identifying the most appropriate solution given the nature of the particular threat or incident.

Bonnie Michelman, former ASIS International President and Director of Police, Security, and Outside Services at Massachusetts General Hospital, told IOMA that she has changed her tune about zero tolerance policies. “I don’t think they are always desirable. There may be occasions when you do tolerate some behavior if you are certain it’s a one-time thing,” she says. Former police chief and security consultant Stephen Doherty also warns that zero tolerance can act as a barrier to complete reporting.

Barry Nixon, executive director for the National Institute for the Prevention of Workplace Violence Inc., is another expert who thinks a focus on zero tolerance is misguided. Organizations adopt such policies because “they sound good,” he said, speaking at the 2010 iSecurity online trade show and conference. “They say, ‘we won’t tolerate this behavior’ under the presumption that it will eliminate the issue, but that is not what we have found.”

An Alternative to a Zero-Tolerance Focus

Promote a zero-incidents approach rather than zero tolerance, suggested Barry Nixon, executive director for the National Institute for the Prevention of Workplace Violence Inc., at a recent security conference. Doing so focuses employees, the security department or the violence prevention team, and management on all the activities that must be taken at many points along the prevention continuum.

1. Detect: focus on identifying and anticipating possible problematic situations before issues actually erupt, bolster employee reporting tools, and educate on warning signs.
2. Prevent: prepare before an incident occurs. Take reports and signs seriously, teach employees and supervisors how to stay calm, intervene to disrupt escalation cycles, and focus on individual and organizational levels.
3. Protect: focus on protecting employees by putting your crisis response plan into motion, take immediate action, and continuously improve your prevention and response plans.
Nixon believes there is a fundamental problem with zero-tolerance policies. “They tend to be reactive in nature. ‘If this behavior occurs, this is what we’ll do.’” He cited an excerpt from an actual corporate workplace violence policy to illustrate: “The intent of this policy is to increase employee awareness of the procedures to be followed in the event of workplace violence.” Nixon and other experts say a program’s focus should be on prevention, not how aggressively it will punish policy violators.

He advocated a “zero-incidents” approach instead, because it puts the emphasis on preventing unwanted behavior rather than describing how the organization will respond to it. “Zero tolerance implies that you won’t put up with it once it happens, whereas zero incidents puts the focus on preventative measures,” Nixon said.

He shared another policy excerpt from a company that he thinks is doing it right: “It is our company’s intent to create a work environment where all employees are safe and secure from hazards,” the policy begins.

“...To ensure this happens, we are placing a high priority on implementing practices and procedures that prevent work violence, and strongly encourage the support of all employees in helping us to create an accident- and hazard-free environment.”

Some workplace surveys have found that a majority of companies with a workplace violence policy include “zero tolerance”—resulting in immediate termination—for employees who commit an act of violence, and roughly half of companies have zero tolerance/termination for threats of violence. Wherever an organization decides to draw the line, companies should recognize that, by itself, a zero tolerance policy is not a solution. Unless companies reinforce it with a comprehensive program, a clear set of standards for what behavior is off-limits, and progressive discipline to accompany it, the idea can fall flat. “It sends up red flags for people; workers become afraid that even casual remarks can get them fired,” warns Lynn Jenkins, a senior scientist at the National Institute for Occupational Safety and Health (www.cdc/niosh).

If a company chooses to include zero tolerance language in their workplace violence policy, it must do so carefully. A government review of the zero tolerance policy in use at the United States Postal Service found that it was causing problems because it had not been clearly defined. Too many workers did not understand the policy and some supervisors did not know the appropriate disciplinary responses, the audit noted.

Also, if employees don’t believe their company’s zero tolerance policy is fair, it can backfire by discouraging them from reporting small incidents or causing punished individuals to retaliate and seek revenge. Both situations can turn small incidents into potentially explosive situations. In the first case, companies will fail to receive a crucial alert to a potentially violent employee. In the other, an organization might push a troubled employee toward a significant act of violence over a relatively insignificant issue.

**Employee acceptence**

The key to any successful workplace violence prevention strategy—whether it’s based on zero tolerance or not—is for employees to perceive it as fair, according to Thomas Germano,
former director of the Long Island District of Cornell University’s School of Industrial and Labor Relations. The following steps help ensure that they will:

1. **Participatory policy development.** Management representatives—such as HR, safety, and security—should work together with high-level labor representatives to develop the policies designed to deal with external and internal threats to workers’ well-being. The mutual goal should be to design policies that “have teeth,” but that employees still regard as fair, says Germano. In unionized workplaces, union representatives must be involved in the formation or review of workplace violence policies. Policies developed without union input will have little credibility with employees.

2. **Adequate policy promotion.** Once policies are in place it’s up to the members of the workplace violence prevention committee to create awareness of them. Education is a crucial step in the violence prevention program that many companies ignore.

3. **Training for individuals who enforce policies.** Supervisors, HR personnel, and violence prevention team members need to have the skills to administer the policies because it is often easier to ignore someone who is behaving erratically than to challenge them, Germano explained. “No one wants to be the bad person, to be judgmental,” and it also can be frightening to confront an individual who is behaving inappropriately, he notes. Only trained people are capable of making the hard decision of removing a person from the workforce or of sending them for the help they need, he says.

4. **Simultaneous healthy workplace initiatives.** To be fair to workers, companies that stress workplace violence prevention also need to work on eliminating those workplace characteristics that are known to create an environment in which acts of worker-on-worker violence are more likely to occur. These include chronic labor-management disputes, job instability, overwork, and excessive overtime.

**Enforcement**

Basing a policy on progressive discipline—as opposed to zero tolerance and a one-punishment-fits-all approach—goes a long way towards getting workers to see it as fair. Progressive discipline is not about giving individuals free passes to break the rules a few times before
you impose the punishment. For example, if a supervisor allows an employee to use foul language twice without punishment and then issues a suspension for the third offense, two preventable infractions occurred. Rather, progressive discipline:

- Makes the level of punishment suitable given the offense.
- Includes any mitigating circumstances.
- Considers the record of the employee involved.

Giving due process to employees charged with violence or threatening violence is another critical aspect of an effective workplace safety policy. It is also one that can be lost amid the zeal to root out potential troublemakers. Elements of due process:

- Strictly adhere to your progressive discipline rules in all cases. Policies must be applied equally to both managerial and non-managerial employees or they will create labor/management conflict.
- Witnesses, including the alleged perpetrator, are given adequate opportunity to express their view of the incident.
- Before discipline is determined, take into account mitigating circumstances—such as instigation of a dispute by someone other than the employee.

Adequate due process also includes intervening on behalf of employees who need counseling. And companies have an obligation to follow-up the cases they refer to counselors. When an employee is sent for counseling because of a work-related problem, the employer needs to work with the therapist to ensure that the therapist is fully informed about how the employee is doing after he or she returns to the workplace.

**Weapons**

The presence of weapons in the workplace environment increases the danger to employees, and most large companies have a policy restricting the bringing of weapons into the workplace.

Of companies with policies, most are a broad prohibition against all objects and agents that could be considered weapons. Only 11 percent of company policies permit employee-owned weapons on organization premises, and more than half of these restrict weapons to employee vehicles.

Overall, one in four companies say they dealt with a weapons policy violation, and surveys indicate that companies have more trouble enforcing weapons policies among site employees than among customers, visitors, temporary

---

**Figure 12. Formal Workplace Weapons Policy by Size of Organization, 2006**

(Source: Society for Human Resource Management)
workers, and vendors. Companies can encourage compliance by taking the following measures:

- Write the weapons policy in plain, clear language, and make it applicable to everyone. Review the policy for ambiguous language such as “no unauthorized weapons,” which employees with carrying-concealed-weapons licenses can misinterpret.

- Define terms in a “definitions” section to eliminate possible confusion over words and phrases used in the company policy, such as “weapon” and “company property.”

- Develop strategies (that fit the type of business) for disseminating the policy as widely as possible. The most common strategies are: include it in an employee handbook; discuss it during new-employee orientation; post it on the company Intranet or other electronic...
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

medium; post it at building entry points; discuss it during staff meetings or organization-wide meetings; post it in break rooms, at the entrance to parking areas, and in company-owned vehicles.

- Specify that any employee who brings a weapon to the workplace in violation of the company’s policy is subject to disciplinary action, up to and including termination.

- Review the weapons-in-the-workplace policy with employees and require signed, written acknowledgment that they reviewed and understood it.

- Provide employees with notification of the company’s search policy, obtain signatures that they’ve read and understood it, and specifically reserve the right of the organization (and contract security services) to search employees’ offices, desks, cabinets, and lockers, whether locked or not, automobiles parked on company premises, pockets, purses, briefcases, and similar places.

- Monitor workers’ attitudes toward their safety at work and undertake strategies to encourage employees to report any fears or security concerns. (Otherwise, workers who feel threatened at work may feel the need to defend themselves by bringing weapons into the workplace.)

Guns-at-work policy restrictions. Increasingly, states are restricting employers from writing weapons policies that include employee vehicles, regardless of whether they are on company property. Indiana enacted such a law in 2010 to join 12 other states with similar laws: Alaska, Arizona, Florida, Georgia, Kansas, Kentucky, Louisiana, Minnesota, Mississippi, Nebraska, Oklahoma, and Utah. Most of these laws have been passed in the last five years, and it’s not the only way in which property owners’ rights are being overridden by the Second Amendment rights of individuals.

In 2010, Georgia’s House of Representatives passed a bill that would allow registered gun owners to bring weapons into areas of Georgia airports not controlled by the federal government, for example. The battle is even being waged on college campuses where, since the Virginia Tech shooting in 2007, students have started to demand the right to protect themselves by carrying a gun on campus if they are properly licensed. Some schools have acquiesced. For example, Blue Ridge Community College, a state school in Virginia, allows students with concealed-weapons permits to carry guns on campus. Elsewhere, a bill passed the Kansas House of Representatives that would allow individuals with a conceal-carry license to bring firearms on college campuses.

The fight is likely to intensify further, according to Jack Lichtenstein, director of government affairs and public policy for ASIS International. He warns that gun activists will continue to take aim at the rights of property owners wherever states are sympathetic to their cause. “They are politically powerful, they want ‘forced entry’ of firearms to be the law of the land, and they will continue to work to have these laws passed wherever they can.”

Advocates are working state-by-state to enact so-called guns-at-work laws, and Florida is one of the states where they had success. Its recently passed law makes it a privacy violation to even ask employees—or customers or invitees to the company, who also are covered by
the measure—whether they have firearms in their cars. It also bars employers from discriminating against employees (including independent contractors, volunteers, and interns) for having a concealed weapons permit.

Organizations in affected states should also review their workplace security measures to assess whether changes are necessary to mitigate the risk from guns in cars on company property. The Proskauer Rose law firm recommends that companies conduct awareness training for security staff and supervisors to alert them to the enhanced risk that the presence of guns might bring.

“People are going to get hurt,” said Allan Weitzman, a partner at Proskauer Rose LLP. “The law has created a situation where there’s going to be a cooling-off period of 30 seconds,” he said. Meaning, rather than an evening back at home, an irate worker could retrieve a weapon immediately from the car.

Michael Mantell, author of Ticking Bombs: Defusing Violence in the Workplace, agrees that the availability of guns in the company parking lot ups the ante for violent acts. “It allows for an increase in the severity you might see in any incident of violence,” said Mantell. “If a person has access to a gun, he or she might use it instead of a punch.” As a precaution, some companies may be installing gun detectors on the premises, Weitzman said.

For crafting weapons policies in light of these new laws, consult section IV, Legal/Regulatory Considerations (item “C,” Policies).

Managing ‘open carry.’ Section IV also details considerations for dealing with a fledgling movement called “open carry,” which encourages licensed gun carriers to wear their firearms proudly as they go about their business—whether stopping in Starbucks for coffee or looking for bargains at Wal-Mart. Opencarry.org, a group based in Virginia, claims thousands of members nationwide. Although the movement does not affect the right of companies to craft policies of their choosing, it does raise practical questions about enforcing them.

At least 29 states grant licensed individuals the right to carry a handgun, and in most of these—as the result of an expansion of gun rights over the last decade—individuals do not need to demonstrate a “need to carry.” They only need the desire to carry a gun and the ability to pass the state’s licensing requirements (usually a background check and safety testing).

While these individuals may be extremely law abiding, the prospect of people moving their firearm from under their jacket to their hip raises important security questions: What should staff members do if someone walks in wearing a gun? Do they know? What if a frightened customer complains? Do staff members understand how to proceed if an individual wearing a gun refuses to leave the premises? Do they know what legal recourse they have?

Retailers and their front-line workers are being caught in the battle as advocates of “open carry” have stepped up their campaign to promote gun ownership and gun rights. Although businesses can generally restrict guns being brought on their property with signs notifying patrons that it is not allowed, this new crop of gun advocate is testing where companies stand on the issue by openly carrying guns into stores like Starbucks, Wal-Mart, and other high-profile retail chains.
Companies have traditionally been able to avoid the issue, but because of this new campaign they must decide how they want to approach the issue of customers who want to openly carry a gun into their establishment. Starbucks, for example, has been ground zero of the controversy. Its stance not to ban guns from its stores has pleased gun owners but angered some employees and customers, who have started a petition campaign to get the company to change its policy. On the other hand, establishments that ban firearms, like California Pizza Kitchen, now face a boycott campaign by gun advocates.

The issue is quickly becoming unavoidable. Companies that have not crafted a specific policy need to do so, as well as train line staff on how they want them to respond in different scenarios.

**D. Background Screening**

One prevention strategy recommended unanimously by workplace violence prevention specialists—especially for preventing employee-on-employee violence—is to develop and maintain a rigorous employee screening process that prevents “putting problems on the payroll.”

A careful criminal history records check is the minimum requirement. There are many additional options, such as work history verification, including previous places of employment and lengths of stay; educational background verification; personal and professional references; license or certification verification; motor vehicles records check; credit record checks; drug screening; and personality testing.

Data from background checks suggest why they are so important. Based on 1.7 million individual background checks completed by ADP in the 2008 calendar year, 6 percent revealed a criminal record in the past seven years. In select industries, nearly one in 10 applicants has a recent criminal record (see Figure 14).

Barry Nixon, executive director for the National Institute for the Prevention of Workplace Violence Inc., believes background checks can be used to improve the safety of the workplace just as drug screening helps discourage illegal substance use. Companies routinely inform potential employees that they will need to pass a drug screen; doing so helps shape their view of the organization as a place where rules are paramount and helps to turn away undesirable job seekers. Nixon suggested that organizations should

*Source: ADP 2009 Hiring Index Whitepaper*
similarly issue a proclamation to job seekers regarding workplace violence. A company should state this up front:

1. We assess all candidates for violence-prone behavior.
2. We conduct background and reference checks on all applicants.
3. We will not tolerate any form of violence, threats, mobbing, bullying, and other behaviors that imply intent to harm anyone, and we deal with all violations firmly.

Raising the issue of workplace violence in the prehire stage warns workers that yours is not a permissive or rough-and-tumble environment where aggressive behavior is tolerated, and it establishes a clear expectation for appropriate behavior.

Background checks have become easier and cheaper to conduct, and more common as a result. A survey of security and HR professionals found that 85 percent perform Social Security number checks and criminal records checks (HireRight Background Screening Benchmarking Report 2008).

Most respondents verify education information in background checks (93 percent), 88 percent verify employment information, 68 percent check driving records (68 percent), and 67 percent conduct drug testing. Less common screenings include credit checks (36 percent), license verifications (28 percent), reference checks (27 percent), military records (19 percent), sanctions checks (18 percent), and social networks (13 percent). The IOMA/SDR on security policies and practices found that 19 percent of organizations conduct personality testing of new hires (see Figure 15).

Although screening is now more common, gaps exist that could impact workplace safety. Job applicants are five times more likely to be screened than current employees, for example. And the “extended workforce,” including consultants, contract labor, and temporary and vendor personnel, are screened one-third as often as permanent, full-time workers.

The extent of a company’s background screening should be tailored to the sensitivity of the position. For example, will the employee be operating a vehicle on behalf of the company? Will the employee be handling money? Will the employee have exposure to vulnerable populations (the elderly, children)?

Although not one-size-fits-all, the background check process used by Airborne Express represents a general best-practice approach for screening out unwanted employees, especially those who may pose a threat to others. They conduct a:
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

- Seven-year criminal background check.
- 10-year previous employment check.
- 10-year previous residency check.
- Five-year credit history check.
- Three-year motor vehicle records check.

Conducting screening

All reputable workplace violence prevention programs will ensure that the organization conducts sufficient background screening to avoid hiring individuals with a history of violent workplace acts. However, it is a myth that a quick pre-employment check will weed out potential troublemakers.

“One of the most important things we can do [to prevent workplace violence] is to do background checks, but the quality of the background check makes a big difference,” warns Bonnie Michelman, Director of Police, Security, and Outside Services at Massachusetts General Hospital. She says that conducting a background check could provide a false sense of security unless it digs deep enough. “People who have [done violent acts] move to new states,” she says. “Personal references aren’t very salient. Be more subtle. Look at gaps in employment, ask unusual questions about handling stress, investigate.”

Craig Kessler, CEO of www.backgroundchecks.com, an online employee investigations firm, sounds a similar warning. Because applicants know that many companies only conduct a criminal conviction check in a single county, usually the county in which the employer is located, they simply cross state lines when looking for work. “Plain and simple, they know the game,” Kessler warned.

Violence Prevention Doesn’t End With Pre-Hire Screening

In March 2007, at a printing plant in California, a 67-year-old veteran employee went to work one morning and shot three coworkers because management had scaled back his hours. He then shot himself before the SWAT team arrived. Just days later, at Johnson Space Center, a disgruntled 60-year-old worker committed a murder-suicide after receiving an e-mail from his employer outlining deficiencies in his job performance.

These incidents are somewhat typical of employee-on-employee shootings in that a negative work event sparked an incident involving a long-time employee. They also highlight the limitations of pre-hire screening to prevent workplace violence.

In IOMA’s survey of company hiring procedures, several respondents said that—in terms of preventing violent security incidents—their background screening process has moved ahead of their ability to manage potentially explosive problems involving employees post-hire. One survey respondent, the chief operating officer at a CPA firm, said that with a sufficient background screening process in place it’s important to move on to improving processes to foresee potential workplace violence involving existing employees. “We do a good job of screening candidates. What we need to focus on is managing employees and coaching [and] understanding them. We need to equip our managers in the office to handle disgruntled employees. We also need to teach our people how to recognize symptoms of problems.”

Workplace violence prevention teams should also keep in mind that the single best predictor of violence is post-hire behavior, not a pre-hire paper trail of past violence.
The first stage, which should be used with all applicants, is the interview and reference check. The second stage, appropriate for all “finalists,” involves a background search, including making sure the information on the résumé is accurate, and checking for a criminal history. And if a company thinks it is important to know about a job applicant’s possible criminal past, it should consider it important to dig deep enough to find out if such a record truly exists.

One best-practices approach is to conduct a residential history for an applicant for the past seven years and conduct criminal checks in all those counties. Screening should also include checking public and private records and use multiple tools, since relying on just one can be incomplete. And in the wake of other red flags, an employee’s history needs additional investigation to determine if there are any less obvious examples of violent behavior. Make sure your relevant team member (security, HR, outside agency) digs deeper than just court records, and investigates military records, school records, and previous work histories, and gathers information from family members or associates concerning violence or possession of and fascination with weapons.

Outsourcing. A majority of companies now contract with an outside company to perform background checks. Given that specialized providers can generally do a more complete and accurate job than HR or corporate security departments, outsourcing is a smart move for many companies. It is typically a less costly option as well—with employers now paying $108 on average, according to IOMA’s 2007 survey of hiring managers.

Not surprisingly, vendor offerings of instant checks are gaining in popularity the fastest, but experts warn that it is a false solution unless you know what is making up the body of information in that instant check database. Companies should be skeptical of vendor claims of checks of a “nationwide” criminal database. There is no true national database, despite some firms’ advertisements (although there are multijurisdiction databases). Consider them as back-up or secondary tools only, and make sure to verify “hits” for accuracy and current status on a database at the courthouse.

Companies must also inquire how often a vendor updates the databases they use to check criminal records. If it is every six months, then a company may be rejecting applicants who committed a crime four years ago in favor of an applicant who committed a violent offense...
five months ago. Additionally, a company needs to make sure that a prospective national vendor understands the particulars of its state’s law addressing background checks and can adhere to its requirements.

Applications. Trying to obtain assurance that a new hire doesn’t pose a threat begins with the wording on a job application, according to Lester Rosen, president of Employment Screening Resources (www.esrcheck.com). The job application form should include an appropriate waiver and release (permitting the employer to verify the information reported on the application) and designed to leverage violence prevention.

- Include standard questions about past criminal convictions and check for gaps in employment. This is often sufficient to prevent a company from “hiring a lawsuit” in the early stages of the application process. (Note: Make sure your application complies with state law. Effective November 4, 2010, Massachusetts became the second state—joining Hawaii—to ban both public and private employers from requesting criminal record information on initial job applications.)

- State on the application form that lying about information on the form is grounds for dismissal, no matter when it is discovered.

- Review applications carefully for red flags such as applicants who avoid questions about a criminal background, who provide no details on criminal convictions, or who “can’t remember” past supervisors.

Some companies are smartly moving to “next generation” employment application forms to facilitate the screening process. Such applications will ask for documented periods of unemployment and the e-mail addresses and Web site addresses for previous employers. These can be a big help in speeding up background checks for employees who worked abroad.

Interviews. By asking the right questions, correctly reading respondents’ answers, and employing a range of other truth-eliciting strategies, managers can support the effort of the violence prevention team by weeding out dishonest and potentially violent employees. To add this element of violence prevention, companies need to give managers the tools they need to spot potentially dishonest employees. Companies should consider providing managers with training, such as that provided by Reid & Associates (www.reid.com) on interview and interrogation techniques.

- Raise background checks during the interview. Rosen says to tell interviewees that the organization does background checks, criminal background checks, and contacts prior employers. Then ask if they have any concerns about these steps.

- Inquire about any unexplained employment gaps.

- Include mention of background checks into the written offer letter: State that the offer is contingent on the completion of a background check that is satisfactory to the employer. “Make it very clear—this is a subjective standard,” Rosen warned.

- Have post-offer procedures in place, including I-9 verification.
Social Security Number Traces. Companies that do not conduct Social Security number (SSN) traces as a routine part of employment hiring decisions are risking violence and a lawsuit, say experts. Even if the screening process consists of little else, companies need to start conducting SSN traces, and companies that do should make sure they are using them to their full advantage.

Companies should check an applicant’s SSN to get previous addresses for running county and state criminal checks. If you run a criminal check only for the areas where an applicant tells you he or she has lived, you not only risk hiring someone who is hiding a criminal past, you are not easing your liability, says Michael Cool, leader of the employee screening services unit for Acxiom Information Security Services (www.acxiominsight.com). “If you just run a criminal check of applicant-given addresses, the courts have every right to ask you where your due diligence is,” he told IOMA. Items to look for in an SSN trace:

- Does the SSN given by the applicant match the subject? If not, verify that the number was entered correctly by the credit bureau and company staff. Ask the applicant to provide proof of the SSN.

- Does the name in the results match that of the subject? The middle name/initial is important for proper identification, especially if the subject has a relatively common name. Obtain the suffix, if one is used.

- Have additional names been revealed? For example, you have Susan Smith applying for a job but she’s only been married for a year. For thirty years, she was known as Susan Thomas, but she didn’t tell you that. If this applicant were to have a criminal record under her maiden name and you didn’t check, you would not be doing your due diligence, says Cool.

- Has the number been issued by the Social Security Administration? Fakers frequently use numbers that have never been issued by the Social Security Administration. Check the SSA's number allocations. If verification shows a bogus number, ask the applicant to provide proof of their SSN.

When Filling the Job Collides With Security

In a moment of rational thinking, an organization may decide it wants to check new hires’ criminal pasts to prevent a tragic event. But immediate hiring pressures can cause organizations to put good sense aside—even when the lives of children are involved.

Florida law requires background checks of workers in child care centers, but loopholes that include “exemptions” and permitting centers to hire-first, check-later have put children in the state at risk, according to a six-month investigation by the Sun Sentinel in 2009. Thousands of workers with criminal pasts, including violent felons and individuals convicted of hurting children, were hired to work with kids; even murderers have gained exemptions, according to the investigation.

In many cases, day care operators are said to have turned a blind eye (or worse) to the sketchy past of new workers, but even when organizations have the best intentions it can be hard to keep the importance of security on the front burner. Following a reasonable protocol and auditing it routinely to make sure it is being followed is a good starting point.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

- In what state was the number issued? It is entirely possible that the number was issued in a state other than the state in which the applicant now resides, and that is not necessarily a cause for alarm. But it can be a signal to dig deeper if the applicant omitted such information, especially if they only recently moved.

- Do the addresses provided by the applicant—and the corresponding time frames—match those obtained from the verification? If not, investigate further. You may also find other addresses listed via an unmarried couple’s joint credit application. “That’s valuable information,” says Cool. You should run a criminal check for the county associated with this newly discovered address, recommends Cool.

After getting back SSN verification, ask:

- In what year was the number issued? Compare the year of issue to the applicant’s date of birth. They should be close. And if the applicant was born after 1984, they should be the same (that’s when it became mandatory to obtain an SSN for a child at birth).

- Do the past employers given by the subject—and their time frames—match those revealed by the SSN verification? If not, question the applicant about the discrepancy.

- Does the applicant-provided date of birth match up? If it is off by more than two years, ask the subject for proof of birth, preferably a birth certificate.

- Is the subject using and/or associated with more than one SSN? It could be a typo, but investigate all additional SSNs anyway.

- Are additional individuals using the same SSN? Verifications can reveal more than one individual using the same SSN. These additional individuals should be investigated. (There are several legitimate reasons for the existence of these individuals, a relative who has applied for joint credit with the applicant, for example.) If the applicant doesn’t know of these individuals, he or she should be advised to contact the credit bureau from which the information was obtained.

**Foreign workers.** Some studies have shown that companies are less likely to investigate prospective employees with foreign backgrounds than domestic workers because of difficulty and cost of obtaining background records for foreign workers. And many companies don’t dig into the backgrounds of workers when non-English speaking countries are involved.

However, if a company’s risk assessment concludes that certain record checks are important, they are important regardless of how difficult they are to obtain. While it’s smart to adjust your extent of background checking depending on the sensitivity of the position you’re filling, it’s a bad idea to adjust it because of the difficulty or expense in obtaining the information.

**Contract personnel.** Lex Holloway, manager of corporate security for Caremark, advocates extending the screening process to capture background information about temporaries, contractors, and vendors. “Anyone with unrestricted access to company facilities or information” needs to have a “pre-employment” screening and background investigation, he asserts. Vendors and service organizations whose personnel make frequent visits or spend long periods of time working at your facility should certify that those individuals meet or exceed your firm’s safety and security requirements. Conversely, contractors who assign
personnel to work at other organizations’ facilities should also consider the host firm’s safety and security policies and practices.

**Existing employees.** John Long, former president and CEO of HireCheck Inc., advises companies to add spot checks of existing employees to their screening program. Although not everyone agrees that this is necessary, companies do need a system for addressing in-house job changes. For example, one woman successfully sued a Tallahassee furniture company for $2.5 million after a deliveryman attacked her. The company had originally hired the employee as a laborer who performed odd jobs and yard work. When the worker was hired as a deliveryman the company did no additional background checks on the employee—which would have shown previous arrests for violent crimes—even though his new job called for contact with the public.

**Psychological testing/personality tests.** Psychological testing in the pre-employment process attempts to identify employees that may be prone to violence. It is worth noting, however, that some prevention professionals have little faith in such tests, and identify ways in which these tests can hamper a corporate workplace violence prevention effort:

- Testing administered and interpreted by unqualified individuals can result in disqualifying worthy job applicants.
- The time span for predicting future behavior is typically too short to be of real use to a violence prevention program.
- Profiling doesn’t recognize that almost anyone can become violent if pushed beyond a certain point.
- Without proper controls, tests can cause legal headaches.

Personality tests can be effective for screening out potentially violent employees, however, legally they “are very tricky,” according to Violence Prevention International president Dr. James Madero. “You need to have the legal department look at what you want to do,” he warned.

**Program controls**

Companies must develop standard protocols for conducting background searches, but they must also audit their programs to identify deficiencies. Problems to look out for:

- **Does your screening process include problematic disparities?** Companies should conduct checks in light of job position—and refrain from seeking information that is not job related (for example, collecting credit histories on employees who don’t have access to financial assets or driving records checks for employees who don’t drive as part of their job.) However, criminal checks need to be conducted universally. If a company conducts criminal background checks on applicants for cash handling positions but ignores similar checks for “customer service” posts, it is raising its risk of liability if an employee commits an act of violence. (It shows that you thought the checks were valuable—but only to protect your bottom line.)
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

- **Have you been specific enough in identifying your hiring standards and process?** For example, a policy can specify that investigators must obtain character references, but unless it identifies what that means, investigators will make their own decisions about what types of references are sufficient.

- **Are you systematically monitoring for shortcuts?** HR managers and vendors sometimes try to cut corners. For example, by occasionally eschewing the in-depth checks they’re supposed to do in favor of conducting a one-county criminal background check to move things along. Companies should regularly pull hiring packages to ensure that standards are being followed and that hiring pressures aren’t causing the company to fill positions before all information is in and checks have been made.

- **Have investigators been given appropriate training (and provided refresher training)?** Once you develop a set of standards for background investigations—or agree with your contract provider about what standards will be followed—ensure that investigators have been adequately trained in the standards. Companies should establish a training infrastructure that regularly updates and tracks investigators’ training. Or, if you use a contract company, check the training records of their investigators.

- **Do you audit to make sure vendors are conducting the right checks for the right workers?** Periodic quality checks can reveal that a company driver may not have received a check of his or her motor vehicle records, for example. Security departments shouldn’t assume HR will always spot (or want to spot) the error. Again, HR’s goal is to quickly and efficiently fill job openings, not double-check security details. For that matter, it’s often a good idea to make sure that HR is actually reading and using the reports that the background-check company submits.

- **Are you meeting specified goals for timeliness and quality?** What is your performance standard for how quickly background investigations must be completed? How often do you meet it? A workplace violence prevention team should conduct routine assessments of the amount of time it takes to obtain the results of background investigations and if it meets the requirement spelled out in the company’s policy or falls in line with what the vendor promised.

- **Have you established formal quality control mechanisms?** Besides conducting periodic reviews of completed background investigations, quality control includes a formal process for providing and soliciting feedback on problems associated with the background

## Background Checks Need Checks of Their Own

A recent study found that 7 percent of companies have experienced a workplace violence problem with an employee—cleared during background screening—who nonetheless had a criminal record (“Background Checking: Uncovering the Facts,” 2006, Taleo Research).

This disturbing finding makes it very clear that companies should regularly conduct an audit of their screening provider to measure the quality of background checks. However, this is something that only 29 percent of companies have ever done, according to the survey.
screening program to senior managers, investigators, trainers, and the contract company (if applicable).

- **Do you test your vendor?** Some security experts recommend sending along a name you know should be a “hit” to see if the vendor’s screening uncovers it.

- **Is your program standardized?** Formalize your employee screening process by defining, in writing, what criteria will knock out a candidate for employment—something many companies don’t do.

### E. Physical Security

Emcore is a pretty ordinary company—a manufacturer in New Mexico of about 700 employees that makes components for voice, video and data transmission over fiber-optic lines. So the “it can happen anywhere” characteristic of workplace shootings was underscored in July 2010 when a person previously employed at the Albuquerque plant forced his way into the building to go after his former girlfriend, an employee, with whom he was engaged in a child custody dispute. He shot and killed two workers and wounded several others, including his ex-girlfriend critically, before shooting himself.

There is also nothing particularly unique about Hartford Distributors, a beer distributor in Manchester, Conn., where an employee in August 2010 ran through a warehouse at the busiest time of the morning firing a gun. When the shooting spree was over, he had killed eight coworkers.

These rampage shooting events, every organization’s worst nightmare, happen quickly—typically, too fast for security personnel or law enforcement to respond. Frequently, by the time professionals arrive at the scene, the shooter has already claimed all his victims and has killed himself.

So when the worst-case scenario happens, it is unlikely to be a fast security response that mitigates the carnage. Limiting harm is more likely to depend on whether the facility where the shooting occurs effectively isolates targets from the shooter.

### FROM THE FIELD...

**What Once Seemed Draconian May Now Be Welcomed**

A report by the Milwaukee Journal Sentinel noted that robberies in the state were up 31 percent in 2008 and that one bank, a Menomonee Falls Associated branch, was hit three times in less than six months in takeover robberies, in which armed robbers ordered customers and staff to the floor.

Given the rise in robberies, evolving public perceptions about the need for security, and growing approval by customers for overt security measures, high-risk targets such as banks may want to reconsider entry systems to include a two-door secure system. An Associated bank vice president said that, after a short learning curve, customers now appreciate its new security entrance.

People enter the outside door when the system recognizes the presence of a single individual outside the bank and a green light comes on. Once inside the glass chamber and before a second door, the system reads for the presence of any large metal object. If none is detected, the door into the bank opens. If an object is detected, the individual is asked to place it in front of a camera for security to inspect from inside the bank.
In a webinar hosted by IOMA/SDR in June 2010, workplace violence consultant Felix Nater recommended to organizations that they examine how their physical buildings—in case a shooter gains entry—might more effectively hinder the shooter’s progress within the facility. “Ask yourself, ‘once in, how do we contain or minimize the impact?’ You want to deny the person the ability to hit the target, and you need to modify the workplace if you have to,” he said.

It is also critical for organizations to evaluate whether security equipment—during typical operation—is sufficient to provide warnings or situational awareness during an incident of workplace violence. Coverage by security devices such as cameras, call boxes, or panic buttons must be sufficient not only in times of optimal operation but also in the typical, actual environment—when a certain number of devices may be out of operation.

Unfortunately, when shooting events occur, a wide gap is often discovered between the security measures that were being relied upon and those in operation. For example, a commission convened to examine a December 2009 shooting incident on a Northern Virginia Community College campus said, “The college currently has an extensive security camera system” but “a startling statistic from the Woodbridge incident is that only nine of the 45 cameras were operable at the time.” It added that the current software used to run the system is not reliable, and it promised that efforts are under way to replace it.

In the wake of high-profile workplace shootings, both the mainstream and security media are eager to report on the efforts of businesses to address the danger. They find a willing partner in security firms’ PR teams that supply case studies of establishments investing in state-of-the-art security technology to prevent future violence. Businesses join in, eager to

seem proactive and calm fears by talking up new prevention measures. The reality, however, appears to be something else entirely.

Not only are companies unlikely to change because of events at other firms, the majority of establishments do not change their procedures or security measures after experiencing an incident of workplace violence, according to data collected in a special survey by the Bureau of Labor Statistics for the National Institute for Occupational Safety and Health. (“The Survey of Workplace Violence Prevention,” 2006.) The study found that of companies experiencing incident(s) in the last 12 months, only 10 percent implemented some change as a result. Only 6.6 percent of employers with more than 1,000 workers implemented change.

The data also indicate that despite the rapid advances and significant investment in security technology, most places of business remain vulnerable to determined intruders and have invested only modestly in security devices such as personal alarms for employees.

The security department or workplace violence prevention team should review the company’s security measures and procedures in the wake of incidents. It should also do so periodically to examine the applicability of new security technology. As a result of assessments, security representatives or the workplace violence prevention team should make recommendations for physical security measures that the organization can implement to reduce the likelihood of violent incidents. Recommendations may include:

- Better interior/exterior lighting.
- Alarms around the premises.
- Property fencing/gates.
- Interior and exterior surveillance cameras.
- Establishment of restricted areas.
- Door controls.
- Electronic access control systems.
- Metal detectors.
- Silent panic alarms.
- Call buttons, blue lights, and other remote help call systems.
- Restricting access to reception areas when no receptionist is on duty.
- Electronic visitor logs or visitor management software.
- Expiring temporary badges for visitors.
- Parking garage/lot gates.
- Employee “safe rooms” for use during emergencies.
- Strengthening locks and reinforcing doors and windows.
- Installing strengthened glass, shutters, or grilles in windows.
- Curved mirrors at hallway intersections.
- Closing down empty building areas after hours to help focus security patrols.
- Installing barriers between workers and the public.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

A report in 2008 on crime prevention—from a joint project of law enforcement, businesses, and community leaders—shared what they see as the most promising strategies for thwarting crimes at commercial and retail establishments. The strategic approach they recommend is familiar: deploy security measures based on a review of risks, vulnerabilities, and incident and crime data. The best solutions are well-known: they are ones that reduce opportunity, limit reward, and increase the likelihood of apprehension.

Although the best strategies for preventing crime haven’t changed, science and technology are developing intriguing new options for deployment at the business level to prevent crimes. Workplace violence prevention teams should make a point to stay informed of emerging security technology and assess whether it might be a good investment in light of their workplace violence risk.

Just one example is the emerging expansion of analytics into the audio realm, with cameras becoming capable of recognizing sounds that might indicate a crime in progress. Just as smart cameras can now see when trouble might be brewing, software algorithms will soon give cameras the ability to hear breaking glass, shouting, a gathering crowd, and eventually even specific words. Cameras will respond as they do now to visual anomalies, by pivoting toward the sound or alarming so that security staff can investigate. In certain environments, such capability may be a very useful tool for alerting security staff to situations that have the capacity to escalate into a serious incident of workplace violence.

CPTED

Crime prevention through environmental design (CPTED) is a tool for understanding how the built environment can help prevent security problems, including workplace violence. CPTED entails the utilization of landscaping and building design to:

1. Discourage access to all but intended users.
2. Allow intruders to be spotted.
3. Establish the boundaries between private and public property.

FROM THE FIELD...

Think About Access Control From a Violent Intruder Perspective

Middle East tensions sparked violence in Seattle in July 2006 when a Muslim American, angry at Israel, shot five women and killed one at the Jewish Federation of Greater Seattle before surrendering to police.

By all accounts the center had tip-top building security, including bulletproof windows and security doors to separate the public lobby from the building’s interior. Staff needed to punch in a security code before opening, and visitor appointments were confirmed before being buzzed in. On any given day, this was probably more than enough to deter casual wrongdoing and get people to follow the rules.

But the shooting that shattered the Federation’s peace reminds companies to also consider how access controls will fare against a determined individual who is willing to simply storm his or her way in. According to news reports, the gunman waited for an employee to punch in her code, and then violently pushed his way in when she opened the door. Access control set-ups in high-risk environments might benefit from layers (such as mantraps) to curb violent intruders and prevent tailgating and forced entry into buildings and parking areas.
Organizations Need to Find Their Own “Protective Glass”

No matter what its primary purpose, any security technology in the workplace (access control, lighting, contraband detectors) helps to prevent, mitigate, or respond to a violent incident. But within each industry, there are often targeted technology solutions that may be the most important tool for preventing violence to workers.

For example, in a panel discussion at the 2008 ISC West conference in Las Vegas, Michael O’Hagen, senior vice president of security for Bank of America, said that of the 700 robberies it experiences in a year, 93 percent occur in banks without bulletproof glass in front of tellers. “The stats are dramatic,” he said, adding that the company is now aggressively deploying protective glass, starting in banks with high recidivism.

While each company must assess its own operation to find the physical security measure that will make the most difference, workplace violence consultant Richard Sem singled out two technologies for everyone to consider:

1. Panic alarms that have two modes instead of just one—one button for requesting assistance and one for immediate police-level emergency response. When a “9-1-1” panic button is the only setting, workers are often hesitant to ask for help in developing situations in which violence might occur, denying security staff an opportunity to intercede before an altercation turns into a full-blown violent event.

2. Visible video surveillance outside of areas in which employees expect privacy. The average worker is now more likely to know that companies are prohibited from installing video inside bathrooms and other sensitive areas, which makes them more likely locations for workplace crime. Sem said a visual record of people going in and out of these areas can provide an important level of deterrence.

While research provides little guidance as to CPTED’s effectiveness in reducing the incidence of workplace violence, the general principles of this approach are widely accepted, according to a report by the Department of Justice. Employers who are contemplating major remodeling, a property purchase, or construction of new premises, should consider how CPTED strategies can discourage violent incidents. Information about CPTED can be obtained from the National Crime Prevention Council (www.ncpc.org/cpted.htm) and the International CPTED Association (www.cpted.net).

The premise of CPTED is that certain design elements can promote specific behaviors among visitors and staff and reduce the risk that individuals will unwittingly do things that create a security risk. For example:

- A building’s lighting design can improve surveillance, which can reduce vandalism and the potential for violence, as well as increase respect for property.

- Proper facility signage reduces the number of individuals who create a security risk by unknowingly entering restricted areas.

- Limiting entry points allows for greater control of the environment and improves property surveillance.

- Controlling building flow—to separate staff from the public, for example—can enhance the safety of building occupants.

- Trash removal, regular repainting, and all similar “housekeeping” items reduces inappropriate behavior and many types of crime, including violent assault and robbery.

- Locating employee parking areas close to the facility enhances safety for employees as they come and go.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

Another Consideration for Locating Security

A detailed after-incident review of a shooting in 2009 at the Woodbridge campus of Northern Virginia Community College (NOVA) raised an issue not often considered when an organizations considers where to physically locate the security department. Namely, how does the location of the security department or office impact the ability to respond to the most likely location of a shooting incident?

Organizations should review security’s location against the most likely entry point of an active shooter. Officers’ being able to respond quickly is a paramount consideration but—as noted in the report on the campus shooting at NOVA—companies also need to consider the need to retrieve equipment and have access to communications technology to respond to an incident. It is helpful to locate these resources in an area less likely to be affected in a shooting incident. (Report of the Presidential Commission on Safety & Security, Appendix F, “Shooting at the Woodbridge Campus, After Incident Report: Lessons Learned and Recommendations,” March 2010.)

- Landscaping and the building orientation can either enhance natural surveillance and reduce the likelihood of crime events or obscure surveillance and encourage crime.

Environmental factors

Closely tied to CPTED, the work environment is another important consideration, as research has proven a link between environmental factors and tempers boiling over into a violent workplace event. Recently, guidelines have been developed for easing tension through environmental measures (“Framework Guidelines for Addressing Workplace Violence in the Health Sector” International Labor Office, International Council of Nurses, the World Health Organization, and Public Services International, 2002).

The guidelines affirm the importance of the traditional prevention strategies that companies use: assessments, policies, training, awareness, and appropriate staffing levels. But beyond the tried-and-true precautions, the guidelines outline very specific environmental considerations that workplace violence teams should take into account to reduce the risk of violent clashes between members of the public and their own employees.

Don’t Just Buy Technology to Address Risk of Violence, Measure Whether It’s Working

When organizations go all in—outfitting a facility that had little or no security with an electronic security system—they expect their investment to prevent crime. In fact, property owners are so confident that these new, high-end systems will deter crime, few of them make an effort to validate the effectiveness of the systems they’ve implemented—perhaps, because no one wants to find out they just spent a lot of money for nothing.

A study published in February 2009 examined the effect on crime of an integrated security management system at an apartment complex in New York City, including 198 surveillance cameras, door alarm monitoring, electronic key cards and readers, interior emergency call boxes, and outside emergency call boxes with attached Pan-Tilt-Zoom (PTZ) cameras. Unfortunately, the researchers could find no proof that the system cut crime at all (“The Effectiveness of an Electronic Security Management System in a Privately Owned Apartment Complex,” Greenberg & Roush, Evaluation Review, Volume 33 Number 1).

Of course, this does not mean that workplace violence prevention isn’t enhanced by building hardening and other physical security measures, but it does suggest that workplace violence teams shouldn’t assume that new security investments have erased the threat. Measure incidents pre- and post-introduction and continually tweak systems to optimize their level of effectiveness in deterring incidents of violence.
Nearly every environmental aspect of a facility has an impact—good or bad—on the likelihood of violence, including the choice of paint color. “The physical features of a workplace are key factors in either defusing or acting as a potential trigger of violence,” the guidelines conclude. Whenever possible, companies should:

- Provide comfortable seating.
- Ensure sufficient space to minimize personal interaction between members of the public and between public and staff.
- Reduce noise levels.
- Use soothing colors (certain golds and greens).
- Eliminate odors.
- Keep comfortable temperature and humidity levels.
- Arrange furniture to prevent entrapment of staff.
- Reduce boredom of those waiting for service (television or other distractions).
- Ensure sufficient ventilation.

### F. Training

There are approximately 16,400 workplace threats of violence every day. That there are fewer than 700 employee victims of homicide annually is evidence of how important it is for employees to deftly handle potentially violent incidents.

Providing awareness education to staff lies at the very foundation of a prevention program. If workers aren’t instructed on what workplace violence is and how to report it, companies are unlikely to be kept informed about the scope of the problem—a prerequisite for addressing it.

Workplace violence training has certainly grown more common in America’s workplaces. Nearly twice as many workers today as in 2000 are likely to say they’ve received it. And three out of four organizations provide training on workplace violence to at least some general workers, according to an IOMA/SDR survey in October 2009 of 300 organizations. Still, less than one-third of organizations provide annual workplace violence training to all workers (see Figures 17 and 18).

Supervisors play a uniquely important role in
violence prevention. They are in a better position than the security or workplace violence team to recognize and reduce the threat of a violent incident, and while well-trained supervisors are a first-line of defense, untrained department heads often make a dangerous situation worse.

Nonetheless, a survey by IOMA of companies with security departments finds that less than half train all supervisors annually in how to recognize trouble and how to intercede (see figures 19 and 20).

Workplace violence/de-escalation training is more common for security officers, but even for protection personnel training is not universal. While it is extremely common in some high-risk environments, like hospitals, it is far less so in others, including manufacturing and production facilities and retail establishments.

Training of security officers on the subject is even more common—74.1 percent of companies require all officers to undergo training on workplace violence prevention and de-escalation. However, while it is extremely common in some high-risk environments, like hospitals, it is far less so in others, including manufacturing and production facilities and retail establishments.

Figure 19. Annual* Training on Workplace Violence Prevention to Managers/Supervisors

*Respondent has, in the last 12 month, required managers/secretaries to attend at least one training or awareness session on workplace violence

(Source: IOMA/SDR Survey on Corporate Security Management, Policy & Practices)
Core elements

Derived from the opinions of experienced trainers in aggression management, a training program for the prevention of workplace violence needs to address 12 basic elements ("Standards for Violence Management Training," Paterson; Security Journal):

1. **Core values.** Training must promote the core values of the organization and tie violence prevention training into the corporate mission.

2. **Risk assessment.** Your actual risk should provide the basis for the extent and content of training. A good training program provides content in light of identifying who is at risk and from what types of violence.

Fixing Holes in Today’s De-Escalation Training

While certain core elements of conflict management training can be found in most training programs, even experienced law enforcement officers say new skills to contend with new risks need to work their way into training content. "Just when you think you’ve heard it all, you realize you haven’t," said Curt Crum of the Boise, Idaho, police department, in an address to the 2010 ISC West conference in Las Vegas. "There is always a new twist, and you learn you may have been unwittingly throwing gas on the fire." To prevent a heated situation from becoming violent, Crum said to stress the following points in your next training program.

1. **Focus on the problem.** When dealing with the complaints of rude and obnoxious customers or other individuals, workers often let their own feelings (such as anger or resentment) prevent them from addressing the issue or fixing the problem that is at the heart of the conflict. "A hostile person may have a legitimate beef, even if they’re handling it poorly," said Crum. The first step in diffusing angry people is to fix the problem if it can and should be fixed. "Genuinely try to help them, even if they are being rude."

2. **Take away the audience.** Crum says his years of personal experience with loud and threatening individuals has taught him that many "feed off of being watched." So a good portion of security training on calming down a hostile individual should address trying to move the individual to a private area. "People who are loud and shouting often calm down."

3. **Demonstrate the 3Cs.** When security officers or staff find themselves in a situation that requires de-escalation, they should be trained to focus on their own behavior—not merely react to the subject. Train them to concentrate on demonstrating their confidence, competence, and control, says Crum. He also suggested that a fourth "C" is worth stressing during employee and officer training—courtesy. Give hostile individuals a minute or two to vent (but no more) and never belittle them, he said.

FROM THE FIELD...

Training Is Critical to Learn About Incidents

The New Jersey Department of Health and Senior Services recently conducted a study of violence experienced by healthcare workers and were troubled to learn, for example, that 90 percent of emergency department nurses said they’re verbally abused at least once a year. But they were even more disturbed that 72 percent of nurses who were verbally or physically assaulted did not report the event.

One reason, they concluded, is that the problem of violence has been normalized in healthcare to the point it has become accepted as part of the job. But then why are healthcare workers more likely to report incidents in California?

They think one reason for the lack of reporting in New Jersey is that it has no legislative training requirements, and so only 72 percent of hospitals in the state conduct training, whereas training is nearly universal in California because hospitals are required to provide it.

FROM THE FIELD...
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

3. **Definitions of aggression and violence.** It is necessary to teach employees how your company defines violence and what types of incidents they need to report (e.g., verbal assaults), and the process for reporting incidents.

4. **Safe systems of work.** Part of protecting employees from violence is teaching them how their physical environment may protect them or put them at risk. Include education on the office design and layout, alarms, how to call for security assistance, how to report an incident, and so on.

5. **Information on the aggressive profiles of the particular individuals that your employees may encounter.** For example, depending on your company’s business, you may need to teach employees about the profiles of irate customers, intoxicated individuals, or people with mental illness. Again, targeting the training toward the actual risk workers face makes it more effective.

6. **Theoretical models of aggression and violence.** Educate employees on why aggressive feelings may occur, both in others and themselves, and how to address those feelings.

7. **Conditions and triggers for the prediction of aggressive behavior.** These will help employees or supervisors anticipate and defuse a potentially violent situation.

8. **De-escalation—both theoretical models and skills practice.** Good corporate workplace violence programs will include skills training on how to respond to aggressive behavior and potentially violent situations.

9. **Legal and ethical issues relevant to the different groups of training recipients.** One example: the restraining methods nurses should and should not employ.

---

**When It Comes to Training, Remember Robberies Aren’t Just at 7-Elevens Anymore**

Commercial robberies still elicit the image of a convenience store stickup or a bank holdup, but FBI data show robbery is on the rise at other “commercial houses.” The robbery trend suggests that some level of awareness education may now be appropriate for a greater number of workers. For example, many recent incidents of office robberies involve small companies with ground-level offices, according to a report in the Wall St. Journal (“Stickups and Burglaries Are on the Rise—at Work,” WSJ, Nov. 17, 2009).

The UK National Health Service Trust recommends that all employees—even those for whom public contact is not part of their job—receive three to seven hours in basic personal safety training. More in-depth violent-intruder training might be appropriate for a range of commercial businesses—from auto parts stores to restaurants to clothing boutiques—in light of the move to nontraditional robbery targets. The British Retail Consortium identified the points that trainers should cover:

- How to reduce the likelihood of being a target. Refer to company policy, guidance, and security procedures.
- Personal safety. Stress that the most important consideration is safety (don’t be a hero).
- Assessing a situation and response options.
- Communications and teamwork. Make sure employees are clear on communications, codes, announcements, etc.
10. **Physical contact skills.** For different relevant personnel, provide skills training on escaping, blocking an attack, or restraint.

11. **Immediate management of hostage situations.** This training should be given to security and relevant management and employee personnel—front window bank tellers, for example.

12. **Awareness education of support programs.** Companies must make employees who feel threatened or have become the victim of a violent incident aware of the resources at their disposal.

**Directed training**

In addition to covering the 12-point curriculum above, a company can measure the effectiveness of its training by how well it focuses on the particular learning needs of major employee groups.

- **Management.** They need less training in direct response but must receive education on their legal obligations for ensuring worker safety and their role in promoting your organizational strategy to prevent violence. This is critical, because “management can seriously confuse things if they don’t know your policy,” according to Judith Matheny, who oversees employee emergency response training for dozens of banks in Colorado for the First Bank Holding Company.

- **Supervisors.** Supervisor training should focus on what supervisors should do with information they receive regarding a report, concern, or incident, and aim to give supervisors all the skills they need to match the level of response they are expected to give to the incidents they encounter. The curriculum should focus on how to recognize signs of aggression, spotting warning signs of troubled employees, and de-escalation and conflict resolution.

- **General staff.** Employees who don’t interact with the public and face no additional risk require less training—one hour of training and an hour of re-training every two years is probably sufficient. However, general staff still form the cornerstone of an effective violence prevention program because success depends on their understanding and cooperation. Training should focus on: (1) promoting employee awareness of the many manifestations of workplace violence; (2) company policy; and (3) employees’ respective responsibilities under the policy. Companies should also make it a goal of training to instill confidence in the commitment and ability of management to effectively and confidentially address the issue. Training should also stress that the ability of the company to help workers depends on workers’ willingness to report all events.

- **Members of the “threat management team.”** All individuals who are involved in analyzing situations and recommending a course of action should receive training necessary to carry out that critical function effectively.

- **Security officers.** Workplace violence, de-escalation, and emergency response are critical components in security staff training, and officers should receive testing to make sure they are competent in each area.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

Direct service staff

Employees who have direct contact with the public, especially those who deal with aggressive individuals, are at unique risk from workplace violence. Like security officers, they commonly encounter violent or hostile situations, yet their general job training usually does not include how to manage such events.

Companies should aim to be more proactive in managing enterprisewide risk, and that should include looking at the interplay between workers and customers for whether untapped strategies exist to reduce conflict and aggression. Companies should also make clear what actions the company does not want employees to perform on its behalf.

1. Ensure employees have the general coping mechanisms they need to deal with aggressive clients and customers. The negative consequences from hostile clients and customers largely depend on how prepared employees are to face the aggression. Staff should receive training to develop specific skills, including:

   - Situation assessment and decisionmaking skills and exit strategies.
   - Calming skills for defusing emotional situations.
   - Appropriate skills for confronting unacceptable behavior.
   - How to respond in high-risk situations including theft and robbery.

2. Give employees the specific skills they need to deal with the types of aggressive behavior they face. All service industry workers are at risk from threatening behavior from the public, but the techniques they need to deal with aggression will depend on whether the source is an unstable patient or a disgruntled customer and if the cause is a long wait time, bad news, or intoxication. So in addition to general training, companies should provide training to staff that deals with customers on how to perform specific tasks that often result in aggression. Training might need to cover:

   - How to deftly take away individuals’ “rights,” such as stopping an individual from smoking or entering restricted areas.
   - How to manage large groups of people.

Teens Are Unprepared for Workplace Violence They Face

After a retail robbery ended in the death of an 18-year-old CVS employee, the Massachusetts Coalition for Occupational Safety and Health, in conjunction with several advocacy groups, conducted a survey of teen workers in several Massachusetts cities ("Teens Affected by Workplace Violence," 2005). Findings:

- Seventy-four percent of teen employees had no training on how to handle robbers or shoplifters, even though 27 percent had encountered such an event at work.
- Thirty percent said they would chase a shoplifter if they encountered such a situation, despite a lack of training.

The study recommended that retail businesses post clear safety policies specifying how employees can protect themselves from workplace violence and train all employees how to respond to armed robbery and theft situations and how to handle angry customers and stress.
• How to work directly with volatile people, especially individuals under the influence of drugs or alcohol.
• How to calm individuals who must endure long waits for service.
• Common warning signs and behavioral traits of potentially aggressive individuals.
• How to deliver upsetting news (cancellations, rejections, and so on).

3. Gather information to help identify and eliminate root causes of client aggression. Data collection serves as the foundation for cost-effective violence prevention. Violence prevention teams must ensure that the company is effectively tracking all events relating to customer or client aggression to understand the root causes of conflict and identify the specific training employees need as well as whether the company may be able to remove sources of conflict.

To gather data, the violence prevention team should frequently remind staff to report all conflicts with customers, including those that do not rise to the level of threats or violence. Corporate security can then analyze the data from incidents and near-incidents, such as who was the target, what time of day it occurred, what was the cause of conflict, and so on.

Armed with data, companies can identify possible solutions to reduce conflict. For example, if long wait times are a frequent source of conflict with customers, a business may choose to take steps to reduce tension such as adding a television in the waiting area. Or if conflicts caused by long waits correlate with a specific time of day, a company may choose to add staff at peak times.

Supervisors

One goal of the workplace violence team should be to give managers the tools to spot and deal with aggression well before it ever escalates into an incident that requires a response. As such, supervisors are the lynchpin of a successful violence prevention program, and need to be instructed on how to be effective aggression managers. They need to know warning signs such as:

• Behavior is usually the first window to escalating anxiety. Employees who end up violent often first display signs of changed behavior, usually by becoming scattered in their thoughts.

If You’re Going to Train Workers to Shelter-in-Place . . .

. . . Make sure it’s a safe directive. After one college had a classroom shooting incident in 2009, an investigation found that telling students and faculty to barricade themselves in classrooms during an active-shooter event wasn’t a very good idea. Many classrooms, it learned, were not lockable from the inside.

So the college is looking to install Sargent Series 10 locksets on 764 classroom doors to prevent unwanted intrusion while still allowing doors to be easily opened from the inside to permit easy exit. Another recommendation made during the review was for reinforced windows of such a shape and placement that an intruder cannot break the glass, reach in, and unlock a door.
thinking and actions. Other behavioral indicators include: spreading rumors, being belligerent toward others, swearing more than usual, becoming increasingly argumentative (changing from trying to make winning arguments to winning arguments at any cost), and referring to themselves as victims.

- Staring is a sign of aggressive behavior. Humans don’t naturally stare at other individuals—they stare at objects. When an employee stares at a manager, the manager has been reduced to an object in the mind of the aggressor.

Supervisors also need to be given the tools for responding to signs of early-stage trouble. For example:

- Communicate the employee’s negative behavior to them in writing. Write down the problem in a neutral, reflective way. It is more difficult to remain neutral when telling an employee what the problem is. And even if phrased correctly, a supervisor may emit body language that puts the employee on the defensive.

- Take responsibility for communication with an angry employee. Effective aggression training should instill in supervisors ownership of potential problems, and not just how to recognize them.

Larry J. Chavez, founder of Critical Incident Associates (www.workplaceviolence101.com), says companies should provide first-line supervisors formal instruction as well as the opportunity to take part in hypothetical, problem-solving scenarios. “They must be trained to identify the warning signs of impending violence and to conduct basic threat assessment to support the documentation and reporting of potentially dangerous situations,” he adds. Finally, organizations need to train supervisors to recognize, identify, and eliminate organizational risk factors that could lead to violence and teach them how to defuse hostile or potentially violent employees. Unique elements of supervisor training may include:

- Policy requirements, risk assessments, and control measures.
- Appropriate ways to handle employee discipline.
- Appropriate use of Employee Assistance Program (EAP) counselor and outplacement services.
- Sensitivity and aggression management.
- Assessing violence potential of individuals (threat assessment).
- De-escalation techniques and conflict resolution.
- Handling of performance reviews and promotions.
- Cultural and religious diversity training in light of the workforce.
- Procedures for conducting preliminary investigations.
- Ways to reduce or remove a threat or actual violence.
- Using a 360-degree-feedback process for early detection of worker anger.
• Method for recording and reporting incidents and for reporting the results of preliminary investigations.
  
• How to protect evidence.
  
• Motivation techniques to encourage employees to prevent and report acts of workplace violence.
  
• How to conduct department-specific workplace violence training for new or transferred employees.
  
• Skills to analyze violent incidents and trends, and in conjunction with the workplace violence prevention team, to develop preventative solutions for their work group.
  
• Procedure for making recommendations to the workplace violence prevention program.
  
• Awareness of how to respond during and after stressful events and their role in supporting staff in the immediate aftermath.
  
• How to provide and facilitate longer-term support to employees affected by violence and manage their return to work.

Dr. James Madero, president of Violence Prevention International, says supervisors should receive, at a minimum, three hours of initial training. They should then receive refresher training every two years for at least one hour, he says. Additionally, they should receive written materials occasionally, such as an e-mail, handout, or newsletter, to keep them up to date and keep the issue of workplace violence in front of them.

Training methodology

When companies use internal staff to conduct workplace violence training, HR staff is most likely to lead (24 percent), followed by safety (14 percent), risk management (13 percent), security (13 percent), and the legal department (3 percent) (“Workplace Violence Survey and White Paper,” Risk and Insurance Management Society; www.rims.org).

The workplace violence prevention team needs to audit whether the individual providing this

---

**Supervisor Training Must Keep Pace With Diversity**

The racial and ethnic make-up of the U.S. workforce is continuing to diversify, so researchers examined workplace studies to learn if it is having any impact—and they found that it is. Studies demonstrate a correlation between workplace harassment and exclusion based on ethnicity. They also found conflict resulting from employees’ use of non-English languages in the workplace (“Emerging Workplace Diversity Issues: Ethnicity, Bilingualism, and Workplace Exclusion,” paper to the Society for Industrial and Organizational Psychology symposium).

This raises questions for violence prevention teams: Have we considered changes in workplace ethnicity as a risk factor for conflicts? Do we know which ethnic groups are growing most rapidly among our workforce, customers, and visitors? Has diversity caused any problems? Should we provide additional training on cultural sensitivity to supervisors to help them handle it?
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

Instruction has the skills to do it effectively. Companies face enormous financial pressures to keep workers working rather than in a training session, so it is important for companies to make violence prevention training worth the time.

1. **Use participatory training.** Eliciting active participation enhances the effectiveness and reduces the need for costly retraining. Adults, more than children, need learning to relate to their actual activities and require active participation for training to have a lasting impact. Companies that use video or lecture-only training have to re-train more frequently because employees more quickly forget the lessons. According to research by the National Institute for Occupational Safety & Health, workers whose education includes scenario-based instruction score better on retention exams, have a more positive attitude toward training material, and think arguments used in training are more persuasive.

   Online or software training can be a useful adjunct to participatory training but should not be a replacement, warns workplace violence consultant Felix Nater. He says that the online training programs he has examined are frequently insufficient and too generic to be truly beneficial. He warns that it cannot provide the same value that in-person training in the actual work environment does, especially for physical actions that employees may have to take, like how they should move or take cover in a workplace shooting, for example.

2. **Use incident reports as a guide.** To ensure that training is relevant to the workers who receive it, use real incidents to help develop course content. One company told us that it recently began making training videos in-house that recreate actual events, and staff has responded enthusiastically to them.

3. **Incorporate the knowledge staff possesses into the lesson plan.** Effective training requires recognizing what workers bring with them to the training, and making workers’ existing knowledge, attitudes, and beliefs the very foundation of training. For example: A violence prevention trainer could opt to give store associates a 40-minute lecture on behavior that signals potential violence, what to do in an emergency, and other policies and procedures to follow. He or she could even test associates at the end to see how well they learned the lesson. But following this type of educational model—telling workers what they need to know—has inherent problems. A better way would be to get associates to share their own experiences, develop role playing exercises, and explain how each security procedure will make them more secure in the workplace.

   Companies should also think creatively to improve workers’ awareness of workplace violence issues without adding to the expense of the program by taking large groups away from their work. Ideas:

   - Include workplace violence training in new employee orientation programs.
   - Provide workplace violence tips and reminders in institution newsletters and publications.
   - Use bulletin board postings for important reminders and procedures for staff to follow in an emergency.
   - Identify the key personnel in your workplace violence program and send them to workplace violence seminars.
• Distribute workplace violence reminders and instructions with employee paychecks.

4. **Deliver a balanced program that recognizes that people learn differently.** This reality should be reflected in violence prevention awareness training that includes verbal briefings, print and reading materials, and visual reminders. And, as often as possible, programs should combine learning materials—a presentation on handling angry customers, delivered verbally, should also include written handouts.

5. **Make an effort to deliver a quality presentation.** Security trainers often make a (convenient) mistake of believing that how they communicate isn’t really important. Security is serious and critical, so style and presentation quality shouldn’t matter, they convince themselves. To avoid a common mistake in security and workplace violence presentation, be brief, simple, and to the point. “We tend to overwhelm people with death by detail,” says Deborah Russell Collins, executive director of the National Security Training Institute and former security awareness instructor at TRW.

6. **Formalize your training program by giving it a goal, developing strategies to meet it, and conducting audits to measure its effectiveness.** Bob Kennedy, chief of the Counterintelligence Awareness Division for the National Security Agency, says his job is much like that of security directors and violence prevention teams except for a different audience, and they should have the same goal: Use a multifaceted approach to continuously raise security consciousness on successive occasions within a carefully orchestrated campaign. Strategic planning won’t raise the cost of your violence prevention program, but it will make it more effective.

**Assessing Training Providers**

Companies that use an outside trainer should carefully select one that is a good fit by conducting a needs analysis, examining the course content of several providers, and speaking with similar organizations for recommendations.

Companies should then focus on three key questions to judge the suitability of training before making a final selection:

1. **What is the values base of the training?** Violence prevention training will not only impart skills and knowledge to your employees, it will transfer values that will infiltrate your company culture. Make sure any presentation is in line with your corporate values and reinforces how your company approaches aggression and violent situations. Investigate what legal and ethical issues the training will cover and if it is consistent with your company policy.

2. **Will it work in your environment?** Training programs, especially those geared toward handling armed intruders, may presume certain conditions, such as the presence of alarms, security personnel, and so on. Research whether the training will support your physical environment as well as your company policies.
3. **Are the techniques relevant?** Any training program should be directly relevant to the situation in which you expect employees to use the skills. As such, you need to assess for gaps in a provider’s training program and fill them in yourself. For example, an outside aggression management trainer probably won’t address your incident reporting structure, so you need to educate employees on it. It’s up to your company to make sure workers understand how to apply the general knowledge they receive during training in your workplace.

**Program controls**

- **Is the knowledge level of your general staff, supervisors, and security personnel commensurate with their role in a violent event?** It’s typical for violent incidents to highlight deficiencies in knowledge. For example, an institutional review of a shooting in 2009 at the Woodbridge campus of Northern Virginia Community College found that some faculty and staff were unaware of how to respond (shelter-in-place versus evacuate). It is important to provide all personnel the tools to protect themselves and the knowledge of where to go under different circumstances.

- **Is training the only significant component of your workplace violence prevention program?** Many companies see it as the best way to prevent violence, but a program must also address issues such as building design, operational policies, staffing levels, and so on.

- **Does your training program receive adequate funding and review?** Use a dedicated budget, periodically monitor training, and review the program and course content annually.

- **Do you provide sufficient refresher training?** Studies show that employee skills in spotting aggression and handling a violent situation diminish sharply over time, thereby making periodic update training critical to program success. Training needs to be frequent enough for people to call it up in a traumatic situation.

- **Do you provide supplemental or more frequent training to high-risk staff?** Go to your incident database and analyze trends for where incidents occur—warehouse, administration, etc.—then make sure the training in those departments is sufficient in light of their heightened risk. Hospitals, for example, may extend extra training to fixed emergency department staff but forget other workers who rotate into that high-risk environment, such as volunteers, clerical staff, contract workers, and physicians.

- **How long is it before staff receives workplace violence awareness training?** Companies too often fail to provide some level of training as soon as employees come on board, which is important to demonstrate to new hires that the organization takes the issue seriously. A company that provides a workplace violence training session to its entire 200-person workforce may not want to go to the expense of providing training again if they hire five to six new workers a month later. But companies still need to provide some sort of training to these individuals shortly after they start, for example, through online training materials.
• **Does your workplace violence training respect organizational priorities?**
Security and violence prevention trainers should be concise during training and must make the training relevant to the audience. In the investigation of the shooting at NOVA, it was clear from minutes of the meetings that officials were concerned that security training would not make effective use of attendees' time. This is a concern that senior management often has about security and emergency training.

### G. Incident Management

No matter how healthy an organizational culture is, or how detailed its background screening, incidents will arise. At times, an employee will exhibit troubling behavior, make a threat, or—more worrisome—commit an act of violence. Because incidents and their precursors will occur, companies need to:

- Spot troubling behavior early and assess its implications.
- Capture incidents in a formal reporting system.
- Assess threats and incidents and take appropriate action.
- Take necessary actions to protect and support victims.

**Incident reporting/tracking**

As noted earlier, if companies hope to effectively prevent violent acts and mitigate threats in the workplace, they first need to learn about them. “A company can spend a lot of money training supervisors to look for warning signs and define what is workplace violence, but you need to have a mechanism so employees can tell someone if they feel afraid,” says Stephen Doherty, a workplace violence consultant and former police chief.

**Non-Reporting Can Severely Distort Workplace Violence Picture**

Most nurses are victims of workplace violence within a 12-month period. But few report it, suggests research of 113 nurses in a suburban Australian hospital (“Examining the characteristics of workplace violence in one non-tertiary hospital,” *Journal of Clinical Nursing*, February 2010).

Of nurses in the study, 92 percent were verbally abused, 69 percent were physically threatened, and 52 percent were physically assaulted in the past year. Twenty-five percent of the nurses said they experienced violent events weekly, 27 percent, monthly, and 25 percent, every six months. Some 40 percent of nurses over the 12 months were involved in an incident involving a weapon: Hospital equipment (32 percent), guns (6 percent), and knives (3 percent) were the most frequently used weapons.

Despite the shockingly high rate of victimization, **only 16 percent of nurses had completed an official incident form in the last year; 50 percent had informally reported an incident verbally to a supervisor.** Thirty percent of nurses said they didn’t file official incident reports because the incident was just a part of the job. Nurses in emergency departments—the most frequently victimized—were less likely to report incidents than nurses in other departments.

Indeed, it is clear from the results of the study that nurses rarely file an official workplace violence incident report unless they also get hurt during the encounter. In 96 percent of the cases in which nurses completed an incident report form, the victim also reported a physical injury.
It is also critically important that a company’s reporting system allow for the aggregation of data detailing workplace incidents. While it is possible to address workplace violence incident-by-incident, an incident database is necessary for analysis and to provide the violence prevention team with an accurate understanding of the issues they face.

Elements of an effective incident reporting system:

1. Develop clear reporting procedures. Establish procedures for the timely reporting of acts or threats of violence. A policy should identify direct reporting to specific individuals, reporting through the supervisory chain of command, and reporting through specific hot lines or online addresses established for this purpose.

2. Educate employees about reporting procedures. All employees should know how and where to report violent acts, threats of violence, or other inappropriate behavior in violation of the company’s workplace violence policy. A system must include distributing to all employees the phone numbers and contact information for people to whom employees should make reports, says James Madero, Ph.D., president of Violence Prevention

### Figure 21. Employee Training at Large Establishments* on Workplace Violence Reporting Procedures** by Industry, 2006

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>60.7%</td>
</tr>
<tr>
<td>Goods producing (private industry)</td>
<td>66.1%</td>
</tr>
<tr>
<td>Service providing (private industry)</td>
<td>58.3%</td>
</tr>
<tr>
<td>State government</td>
<td>71.7%</td>
</tr>
<tr>
<td>Local government</td>
<td>55.9%</td>
</tr>
</tbody>
</table>

*1,000 or more employees
**Training on how employees can report workplace violence concerns and incidents is offered by the organization

### Why VA Workers Weren’t Reporting Workplace Violence

Statistics from the U.S. Department of Justice suggest that employers never hear about 43 percent of personal threats and 58 percent of harassment incidents in their workplaces. But how can that be? Especially if an organization has a clear policy on what employees should report and frequently communicates that policy to staff?

An official at the Department of Veterans Affairs shared with IOMA the results of an internal investigation into why a significant number of workplace violence cases were going unreported at VA facilities and hospitals:

- Burdensome paperwork requirements associated with reporting incidents.
- Employees fear that they themselves will be blamed for the incident.
- The intent of the attacker is often not clear.
- Employees are accustomed to being assaulted by patients or have been told to expect such treatment upon taking the job.

FROM THE FIELD...

© 2010 Institute of Financial Management, a division of Management Networks, LLC. No part of this publication may be reproduced, stored in a retrieval system or transmitted by any means, electronic or mechanical, without prior written permission of the Institute of Financial Management, Greenwich, CT USA.
International. Employees should also receive a reminder every six months of how to report workplace violence.

3. **Educate employees about what to report.** Employees need instruction, including practical examples, of the type of bullying or other nonviolent aggressive behavior that they should report. (Employees sometimes don’t think smaller events, such as verbal threats, are worth reporting.) The system should capture every reported incident, no matter how small, says Madero. Also, inform employees that no worker who reports or experiences workplace violence will face reprisals.

4. **Allow anonymous reporting.** “Organizations must honor anonymity when the reporting person asks for it,” according to Larry Chavez, consultant and trainer for Critical Incident Associates. Failure to allow for anonymity could result in the loss of valuable life-saving information, he warns.

5. **Give employees a way to report incidents 24/7.** Employees need to be able to report an incident after hours and on weekends. This is necessary to prevent an incident that happens away from work from spilling over into the workplace. For example, an employee who faces a domestic violence issue during the weekend should be able to report it then, rather than having to wait until Monday morning. Or if a fight occurs between two employees away from work, the company should have a reporting system that makes it possible to hear about it before the next workday. In both instances, immediate after-hours notification will give the violence prevention team additional time to discuss intervention and security before people are back at work. This could make the difference between a peaceful morning or one disrupted by a violent act, warns Madero.

6. **Make sure events travel up the chain and into a centralized database.** Imagine two employees are involved in a shouting match on the plant floor during the night shift. The shift manager responds appropriately and does everything she should to diffuse the situation and mitigate tensions. But does she also notify an individual in charge of keeping a central database that tracks all such incidents? “Whenever you have an incident like that, the violence prevention team should learn about it,” says Madero. “You need a central place where things get reported because it could be a single episode or it could be the fifth or sixth time that an employee has been involved in such an incident.”

---

**Does Your Corporate Hotline Know What to Do With Violence Reports?**

The Network, Inc. (www.tnwinc.com) operates corporate hotlines for more than 500 major companies, many of which use them to meet Sarbanes-Oxley requirements for anonymous fraud reporting. The hotlines handle all types of reports, according to a study by the group. Some 22 percent of callers dial-in to report theft; and reports of discrimination (16 percent) and wage and hour issues (13 percent) are also common.

But a call to report bogus expense account charges demands a different response from one reporting a threat of violence—and 5 percent of calls to corporate hotlines are to report workplace violence or threats, according to data from The Network.

Hotline operators (or internal call handlers) must have clear instructions on the types of calls that demand immediate, expedited reporting (workplace violence, release of proprietary information, etc.) and those that can go through the normal dissemination process.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

7. **Educate witnesses about their responsibilities.** Employees should understand their obligation to report threats, harassment, and other aggressive behavior they observe in the workplace—not just those they experience.

8. **Track details about all workplace violence incidents.** Companies need to track when, where, and how often threats or violence occurs to assist in the review and improvement of your workplace violence prevention plan.

9. **Develop a detailed incident reporting form for capturing workplace violence reports.** The more details these report forms capture, the more targeted—and effective—violence prevention solutions are likely to be. In order to be of use for later analysis, a security incident report needs to contain seven minimum elements (and the same is true whether it is an in-house security officer who completes the form or an officer from a contract guard firm). Incident reports should include:

   - Nature of the incident.
   - Date of incident.
   - Time of incident.
   - Precise location on property of incident (not “parking garage”).
   - Name/information regarding victim(s), if any.
   - Name/information regarding witness(es), if any.
   - Modus operandi used by perpetrator.

**Incident response**

If a worker violates the company’s workplace violence policy, employers have a range of possible responses. Among them:

   - Termination.
   - Counseling by supervisor.
   - Refer for medical examination.

**Confidence In Incident Reporting System Helps Capture Warning Signs**

Recognizing and reacting reasonably to potential warning signs is no small matter—and no easy task. Whenever a shooting rampage occurs, like the Virginia Tech massacre or the more recent Ft. Hood killings, it seems at first to be out of the blue. Then, little by little, reports of “missed signals” and “gaps in communication” emerge. Often, these reports reach a level that gets the public and jury members wondering, “How could you miss that?”

So it was in a shooting on a community college campus in 2009. The student, it was suggested in the post-incident investigation, may have been giving signals that he was troubled. A focus on enhancing preventative capabilities needs to include a review of the extent to which people understand and will use proper channels to report threats and other indicators of a potential problem. “People need to have confidence in using this reporting system and understand that the institution supports and protects them,” noted the commission that investigated the incident.

---

**FROM THE FIELD...**
• Refer to employee assistance program (EAP).
• Obtain fitness-for-duty evaluation.
• Place individual on medical leave and re-evaluate after treatment.
• Mandatory counseling with treatment monitoring.
• Opportunity to resign without prejudice.
• Discipline.
• Voluntary counseling.
• Restraining order.
• Contact law enforcement and place criminal charges.

The appropriate course of action is often unclear, so companies need to be sure they have elements in place to help reach a decision in a range of instances. Some helpful steps in this regard:

• Write procedures for conducting a workplace violence investigation. Investigations are frequently incomplete because companies don’t document how they should handle them, says Madero.

• Establish access to an individual(s) who is competent to conduct a threat assessment. This could be workplace violence prevention team members, but should also include an individual with a mental health background. Even if the company has personnel who are experienced and trained in conducting threat assessments, contacts with outside experts should be developed and maintained in the event these personnel are unavailable or if the event is unique and outside internal team members’ comfort level.

• Establish contact with a licensed behavioral psychologist in the event such an expert is needed to help evaluate and manage a threat.

When an incident occurs, the violence prevention team should identify all the resources that will be necessary to manage the situation until resolution, which may include help from outside the company. It is also important to:

• Thoroughly investigate the act and take immediate and appropriate action to deal with it. Every act or threat of violence must be taken seriously and dealt with quickly, but companies must also gather relevant facts before making decisions that have a lasting impact.

• Collect necessary data on individuals committing a violation of the workplace violence prevention policy. Especially if a company plans on taking an adverse employment action against an individual, it is not enough to understand the threat posed by an individual. Companies must have documentation to convince others of the threat and justify their decision. In the absence of solid evidence, arbitration professionals, who are often unaware of the magnitude of the problem of workplace violence, may insist an organization reinstate dangerous people into a workplace.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

Threat assessment

In the event an employee violates the company workplace violence policy or exhibits other troubling behavior—such as threats, aggressive outbursts, verbal abuse of co-workers or customers, or e-mail or telephone harassment of others—it will be up to the threat assessment team to examine that situation, assess its level of seriousness, and recommend a course of action.

This moment—when troubling behavior is first reported or a troubling event occurs—is a critical and tricky time for the workplace violence prevention team. Act too slowly and a facility may allow a problem to fester, but intervene too aggressively in a pre-incident situation and it may actually spark an incident that would not have otherwise occurred. “We train to recognize three levels of violence,” says Madero.

- “Level 1 is when somebody is verbally abusive, critical, argumentative with coworkers, or somewhat belligerent. Most of these situations a company can handle internally with training.
- “Level 2 includes threats, such as ‘You’ll be sorry,’ or ‘I’ll get you,’ or when an employee is extremely belligerent. Companies need experts to evaluate these events.
- “Level 3 includes fights, which may be appropriate for calling in the police.”

Events that hint at the potential for a serious act of workplace violence will occur in every workplace. The important question then becomes: How good is your threat assessment in the wake of such an incident? Will it be good enough to distinguish between a one-time aberration and an incident that is a precursor to a potential explosion? For a threat assessment model to work, three primary elements need to be in place, according to workplace violence consultant Joseph Kinney.

1. The team should conduct behavior assessments at the earliest indication of a possible problem.
2. Individuals trained in recognizing violent behavior should make the behavior assessments. These individuals also need to have an understanding of methods that can reduce the threat of violence.
3. When examining behavior or characteristics, teams should be mindful that no single indicator, by itself, is necessarily highly significant. Teams should give significantly more weight when an indicator occurs in conjunction with other signs that a person is likely to become violent.

Threat assessment principles. Trying to determine whether an employee is going to explode or is just blowing off steam is terrifically complicated. Yet you can boil down much about workplace threats to simple facts—basic tenets that have important implications for developing a threat assessment process that can prevent violent events and withstand the scrutiny of a lawsuit. The principles:

- **There is no reality.** “People only act out of their perception of reality,” notes James Cawood, CPP, president of Factor One (San Leandro, Calif.). When conducting a threat assessment, facts can’t help you gauge the likelihood of violence. So, for example, if a rather
benign comment sets a worker off, it’s a mistake to think he or she will quickly get over it because the comment wasn’t severe. In making a threat assessment, the actual severity of the remark doesn’t matter. “It only matters how the employee perceived it,” said Cawood in an address to the 2006 annual meeting of the International Association for Healthcare Security and Safety.

- **Employees commit violent acts for only one reason.** All intraspecies violence boils down to a single cause, said Cawood: to establish (or re-establish) control. (Note: This applies to workplace violence in which mental illness is not a contributing factor.) Implication: “When we diffuse situations we need to give the individual a perception of regaining control, because this is what all anger events are about. If you can make them think they have gained some control, you can divert 85 to 95 percent of events,” said Cawood.

- **The perceived need for control dictates an individual’s response as much as his or her characteristics.** People tend to establish patterns in their response to difficult situations. That’s why learning that an individual has been violent in the past is a huge factor in a current threat assessment. However, research also shows that the particulars of the work situation are important. So, in addition to an individual’s behavior pattern, a threat assessment must examine job-specific variables, such as how important the job is to the individual. For example, when a worker doesn’t perceive an option to leave a job, he or she is more likely to go to extremes to fight for control in a workplace conflict. However, the same worker in a similar dispute in a second or part-time job is less likely to engage the conflict. In short, a company couldn’t drive the average worker to violence even if it tried, but for “borderline” workers, job factors will play a big role in whether they let something slide or not.

- **There is only one sure path to long-term protection from an individual.** Many strategies can help keep the peace, such as separating the aggressor from his or her target or taking measures so that a potential aggressor is more likely to think his or her attempt to gain control will fail (such as CCTV, security officers, etc.). But administrative actions, restraining orders, and other actions taken by a company don’t truly eliminate the threat. Real safety is only possible if the potential aggressor willingly chooses to not commit an act. As a result, the ultimate goal of any conflict intervention must be to help the individual make that choice. Anything you impose on the individual doesn’t truly remove the potential for violence.

- **Violent events follow a pattern of escalation.** All situations start when an individual does or doesn’t do something the aggressor wants, then follows the aggressor’s idea of how to regain control, which typically depends on what he or she has done in the past in similar circumstances that resulted in success. But even then, a physical attack is stages away—after research/planning, preparation, and testing. So when an offender’s “threat” comes to the attention of the threat assessment team, it must work to fit the event into a chronology. Does the investigation suggest it is part of an escalation or is it just the individual’s normal pattern, which suggests that things will soon revert to normal? Similar actions don’t necessarily have similar implications, and threat assessments should be working to gather the information to help tell the difference.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

- All employees/threat assessment teams have an easy excuse to look the other way. “When people deal with people who slam doors or shout, they dismiss it because they have probably done the same thing in the past, and that gives them an excuse not to act. But [another person’s] reason for slamming the door has zero to do with why you might have slammed doors in the past,” notes Cawood. This same reasoning causes threat assessment teams to downplay events that do come to their attention. “Your ‘reality,’ values, and life experiences are the greatest obstacle to effectively predicting violent behavior,” warns Cawood. Unless employees and teams are trained not to filter the behavior they witness through their own (nonviolent) prism, they will always shrug at potentially violent signals and think, ‘heck, I’ve done that.’

- You can’t rely solely on psychologists. Most psychologists are not trained in violence risk assessments, warns Cawood, and even ones who are can’t be a one-stop-shop for your company’s violence threat assessment. While psychologists can help conduct interviews as part of a threat assessment process, they are not likely to do the background and records checks that must be part of a violence assessment protocol that will stand up in court.

Threat assessment protocol. When conducting a threat assessment, more information, independently corroborated, provides for better assessment of current and future risk of violence. The team charged with conducting threat assessments can use the following questions and information to help reach a determination:

1. What is the nature of the current situation? Conduct a detailed investigation and interviews to uncover the extent—and to create a timeline—of intimidating, threatening, or violent behavior by the aggressor. Information to get at during investigation and interviews include: entire history of the relationship between the aggressor and victim; current family relationships of aggressor and victim (proximity, intensity, dynamics, and support); and the mental and emotional history of aggressor and victim as known.

2. Is there any earlier record of the suspect acting in a violent manner? Conduct a direct check of law enforcement records for both aggressor and victim (NCIC, CII, Weapons

FROM THE FIELD...

Supervisors Play Key Role in Threat Assessment Process

In a series of IOMA interviews with workplace violence experts after the shooting at Virginia Tech in 2007, most experts thought the incident was typical in one respect: You could see it coming. “There are almost always warning signs,” said Mark Braverman, a consultant who works on workplace violence issues (Braverman Group; www.bravermangroup.com). So how come they are so often missed?

Experts said the problem typically is not that threat assessment teams reach the wrong conclusions when following their threat assessment protocol. It’s that early stage warning signs go unnoticed, and tragedy unfolds before a threat even comes to the attention of the threat assessment team.

Michael R. Mantell, a clinical and corporate psychologist based in San Diego, said companies need to, “Make sure all management staff are trained in how to identify and respond to the early warning indicators.” Warning signs they need to share, Mantell said, include “people who seem to be loners, people who the only thing they have in life is work, people with addictions, people going through major crises in life, or those who find themselves teased or the brunt of jokes.” Other early warning signs include holding grudges, an inability to handle criticism, blaming others, chronic complaints about being persecuted, and joking or making offensive comments about violent acts.
Registration, and Domestic Violence Registry). The most important documentation to examine is any criminal history or conviction for violent offenses such as assault and battery, armed robbery, rape, domestic assault, etc. However, consider any criminal history—even property offenses—as an indicator of past behavior of a violent nature. Furthermore, a history of traffic violations may indicate a drug or alcohol problem, poor impulse control, or other behavioral issues.

Threat assessment teams should not presume that the pre-employment screening was thorough and turned up all relevant records. This is especially true for employees who have been in place longer than your current pre-employment screening procedures. If there is any question about the completeness of the pre-employment scrutiny, conduct a more exhaustive review in the wake of conflict involving an employee. Dig deeper than the company did during its routine pre-employment investigation if an incident indicates the potential for violence.

Include in your threat assessment any information you can legally obtain. Possible official sources of information include:

- Public records, criminal and civil, at the Superior, Municipal, and Small Claims Courts and the Recorder’s Office for the last seven to 10 years.
- Military records, particularly records relating to court martial and discipline.
- School records, which may highlight behavioral problems or gaps that indicate possible institutionalization.
- Previous work history. Look for suggestions that fighting, possession of weapons, or other aggressive behavior caused a previous employer to fire, discipline, or force the individual to quit.
- Information from family members or associates. Do they report violent behavior? If the subject is recently divorced or separated, investigate for a possible connection with violent behavior.
- Weigh-in unofficial but reliable reports from associates and co-employees regarding past violent behavior.

**Threat Assessments Can’t Only Look at Guns**

Investigating whether an individual who has made workplace threats also has access to guns is pretty standard threat-assessment stuff. After all, an individual’s fascination with guns is a well-known warning sign.

However, an FBI report of violent incidents on college campuses suggests that individuals’ access to weapons does not necessarily determine the level of threat they pose. Firearms and knives/bladed weapons were used most frequently during violent campus incidents but one in four incidents involved neither, instead including strangulation, blunt objects, poison, vehicles, explosives, incendiary/arson methods, or physical assaults without a weapon.

“Understanding the varied weapons used in these incidents may prompt investigators to look beyond whether a subject possesses or has access to a more traditional weapon (firearm or knife) when evaluating his or her risk.” (“Campus Attacks: Targeted Violence Affecting Institutions of Higher Education,” United States Secret Service, United States Department of Education, FBI; April 2010.)
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

• Give some weight—although less—to “impressionistic assessments of violence.” For example, consultant Joseph Kinney says that a family history of violence may suggest a predisposition to consider violence. Don’t overemphasize this type of evidence, however, because an individual’s past behavior is a more reliable predictor of future violence.

3. Does the suspect own or have easy access to and/or familiarity with weapons or other dangerous devices such as explosives? Possessing a weapon doesn’t necessarily indicate potential danger, although a fascination with weapons and possession of multiple weapons should be a concern. This includes individuals who talk at length about weapons, subscribe to magazines dedicated to firearms, often practice with weapons, or are members of paramilitary or survivalist organizations. If combined with a threat against a coworker, consider individuals who fit into one of these categories as a high risk. Also, investigate whether the individual has recently obtained a weapon and, if so, what type. Relatively lethal weapons, such as semiautomatic weapons with a magazine capacity of 20 rounds or greater or semiautomatic pistols of 9 mm or larger caliber, are a greater cause for alarm.

4. Does the individual appear to harbor resentment or anger toward the company or coworkers? Be sure to consider the current employment status of the aggressor, as well as his or her length of employment—the longer the duration, the more angry employees are if they perceive they’ve been treated unfairly (being fired, passed over for promotion, and so on). Regard the threat as higher if the employee has named or shown an inclination to hold a particular individual responsible for some perceived mistreatment. The risk is higher with specific threats, rather than generalized comments that indicate anger.

5. Are other signals of potential danger present? Any of the following should bump an individual up a notch on your threat assessment scale:

• Historical and current use or abuse of alcohol and drugs.

• Other current or imminent issues being experienced by the aggressor which are, or could be, disruptive or stressful. A simmering employee is more likely to explode under increased pressure, such as that arising from a death in the family, a divorce, or the loss of a child as a result of divorce adjudication.

• Past expressions of sympathy, fascination, or interest in publicized actions of violence.

• Sabotage or destruction of company property and assets.

• Increasingly deteriorating work performance and attendance problems prior to the action that concerned the threat assessment team.

• Indications of extremely low self-esteem, depression, or suicidal thoughts. These include: statements of a fatalistic nature or actions such as closing out bank accounts, giving away valued property, or clearing out personal possessions from their desk.

After gathering the necessary information, the threat assessment team should complete its threat assessment—preferably using a validated assessment instrument. One such validated
instrument is the HCR-20 (History Clinical Risk), a 20-item checklist to assess the risk for future violence. Companies can also use the White/Cawood Assessment/Response Grids (Factor One; 510-352-8660). In domestic violence cases, companies can use the SARA (Spousal Assault Risk Assessment) Guide. Finally, as noted earlier, mental illness injects unique considerations into threat assessments. To assess if it might be playing a part in an employee’s behavior, companies can use the Hare-Psychopathy Checklist. Both the SARA Guide and Hare PCL-R are available from Multi Health System (www.mhs.com).

**H. Crisis Response**

Prevention is clearly the focus and primary goal of a workplace violence prevention program. But crisis response demands attention because interceding and managing an unfolding violent event is a company’s very last opportunity to prevent tragedy.

Corporate emergency plans have received greater attention as a result of Hurricane Katrina and other devastating natural disasters in recent years. Often, however, plans to respond to crisis are overwhelmed by actual emergencies. The spill following the explosion of the Deepwater Horizon oil rig in the Gulf of Mexico brought into sharp relief the danger of a crisis response plan built on rosy assumptions.

BP’s spill plan promised it would be able to contain any leak by collecting more than 20 million gallons of oil per day but most of the oil went uncollected during the months-long spill. In the meantime, BP looked feckless—failing time and again to stop the gushing oil, including ridiculed efforts to plug the well with golf balls and mud.

As bad as BP seems to have handled the spill and the public relations fallout, corporations are better prepared to handle those types of emergencies than a violent incident in the workplace, according to Richard Sem, former chief security officer for Waste Management and longtime consultant and expert witness in workplace violence cases (Sem Security Management; www.semsecurity.com). Sem says the difficulty in planning for such events has caused companies to ignore such planning. “Crisis response plans are much better on accidental causes like fire or hazardous spill than for handling purposeful events like violent incidents.”

**FROM THE FIELD...**

**Intel Finds Assessments Key to Program Success**

By the most fundamental measure, Intel Corporation’s violence prevention program has been successful. Intel has nearly 100,000 workers, and corporations should expect between 15 and 20 high-level threats per 10,000 employees, according to Dr. Harley Stock, forensic psychologist and managing partner at Incident Management Group (www.theimg.com).

Since the establishment a decade ago of Intel’s workplace violence response team, it has managed 2,000 potentially harmful situations with zero serious incidents, says Tim Garcia, the company’s investigative programs manager. He believes one primary tool for success has been the creation and company-wide use of a behavioral threat assessment to evaluate potentially violent individuals. The same model is used throughout the company, although it is tweaked in light of cultural issues in certain locations.
Companies often lack the same amount of planning because the existence of a thoughtful enemy creates an added layer of difficulty in crisis response that companies simply shy away from. Evacuation planning, for example, is much harder when you must also account for the possibility that a violent individual has built an evacuation into his attack and plans a secondary attack at the evacuation site. But rather than refusing to deal with these added complications, companies need to conduct tabletop exercises for purposeful events to figure out how they might deal with them, said Sem.

**Emergency planning**

The workplace violence prevention team should ensure that the organization’s emergency response plan includes contingencies and planning for a significant violent event in the workplace. This is not the case at many organizations, according to nationwide surveys. Surveys have traditionally shown that between one-quarter and one-half of companies do not have a crisis management plan that includes acts of workplace violence. Workplace violence prevention teams need to:

1. **Develop a contingency plan.** Set up a contingency plan that details how the company will respond during and after a violent incident. Make plans for activating the threat management team.

2. **Hold orientation and education sessions for individuals who have responsibilities in the event of a workplace violence emergency.** Conduct short, but regularly scheduled meetings to provide information, answer questions, and identify needs and concerns. In this type of session you can cover general information on:
   - Individual roles and responsibilities.
   - Information about threats, hazards, and protective actions.
   - Notification, warning, and communication procedures.

### FROM THE FIELD...

**Practicing Is the Single Most Important Activity to Make a Company Crisis-Ready**

The reservoir of good advice for making an organization crisis-ready is nearly bottomless. Why, then, do report cards on readiness so often hand out bad grades?

The reason may be advice overload, says a report by the Project on Organizational and Community Preparedness (“Predicting Organizational Crisis Readiness: Perspectives and Practices Toward a Pathway to Preparedness,” Center for Catastrophe Preparedness & Response and Public Entity Risk Institute, August 2008).

“Literature and research on crisis readiness offer a deep inventory of advice on how organizations can improve. Name an organizational intervention for improved performance or readiness, and it is likely to be on the long list of suggestions,” writes lead study author, Paul Light, Ph.D. “Asked to do everything, some organizations may simply assume that crisis readiness is beyond their reach.”

So their research examined 23 measures to find which are the most significant predictors of crisis readiness, and it narrowed down the essence of crisis readiness to two factors and a single piece of advice: “For organizations that have not experienced such a threat, readiness must involve at least some effort to simulate the realities of a crisis, particularly through planning and practice.”
• Means for locating family members in an emergency.
• Emergency response procedures.
• Evacuation, shelter, and accountability procedures.

3. **Conduct tabletop exercises.** These are often the most valuable exercises a company can perform and yet they involve few resources and only members of the emergency management team. Meet in a conference room setting to discuss each individual’s responsibilities under a range of different active shooter/workplace violence scenarios. This is a cost-effective and efficient way to identify areas of overlap and confusion before conducting more demanding training activities. Including a complete range of violent events in crisis scenarios is also a way to be sure that all potential events receive at least some practical crisis planning consideration.

4. **Conduct walk-through drills.** In these exercises, the emergency management team and response teams actually perform their emergency response functions. While they involve more individuals and are more thorough than tabletop exercises, they improve the skills of those who actually carry out the emergency plan—without major business disruption.

5. **Conduct functional drills.** These drills test specific crisis response functions, such as medical response, emergency notifications, warning and communications procedures, and equipment. Personnel involved in the specific tests then evaluate the system and identify problem areas. By testing different functions at different times, companies can reduce the disruption to the business as a whole while improving emergency preparedness.

6. **Conduct evacuation drills.** If companies test the other aspects of their response to a workplace violence emergency, they can limit the scope of evacuation drills to simply making sure personnel walk the correct evacuation route to the right designated area. Because a wide variety of emergencies may require a workplace evacuation (tornado, chemical spill, workplace violence, etc.), companies should identify when and how employees are to respond to different types of emergencies. How companies want workers to evacuate under an active shooter event may be different from the procedure for other emergency events (use of a safe room, for example, rather than evacuating to an outside assembly area).

**Program auditing.** Part of successful continuity management in the event of a major workplace violence incident is an ongoing assessment of readiness. Workplace violence teams should regularly ask questions about their preparedness to handle a major event:

• How well does senior management support the responsibilities outlined in the plan?
• How effective is the process at defining for individuals their emergency management responsibilities with respect to violent incidents?
• Do opportunities exist for distributing emergency preparedness information through corporate newsletters, employee manuals, or employee mailings that could help mitigate the damage from a violent workplace incident?
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

- Do personnel know what they should do in an emergency caused by a violent incident? Have you surveyed personnel to find out?

- In an emergency, would the crisis team have information about the location of key personnel?

- Have you already established a method for contacting key personnel and their family members in the wake of an event?

- Do you have contingency plans that include backup personnel who can assume responsibilities in case an employee is not able to perform them?

Finally, a crisis management plan should delineate individual responsibilities with respect to the handling of media in the event of a violent workplace incident. A well-executed media plan can minimize the damage from media reports of a violent workplace incident and is an increasingly important part of planning for the containment and control of an event. “Media response is more assured than ever, so getting your story out there before they define it is now a more important element of crisis planning,” says consultant Richard Sem.

Active shooter response

In an act of workplace violence—be it a rampage shooter, robbery, or some other violent event—the efficacy of a company’s security response will be vital in minimizing the extent of the damage. A well-trained security force that responds quickly and effectively to emergency calls is an important part of workplace violence prevention.

However, organizations should be wary about putting too much faith in a strong security presence. Most experts agree that even armed security guards are a relatively poor deterrent to acts of worker-on-worker violence. For example, Dr. James Madero says that only in a few select companies—such as high-risk, single location facilities—will a trained and armed response force effectively contain a violent incident.

In companies with multiple locations, campus environments, or even in single facilities that have three floors or more, the ability of armed officers to effectively mitigate the carnage of a shooting once it is underway is severely limited. Madero believes, as most experts do, that an organization has a better chance of preventing incidents from occurring than containing them once they start.

Crisis alerts. The mass shooting that occurred at Virginia Tech University raised critical issues about active shooter response, and emergency alerting in particular. Especially in open environments, a system for providing emergency alerts is as critical for managing an event as the response of emergency personnel. Unfortunately, there is evidence that the ability of organizations to deliver timely crisis warnings is still lacking.

More than one-third of America’s largest corporations still do not have procedures in place for mass notification, according to results of a study on security in large companies conducted by STAT Resources Inc. (Boston). Additionally, nearly one-half of large companies have not
invested in hardware and software specifically for the purpose of alerting employees to
dangerous or hazardous situations, according to findings released in April 2007.

Workplace violence prevention teams need to take a closer look at developments in crisis
communications technology, recommendations for improving emergency alert programs,
and lessons from the shootings at Virginia Tech.

1. Expanding options. Organizations need to have more than one way to issue emergency
alerts. At colleges, for example, students at a given time are in the library, in classrooms,
walking the grounds, or arriving at campus. Businesses, especially those in a campus environ-
ment, have similar considerations—in addition to traveling workers and telecommuters.

Like schools, organizations should strive to have as many ways to contact stakeholders in
an emergency as those stakeholders have to receive information. For colleges, that has
meant going beyond sending students e-mail alerts and putting emergency notices on
school Web pages. Many are adding siren systems and text-messaging alert networks to
their emergency plan.

One emerging idea in emergency communications management is leveraging peer-to-peer
alerts. Emergency management has traditionally worked on a command-center model—
where announcements and warnings are centrally crafted and delivered and where ‘too
many hands’ are perceived as antithetical to a coordinated response. This is a legitimate
fear, and the traditional emergency model hasn’t been replaced, but some experts now
suggest that emergency managers should keep an eye on incorporating ‘wiki’ strategies
where it makes sense to do so.

The idea is to use people in crisis situations to gather information about an unfolding
crisis, employ them to help spread official alerts, and exploit online-bulletin-board-type
networking to facilitate accounting for individuals during a crisis event. Talk in emergency
communication circles now is sometimes peppered with discussions of “smart swarms,”
ad hoc alert networks,” and “word-of-mouth meshes.” In our view, the current takeaway
from these new ideas isn’t to initiate a wholesale change in strategy but to acknowledge
that limiting communications during a crisis may not always be practical and opening up
to the idea that exploiting informal communication networks, in some cases, may improve
crisis response.

FROM THE FIELD...

Call Police Before You Need to Call 911

One strategy no major company can overlook is to involve law enforcement in planning for an active shooter incident,
says Tim Garcia, investigative programs and events manager for Intel Corporation.

Intel has a specific plan for dealing with such an emergency, which includes education for employees on how to protect
themselves and the establishment of a command center to manage the incident.

Garcia says the company shares the plan with local law enforcement to coordinate incident response. “It includes
active shooter response maps, so they know where we will turn over control to them.”
2. **Leveraging technology.** Technology is at the heart of the most effective mass alert systems, and emergency teams should have an active strategy for staying current with new devices and advances in system design. Popular systems today include public address systems communicated via a secure/encrypted wireless network and distributed through building speakers and communications software that automates companywide notifications via e-mail, phone, PDA, cellular phone, or other portable wireless device. Relatively new technology options also include:

- Desktop computer systems that allow an organization to flash a warning simultaneously on all network computers, which could then be followed with a more detailed e-mail message on the nature of the alert.

- Mobile phones utilizing the Global Positioning System so that individuals can alert security with their location if they are in trouble or the emergency team can locate staff whom it is having trouble reaching.

- Two-way emergency call boxes that can broadcast emergency warnings (in addition to their traditional role of operating as a panic station for individuals in trouble).

---

**Schools Learn Lessons From the Virginia Tech Shooting**

It’s no surprise that the mass shooting on the campus of Virginia Tech caused colleges to reassess their emergency communications capabilities. What did they decide to do? Published reports and interviews reveal some of the mass notification strategies they’re employing:

- Creighton University, the University of New Orleans, and Vanderbilt University are among many institutions examining and implementing an emergency text messaging system.

- The University of California, Berkeley, is looking to add an outdoor public address system to deliver instructions in an emergency. Washington State University spent $114,000 on its new system of speakers that sits atop five buildings and can sound both sirens and specific messages. Indiana University is testing whether siren loudspeakers on its campus can also carry voice messages.

- The University of Georgia is among several universities employing third-party mass communications systems through which students receive emergency messages sent via phone systems outside the local area to avoid congestion in local phone lines.

- The University of Florida and local police are collaborating on a system to automatically send weather-related alerts to campus telephones.

- Montclair State University issued cell phones to students with a link to campus police so they can receive text message alerts.

- In Massachusetts, school administration officials and law enforcement are collaborating on a system to connect participating campuses to a police radio network.

- The University of Nebraska at Lincoln is deploying a campus emergency notification system that allows administrators to broadcast a warning simultaneously across the university’s computers.

- The University of North Carolina in an emergency sends out campus-wide e-mails marked “Urgent” and broadcasts voice-mail messages. A new program will allow its on-campus residents to obtain GPS-enabled cell phones at less-than-market cost.

- Purdue University has created an emergency notification group on a popular social networking Web site to contact students and staff in emergencies (in addition to having sirens, phone trees, and sending e-mail alerts).
• Blackberrys for use by members of the emergency team. These devices are becoming increasingly standard because users can directly communicate using PIN-to-PIN messaging in emergency situations, which has proven reliable in mass emergency events. The devices also support advanced features that can further help emergency team coordination during an event, such as a mapping application that can plot where everyone on a response team is geographically located at any given time. The fact that such devices are useful for everyday work makes them more valuable for emergency communications, according to Rob Moffat, president of Wallace Wireless (www.wallacewireless.com), a maker of mobile applications for enterprise emergency operations. “If you can establish the ROI for Blackberrys for ordinary business use, then you don’t have to sell management on the need to spend additional money for emergency communication devices,” he says. “And it’s already on everyone’s hip, so you don’t have to worry about members of the emergency team being without their devices.”

3. **Keeping it current.** An organization should strive to issue emergency alerts via as many avenues as possible, and it also needs to put in place process elements to ensure that crisis communication is continuously assessed alongside changes in the way individuals communicate. In schools, for example, text messaging—and even podcasts and alerts via social networking sites—now has a role in emergency communications because it has become a common means of receiving information among students. Likewise, all organizations must ensure that their processes for delivering crisis alerts evolve alongside the way employees work, live, and communicate.

4. **Redundancy.** Using many methods to deliver crisis communications helps organizations reach more people, and it also helps when one avenue gets cut off. For example, emergency responders often rely on wireless communications to coordinate operations and provide or receive status alerts, but the infrastructure may not be able to handle the volume of calls that accompany a major event. It reaffirms the lesson that cellular phones can’t be relied upon for emergency communications in a major crisis event.

Companies should assess the extent to which they rely on wireless communication services for disaster recovery and business continuity. Also, consider splitting wireless communication between at least two carriers, provide individuals with long-distance calling cards, and plan for a mix of both low-tech options (such as traditional sirens and fire alarms) with newer options (such as text and cellular phone alerts).

5. **Maintenance and upkeep.** There have been important advances in emergency communications technology, but new devices aren’t devoid of challenges. For example, if an alert system sends 10 text messages per second, it would take a half-hour for 30,000 people to get the warning. Wireless technology can have associated contract costs even when it isn’t used, and simple expenses such as replacement batteries for emergency radios can add up. So while the decision to invest in security and emergency communication devices may seem like a no-brainer, upkeep and maintenance need to be figured into the calculation.

6. **System usage.** Having an emergency communications system provides the necessary foundation for delivering crisis alerts, but it doesn’t inform an organization when to use it or what to say. Effective emergency warnings still rely on the appropriateness of the decisions made by crisis team leaders.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

It’s a critical issue, and not only for life and safety but—as the Virginia Tech case demonstrates—with respect to an organization’s liability. Lawsuits in the wake of crisis events often center on whether an organization decided to issue an alert or not. A crisis event such as a random shooter may not be foreseeable before it occurs but may become legally foreseeable as it unfolds. So the when and what of crisis alerts can have significant legal consequences.

7. Policy and plan development. In a study of the ability of Massachusetts’s schools to handle a violent campus incident, consultants found that one-third of that state’s schools did not have a formal policy for use by their mass notification system. “In such cases, there is no guidance about what kinds of events should initiate the use of the system, who is authorized to launch the system, who should be notified, and what information should be provided.” Consequently, one of the report’s principal recommendations was for all institutions to establish a formal policy for the use of their mass notification system (“Campus Violence Prevention and Response, Best Practices for Massachusetts Higher Education,” Applied Risk Management, 2008).

Consideration should also be given to associated facilities. For example, if a shooting incident occurs at one company facility (or a bomb threat), how do you want other nearby locations to respond? If no plan is in place, organizationwide confusion is likely to result.

8. Training. Alarms and alerts have typically been associated with evacuation, but in an active-shooter incident individuals must be aware that an emergency alert may be giving them the exact opposite instruction. Shelter-in-place has become more important as the risk from an active shooter has grown.

Training of emergency leaders is just as critical. Because the human element will always be critical regardless of the technology in place, companies should routinely conduct exercises to sharpen the ability of crisis managers to evaluate situations and make decisions under duress.

9. Alert message development. Organizations should develop a pre-approved list of emergency messages to choose from during an incident. In a post-incident report following a shooting on a Northern Virginia Community College campus, a commission cited a lack of pre-approved functional language for the initial e-mail and text notification messages. According to minutes from commission meetings, a representative from information technology explained that one of the primary challenges of the day of the incident was to determine the appropriate message to send to the campus community so as not to create a panic. Having to craft messages on the fly can slow notification and is especially challenging in light of strict limits on the number of message characters you may be allowed. In its recommendations section, the report says the college is looking to develop an alert notification policy that provides pre-approved alert notification messages and technology based upon the type of incident.

Mass notification system limitations. Mass notification systems have grown more common, according to an IOMA/SDR survey in October 2009 of 300 security executives. Overall, 39 percent of respondents said their organization has a companywide mass notification system...
capable of delivering emergency text (and/or voice) alert messages to all stakeholders. Another 25 percent said they have such a system covering “some locations.” Thirty-three percent said they do not have such an alert notification system. Hospitals and educational institutions have been most aggressive in adopting them, according to the survey (see Figure 22).

### Figure 22. Prevalence of a Mass Notification System* by Industry, 2010

<table>
<thead>
<tr>
<th>Industry</th>
<th>Yes, companywide</th>
<th>Yes, some locations</th>
<th>No</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing &amp; Production</td>
<td>26.5%</td>
<td>29.4%</td>
<td>44.1%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Banking &amp; Other Financial Services</td>
<td>45.7</td>
<td>30.4</td>
<td>19.6</td>
<td>4.3</td>
</tr>
<tr>
<td>Retail Sales</td>
<td>33.3</td>
<td>14.3</td>
<td>47.6</td>
<td>4.8</td>
</tr>
<tr>
<td>Government</td>
<td>64.3</td>
<td>14.3</td>
<td>21.4</td>
<td>0.0</td>
</tr>
<tr>
<td>Educational Institution</td>
<td>63.6</td>
<td>36.4</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Utility</td>
<td>70.6</td>
<td>17.6</td>
<td>11.8</td>
<td>0.0</td>
</tr>
<tr>
<td>Transportation</td>
<td>35.7</td>
<td>42.9</td>
<td>21.4</td>
<td>0.0</td>
</tr>
<tr>
<td>Entertainment</td>
<td>31.8</td>
<td>22.7</td>
<td>45.5</td>
<td>0.0</td>
</tr>
<tr>
<td>Hospital/Healthcare Facility</td>
<td>53.8</td>
<td>38.5</td>
<td>3.8</td>
<td>3.8</td>
</tr>
<tr>
<td>Security Services</td>
<td>19.6</td>
<td>19.6</td>
<td>55.4</td>
<td>5.4</td>
</tr>
<tr>
<td>Professional, Scientific, Technical, and Business Services</td>
<td>37.5</td>
<td>18.8</td>
<td>43.8</td>
<td>0.0</td>
</tr>
</tbody>
</table>

*Capable of delivering emergency text (and/or voice) alert messages to all stakeholders

(Source: IOMA/SDR Survey on Corporate Security Management, Policy & Practices)

The Panic Problem

In what one student said was “probably the most colossal miscommunication ever,” a phantom campus shooter was the source of panic on the campus of Oklahoma City Community College (OCCC) in February 2010. The incident is a useful teaching tool; it’s also a warning that as an alert system expands, so grows the responsibility for activating it judiciously.

Exactly what happened in the OCCC incident may never be pieced together, but news reports, official statements, and firsthand accounts suggest the following unfortunate chain of events:

1. An e-mail message warning of a possible campus shooting (somewhere in the country) made its way from the Oklahoma Information Fusion Center to the office of campus safety and security and of community outreach and education at OCCC.
2. A student-employee in the outreach office appears to have spread the warning to faculty, including using a campus call box.
3. Overhearing word being passed around about an active shooter, someone called the police.
4. Campus security sent out an alert through the IP phone system instructing students to shelter in place, which many misinterpreted as a fire alarm and instead evacuated and congregated outside campus buildings.
5. Fear that an active shooter was on campus was fueled when a security officer accidentally discharged his gun while searching for the phantom gunman in the campus library.
6. The rumor-turned-alert caused administration officials to send all students and faculty home for the day.

Balancing the dissemination of important information with the risk of causing unnecessary panic is something all organizations must explicitly examine through discussions of the emergency response team. For example, Rutgers University in New Jersey in March 2010 faced the tough task of notifying students while maintaining calm when a threat was discovered on a bathroom wall reading, “Everybody in Hickman [Hall] will die.”
Cell phones are a terrific medium for distributing messages to people wherever they are, and efforts are under way to make networks more robust for handling emergency message loads. But there is an element of hype to current third-party text messaging products, suggest researchers. “Many such services advertise text messaging as an instant, targeted disseminator capable of delivering critical information to tens of thousands of mobile phones when it is most needed.” But those are inflated claims, according to testing. “Such services have been purchased by colleges, universities, and even municipalities hoping to protect the general public. Unfortunately, such systems will not work as advertised.” (“Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Services,” Patrick Traynor, Ph.D., Georgia Institute of Technology, September 2008).

The fundamental problem is that cellular networks are not designed for the delivery of emergency-scale traffic loads. So they simply cannot handle the influx and congestion that blocks the delivery of emergency alerts, according to the research. “Moreover, we have demonstrated that the extra text messaging traffic generated by third-party EAS will cause congestion in the network and may potentially block the delivery of critical information, such as calls between emergency responders or the public to 9-1-1 services.”

The day may come when cellular networks can seamlessly handle mass notification, and protocols being worked on right now are helping to move things in that direction, but it “will take time,” the GIT report warns. Until then, emergency planners need to test systems for their actual capabilities, challenge vendors on their claims, and expect system weaknesses when creating an overall strategy for trying to get word out to stakeholders about an emergency situation.

Additionally, congestion isn’t the only potential drawback that emergency planners must consider:

- Geographic targeting is currently difficult. So sending a text alert to mobile numbers on file for employees or for faculty and staff will deliver alerts to those individuals wherever they are, even if they are hundreds of miles from the danger. Conversely, this type of alert system isn’t helpful for visitors or others who are on-site and in danger but who are not signed up to receive the alert. The GIT researchers view this drawback harshly. “Such services therefore fail to achieve the fundamental property required of EAS infrastructure—that all individuals with a device capable of receiving alerts can do so.

- Message authentication is impossible. As such, recipients need to trust the alerts they receive. However, it is possible for false text alerts to go out (and this has, in fact, occurred). “The implications of this limitation are significant. For instance, in the event of an emergency such as a chemical leak, it would be easy for a malicious party to send an ‘all-clear’ message before the situation was deemed safe. Because it would not be possible for users to verify the source of the information, maliciously induced confusion is a real threat.”

- The order of message delivery isn’t always predictable. The assumption is that text alert messages will be received in the order they are sent, something that emergency planners count on for providing continuity in instructions during the course of a crisis. However, the order that messages go out can be affected by a number of technical factors, and
the effect can be troublesome, note the GIT researchers. The report quoted a Pepperdine University student who said messages during a wildfire evacuation created more confusion than clarity. "Each notification that was sent came through in six to eight text messages . . . And they were jumbled, not even coming in order."

**Social media.** It is not yet clear how a large company might best harness social media to enhance emergency communications in a disaster like a workplace shooting event on a corporate campus—or curb their use to control an alert message. But the speed of the communications revolution demands a substantial rethinking of disaster plans. National emergency planning experts from private organizations and public agencies convened recently and concluded: "The explosion of social media—everything from social networking Web sites to blogs to broadcast text messaging—has changed the way anyone involved in risk communications must look at overall communication plans."

Online information networks are changing the way people communicate during disasters, though it is unclear exactly how. Some companies have indicated they will be using Twitter as their emergency notification system during hurricanes and other emergencies.

"Digital" crisis communications can be valuable to reassure customers, notify the media, or quickly get out your side of the story in an unfolding crisis. The Centers for Disease Control (CDC) uses Twitter to relay information and updates during emergencies, for example. When floods hit Fargo, N.D., forcing evacuations, hospitals used Twitter to inform the media and the public about their status.

Makovsky & Company, a New York City public relations and branding firm, warns that social media are immediate and viral, and that rumors can spread rapidly throughout the Internet via blogs, Twitter, Facebook, and YouTube, which in turn inform traditional media. The result is that a crisis goes public more quickly, requiring companies to update their crisis communication plans, "perhaps with greater frequency given the rapidly changing world of social media," says the firm.

It’s likely that companies will increasingly be integrating social media formally into crisis communication plans. However, this is generally in service of an external audience. It’s less certain that these tools can be reliably used internally by companies to protect people and assets in an emergency. Twitter is unproven as a tool for delivering crisis alert notifications, for example, especially after a denial-of-service temporarily shut it down in August 2009. Regardless, it and other social media (e.g., blogs, social networking sites, RSS feeds, texting, etc.) are already shaping how crises are communicated and responses are coordinated—and some benefits are apparent. They are an avenue for connecting with employees during a crisis, providing instructions, and correcting misinformation—and one way to reach those without access to the company intranet. They also provide a means for jointly responding to employee questions and coordinating internal and external emergency communications.

As an interactive forum, social media generally run counter to top-down, "official" alert systems that are typically the centerpiece of emergency communications. But even if disaster preparedness teams are skeptical of using social media for life safety, their usefulness can’t be ignored—and learning about the available tools is a critical first step. The Virginia Tech
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

campus shooting was a lesson that even if companies don’t use social media in a crisis, employees will be using them to get their information from other sources.

Jim Satterfield, president of Firestorm, a business continuity planning firm, said his group has conducted surveys of businesses and schools, and that both employees and students report learning a majority of information regarding disasters and crises from peers, the Internet, and social networking sites. “Failure to recognize and utilize these channels limits management control in a crisis,” warned Satterfield. “Misinformation in a crisis can be its own disaster and increase confusion.”

Organizations should start with company leaders jointly strategizing on how they want to use social media in a crisis event. Experts say this step is often missed, exacerbated by the fact that a company’s most senior executives are often the least knowledgeable about social media tools and their potential uses. Individual departments may be examining how to use them, but maximizing their effectiveness requires consultation among members of the disaster team, human resources, business continuity leaders, security executives, and corporate communication and public relations teams. Coordination can lead to planning that smooths emergency communications in an event, such as through the development of “dark sites”—digital templates that can be prepared ahead of time for different types of emergencies and filled to quickly go live when an event happens.

Despite questions over its security and reliability, Twitter looks to be the social media tool with the most utility as a disaster notification and alert system—and its popularity is one reason (more than 1,400 percent annual growth). It has also been used successfully, for example, by the Los Angeles Fire Department to provide updates about public rescue operations after a commuter rail crash occurred outside Los Angeles in 2008. An organization that wants to use social media effectively should take stock of which tools are popular among its employees. It also needs to keep track, as popular sites and technology change rapidly.

Twitter recently added a geolocation feature, which means, if activated, the physical location of the individuals posting messages is also reported; it could be very useful to learn the whereabouts of personnel in a terror attack. Again, though, whether tweeting will be possible in a mass disaster event is an open question.

Emergency planning experts from organizations and agencies including Booz Allen Hamilton, Centers for Disease Control, and American National Red Cross offer recommendations that are important for corporate disaster teams to consider as they examine using social media to their best advantage in an emergency (“Expert Round Table on Social Media and Risk Communication During Times of Crisis: Strategic Challenges and Opportunities,” July 2009):

- Centralize use of social media to eliminate multiple communication strategies from multiple departments.
- Be aware of the three main barriers: leadership buy-in, sustainability, and IT/access issues.
- Choose a few social media tools and develop them well (avoid adopting every new tool that emerges as soon as it emerges).
• Get feedback from users.
• Use social media to support a unified message. Instead of creating a new message for social media, use social media to support your existing message in a larger communications model.
• Keep messages brief and pertinent.
• Have a Plan B. Suppose phone lines are jammed and/or computers are down?
• Develop a plan for how you will evaluate the effectiveness of using social media in disaster communications.
• Realize that social media are a moving target, and adapt your communication strategy accordingly.

Security response. Security forces should undergo regular practical training exercises on responding to an active shooter. Surprisingly, even in high-threat environments, such training is not always provided. Following a school shooting in the state, a study was ordered to determine the ability of Massachusetts’s schools to handle a violent campus incident. It discovered that only half of the institutions in the state train security officers on response protocol.

However, while alert notification and hostage-taking security protocol are clearly essential elements of active shooter planning, organizations must also consider planning for a mass casualty medical event. One recent incident provides an excellent case study on this point.

On Valentine’s Day 2008, a former student entered a Northern Illinois University lecture hall at 3:03 p.m. and began shooting students attending an “Introduction to Ocean Sciences” class.

At 3:07, central dispatch received the first emergency call about the gunman, and NIU officers were on the scene within one minute. Yet, by the time they arrived, the attack had already been over for several minutes—lasting just long enough for the killer to squeeze off 60 rounds, including one to his head. The timeline makes the point that—absent successful threat intervention—response to an active shooter will probably be triage rather than the interruption of a shooting in progress.

Even emergency alert notification—which has been the focus of many campus safety initiatives since failures were identified in response to the mass killing at Virginia Tech—is often not rapid enough to make a difference. NIU’s public affairs office—only eight minutes after receiving authorization for an emergency alert—posted an alert on its Web site and simultaneously sent broadcast e-mails and voicemails and recorded a hotline message, stating, “There has been a report of a possible gunman on campus. Get to a safe area and take precautions until given the all-clear. Avoid the King Commons and all buildings in that vicinity.”

The alert notification was critical, effective, and quick; yet, at 3:20 p.m., it came 15 minutes after the shooter was already dead.
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

An active shooter incident is often so swift that the presence or response of security officers is moot, and the NIU shooting provides some useful lessons for improving the often forgotten element of active-shooter planning—triage and treatment.

• **Equipment.** The shooter killed five students and wounded 18, some critically, before killing himself. Early in the response to the mass casualty event, medical equipment shortages were evident, according to a study of the shooting by the U.S. Fire Administration (Northern Illinois University Shooting, U.S. Fire Administration Technical Report Series 167, August 2009). Since the event, NIU pursued a grant to acquire EMS equipment that would be interoperable with the city’s fire and rescue department equipment. Response also highlighted the importance of pre-positioning available supplies at various locations to improve the ability to medically respond to victims. Security teams operating on corporate campuses or manufacturing facilities covering a significant geography need to study where workers are located for the strategic staging of emergency medical equipment and supplies.

• **Lifesaving training.** The Fire Administration’s analysis identified 12 key lessons in areas ranging from the response of the coroner to victim assistance, and it highlighted the emergency medical training of officers. “The NIU officers first on the scene at Cole Hall used their emergency medical training to great advantage. This training is valuable and noteworthy.” It is also critical that security officers’ first aid refreshers reflect updated AED/CPR guidelines.

• **Threat evaluation.** In an event like the shooting at NIU, arriving officers will face the immediate task of ruling out the possibility of other shooters so that emergency medical responders can be cleared to come on site. Training is critical so officers can quickly assess the situation and ask victims the appropriate questions to determine whether a threat still exists. Any delay can slow medical response and add to the casualty count.

• **Victim identification.** Fast response to the scene of a shooting to medically assist victims is critical, but locating fleeing victims and dispatching personnel to help them may prove equally so. Only five critically wounded individuals were in the lecture hall at NIU

---

**FROM THE FIELD...**

**After a Shooting Incident, How Long Would it Take to Announce “All Clear”?**

On Dec. 8, 2009, on the Woodbridge campus of Northern Virginia Community College, a student stood outside his math class with a high powered rifle concealed in a duffel bag waiting for the instructor to arrive and class to start.

“He entered the classroom and proceeded to remove, aim, and successfully fire two shots from his rifle in [the instructor’s] general direction at a distance of no more than six feet,” according to the incident summary. But both shots missed and the gun malfunctioned when the student attempted to reload it; he then left the classroom, sat down in the hallway, and waited for the police to arrive and arrest him.

The incident ended as well as such incidents possibly can, but campus police did not have floor plans and master keys, which considerably slowed the ensuing campuswide search and increased the time to deem the campus clear, restore order, and calm nerves. To speed building searches and more quickly resume operations, the incident report recommended that the school increase the number of authorized personnel that can perform searches. (Report of the Presidential Commission on Safety & Security, Appendix F, “Shooting at the Woodbridge Campus, After Incident Report: Lessons Learned and Recommendations,” March 2010.)
when responders arrived, while the remainder of the shooting victims (13 students) dispersed to five locations away from Cole Hall: the student center, three different dormitories, and the health services building.

• **Triage.** After arriving at a scene, responders will need to make choices about whom to help, so establishing and providing training on mass casualty protocols is essential. In the NIU shooting, “decisions had to be made about whether to use Herculean efforts and all their resources to try to revive victims who were not breathing and had no pulse or to focus first on several victims who, despite significant injuries, might be saved,” according to the investigation.

• **Creating zones from which responders will operate is a critical component of active-shooter planning.** NIU, in the wake of the Virginia Tech shooting, conducted a drill so that arriving emergency personnel would know where to go. It proved to be a great benefit when the real incident occurred. “The group identified specific areas on campus where responding units would be staged, one for fire and EMS resources, another for law enforcement, and so forth.” It’s also important to review the size of staging areas against amount of space emergency vehicles need for maneuver. “Rather quickly, fire officials recognized that Lot 21 was not large enough to handle the number of responding units ... when some pieces of equipment experienced problems turning around. However, even at that location, due to the layout of the campus, responders had to walk about 150 yards to get to Cole Hall.”

• **Traffic control.** This is another essential function that security teams must be prepared to fill during an active-shooter event. Although response to the NIU shooting was excellent overall, a bottleneck of response vehicles occurred at University Circle. “The area became congested, and fire personnel had some difficulties maintaining open lanes for the ambulances.” Many types of responding vehicles were not needed, suggesting the need to meet arriving vehicles as far out from the scene as possible and to prioritize the flow of emergency vehicles.

**Incident aftermath**

“You have companies willing to spend $50 million on surveillance cameras and dedicate three days of training to people on that, but won’t put resources toward helping people cope after something happens,” says Gerald Lewis, Ph.D., director of Gerald Lewis & Associates, P.C. (www.geraldlewis.com). Yet he believes that focusing on helping people “is probably the cheapest thing to throw money at [in crisis response] to get the most bang for the buck.”

Companies tend to offer help to workers for the first two weeks after a major crisis event like a workplace shooting, but then “really drop the ball,” says Lewis. At approximately the two-week mark—when most companies return to business as normal—people need the most support. Sleep disturbance, anxiety, depression, fatigue, and self-medication grow more acute, resulting in performance problems, absenteeism, and aggressive behavior that can lead to additional workplace violence.

Companies may rely on corporate employee assistance programs (EAPs) to address the issue, but these typically put the burden on employees to seek help, and many don’t in the
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

aftermath of a violent event.

The key, as with workplace violence prevention in general, is the training of first- and second-line supervisors. If they understand their people, can spot when they’re having difficulties, receive training in how to support staff, and operate under a corporate mandate that the well-being of workers is a prerequisite for meeting production goals, then companies can help avert the personnel problem that can accompany crisis events.

**Trauma response plan elements.** According to the National Institute for Occupational Safety and Health, a workplace violence policy is incomplete unless it addresses the following points:

1. Specific procedures, including each person’s responsibilities to be taken in the event of a violent incident.
2. How the response team is to be assembled and who is responsible for the immediate care of the victim(s).
3. How to carry out stress debriefing sessions with the victim(s).

Companies that fail to effectively respond to incidents of workplace violence only serve to deepen the impact of the event. An ineffective response may also dampen the effectiveness of future security awareness programs. If employees believe that the corporate response to security incidents is insufficient, they are less likely to believe that the program truly has their best interest at heart.

**Trauma response goals.** The violence prevention team should articulate in the violence prevention plan the goals for the organization’s trauma response program. They are:

- Enable your organization to respond to traumatic security incidents in a systematic manner.
- Demonstrate your organization’s commitment to your employees and their well-being.
- Provide an opportunity for employees to share their experiences with their peers.
- Help organizations identify those employees who need additional help.

To meet those goals, Noreen Tehrani, a researcher with Employee Support Training & Development (Twickenham, U.K.), says core trauma services must be effective at all stages. These are:

- Crisis management and diffusing.
- First-line debriefing.
- Psychological debriefing.
- Trauma counseling.
- Auditing and evaluation.
**Trauma response options.** Key elements of an effective trauma response may include:

- Providing information and offering counseling services to employees and their families.
- Providing a debriefing 24 to 72 hours after a serious incident of violence to all affected employees so that the cause of the violence and expectations can be discussed, a plan of action can be addressed, and those needing further counseling can be identified.
- Allowing employees to take liberal leave/leave of absence.
- Offering counseling for employees not directly involved in the incident.
- Providing a group debriefing for immediate coworkers in how to communicate with the victim/coworker who is re-entering the job after absence.
- Providing ongoing follow-up treatment, as needed.

**Trauma response assessment.** If a violence prevention team questions whether its trauma response is sufficient, Tehrani suggests asking questions within each area commonly used to measure success:

1. **Organizational appropriateness of the program.** Does the trauma response program meet the needs of the organization?

2. **Level of satisfaction by users of the program.** How do users rate your trauma response program? Would they use the service again? Would they recommend it?

3. **Reduction in sick days and medical retirements.** Did the program effectively minimize the days off taken by workers in the wake of an incident? What was the financial benefit?

4. **Quality of the training and education.** How useful was training? How informative did users find the educational materials?

5. **Quality of the professional support for employees and managers.** What was the quality of the professional support? How did employees regard the professionals’ skills? Did the service meet agreed upon service standards?

### I. Partnering

Stephen Doherty, a former police chief and workplace violence consultant, believes the majority of organizations do themselves a disservice by not enlisting greater help from local law enforcement in the effort to curb workplace violence. James Madero, president of Violence Prevention International, agrees that most organizations could probably benefit from taking better advantage of expertise and resources from local sources, such as domestic violence organizations or their insurance carrier.

Workplace violence prevention teams might want to ask two key questions about their use of external resources:

1. **Do we try to handle too many incidents internally?** “It’s a challenge for the company: ‘Do we take care of this internally even if a criminal act has occurred? Do we handle
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

it within HR? That is a tough question,” acknowledged Doherty. “I like to think of it as: ‘If you put the act in the home, or the street, what would the reporting be?’”

2. Is our Rolodex sufficiently full? Companies should be on a “name basis” with at least two members of local law enforcement who are higher than foot patrol level, according to Madero. Organizations also need to have a relationship with a private security company in the event security requirements exceed what the organization can do itself. They should also have the names and contacts for at least one nearby organization that deals with domestic violence, crisis counseling, and threat assessments.

Law enforcement

Even if area law enforcement doesn’t promote their resources to the business community, employers should initiate contact with local police to ascertain their interest in opening a dialogue on workplace violence prevention. Companies can:

- **Invite local police into the firm to promote good relations and to help them become more familiar with your facility.** The police can explain what actions they typically take during incidents involving threats and violence, and visits can help your firm coordinate better with police when incidents do occur.

- **Coordinate plans for response to an active shooter incident.** Police should know where to go to take over operation control of an active shooter incident and who they will coordinate with during the incident. Companies may also enlist police support in conducting site reviews and reviewing incident response plans for recommendations to mitigate damage in an active shooter incident.

- **Share your threat assessment model.** “So if you need to bring in law enforcement, it will already know what process you’ve been through and that the case has been vetted to the point that it has been brought in judiciously,” says Dr. Harley Stock, forensic psychologist and managing partner at Incident Management Group (www.theimg.com).

- **Consider contacting them when preparing for an employee termination.** In these situations, the level of employee threat is the focus, but an organization must also consider its skill in handling the situation and whether police support is necessary. In high-risk scenarios, such as large-scale layoff announcements, companies may also be able to seek the support of law enforcement.

- **Seek better ties with law enforcement to gain access to crime information.** Many cooperative efforts allow private security departments greater access to information such as local crime trends, modus operandi, and real-time incident reports via e-mail trees, Web pages, fax alerts, and telephone calls.

- **Establish guidelines for exchanging information.** This can include acquisition of background information about a worker or job applicant.

- **Develop drills and exercises with local law enforcement.** This may be possible in some locations and for certain facilities, such as academic institutions, in which active
shooter incidents have become a political issue. In New Jersey, for example, the state’s homeland security director noted that more people have died from active shooter incidents than school fires and said the types of drills and exercises that agencies and institutions conduct need to reflect this new reality.

- **Prevent crime through joint efforts.** You may be able to cut crime at your workplace through participating in business improvement districts; consultation services on crime prevention through environmental design; and specially targeted joint efforts on specific topics, including workplace violence.

- **Provide additional training to security staff and employees.** A mainstay of the current crop of cooperative programs between law enforcement and private companies is expertise sharing. Companies can ask law enforcement to speak to their employees on subjects such as drug and alcohol abuse, sexual assault, conflict resolution, and how to avoid being a victim. Law enforcement may also be available to instruct private security forces on evidence gathering techniques and violence prevention. “We also invite police to attend our workplace violence training programs,” says Tim Garcia, investigative programs and events manager for Intel Corporation.

- **Obtain operational support.** Once a company has a closer connection with local law enforcement it is easier to gain support for specific operations where law enforcement expertise may be useful, such as conducting investigations in high-threat cases.

**Using police wisely.** Companies should be aware that calling on law enforcement in a specific incident could have drawbacks. “If you wait to call law enforcement when there is trouble, it’s already too late,” says Garcia. “But there can also be problems from involving police, including a loss of control. They can say, ‘get out of our way,’ and they have a different model of threat assessment. There are often competing agendas,” he said in a presentation at the 2007 annual conference of ASIS International in Las Vegas.

Park Dietz, M.D., Ph.D., president of the Threat Assessment Group Inc. (www.taginc.com) also warns threat assessment teams to be wary of calling for law enforcement assistance “too early.” It is possible that bringing in the police can escalate a low-level problem that could have otherwise been handled internally, he says.

Police readiness and capabilities are an important consideration in this regard. Workplace violence teams should assess the understanding and sensitivity that local police have toward issues of workplace violence, so they can better judge when to call on police to assist with a potentially violent employee. Also, in locations where local law enforcement is less well-trained or lacking in resources, companies may need to enhance their own security measures and use greater caution when faced with potentially dangerous situations.

Stock says a relationship with local police is especially important in smaller communities where police are less likely to understand how a corporate violence prevention program functions, and that it may be necessary to do a certain amount of educating. “Most police agencies don’t have threat management units that are up to speed on this stuff.”
I. VIOLENCE PREVENTION PROGRAM ELEMENTS

In all aspects of threat assessment and incident response, a realistic assessment of the organization’s internal competencies against that of available law enforcement should guide what type of relationship with police is appropriate. “The level of sophistication of the company and police will dictate the level of police involvement you want,” says Stock.

Specialized experts

Organizations need to examine their internal capabilities and form working relationships with outside experts to help formulate, support, or audit a violence prevention program and provide expertise in specialized areas, such as behavioral threat assessment, expert witness testimony, or security technology. Some advice:

1. **Develop a working relationship with a mental health professional who specializes in workplace violence prevention.** Many situations may go beyond the capabilities of the internal threat assessment team and require the assessment of a mental health professional. Violent or antisocial behavior can be the manifestation of mental health issues instead of deep-seated aggressive tendencies, which make the view of a mental health expert critical.

2. **Develop a working relationship with a workplace violence consultant.** Even organizations that possess excellent violence prevention programs should forge a partnership with an external workplace violence consultant, even if his or her role is limited to providing an independent review of the internal workplace violence prevention program. Consultants add an important “second pair of eyes” to violence prevention programs and can act as an on-call adviser to assist the regular team.

Be mindful to choose an independent consultant who will not come in trying to sell you a product. Policy reviews and recommendations typically take 40 hours and cost $6,000 to $10,000. These consultants can then be called upon to serve as an expert witness in the event of a lawsuit, and will be able to testify that you had the right intentions and put a plan into place for the right reasons. Consult the International Association of Professional Security Consultants (www.iapsc.org) for a list of experts in your industry.

3. **Consider utilizing local associations and community organizations.** Participating in a chamber of commerce, security organization, and other area business groups may be helpful for staying abreast of crime trends that could increase the risk of violence at your organization.

4. **Be a careful shopper.** Since the mid-1980s, consultants—among them psychologists, former police officers, and risk managers—have stepped-up to offer workplace violence “solutions” that include tests to measure aggression, training programs, and screening tools for hiring. Not all consultants or programs are equal, however. “The advice you get ranges from okay to bad,” warns Ann Brockhaus of management consulting group Organization Resources Counselors Inc. (www.orcinc.com). Companies should conduct rigorous research before selecting a specific program or vendor. “There are lots of strategies suggested, tried, proposed, and implemented with very little rigorous evaluation,” she notes.
II. CAUSES/COUNTERMEASURES

A media firestorm is certain to follow a mass workplace shooting. The media onslaught that accompanies these extraordinary events—while other types of violence receive no attention at all—makes it a challenge to maintain a realistic view of workplace violence.

The Bureau of Labor Statistics (BLS) seems concerned that employers can get the wrong idea about the risks. “Mass shootings receive a great deal of coverage in the media, as we saw with the Orlando, Fla., office shootings in November 2009 and in the shootings at the manufacturing plant in Albuquerque, N.M., in July 2010,” it writes in a report on workplace violence statistics. It then points that out of 421 workplace shootings recorded in 2008, the highest percentage (24 percent) occurred in retail trade, suggesting—while a shooting can happen in any workplace—it is most likely to occur during the commission of a robbery.

A detailed study conducted by the BLS in 2005 and 2006 examined the frequency of each type of workplace violence. Three sources—criminal, customers/clients, and coworkers—

...
contribute almost equally to workplace violence overall, while incidents caused by domestic violence occur somewhat less frequently (see Figure 23).

However, as noted at the outset of this report, the type of incident most likely to happen at a specific organization depends on its type of work. The vast majority of workplace violence incidents at a convenience store or a bank are criminal, for example, while customer/client incidents occur most frequently at hospitals.

A. Criminal

Workplace violence that results from a criminal motive is a higher consequence incident than most. Examples include a security officer who is assaulted while confronting a gang of trespassers; a female worker who is sexually attacked in the company parking lot while heading to her car; and a retail associate who is attacked after confronting a suspected shoplifter.

At greatest risk are workers who handle cash and valuables, such as convenience store clerks, retail food outlet workers, and taxi drivers. Criminals who confront these workers are often armed and may be on drugs, desperate, and behaving irrationally. “For someone to risk heavy jail time for $100 they must be desperate, and already aren’t thinking straight,” notes Curt Crum, crime prevention unit supervisor in the Boise (Idaho) Police Department.

Robbery

The Uniform Crime Reporting Program defines robbery as the taking or attempting to take anything of value from the care, custody, or control of a person or persons by force or threat of force or violence and/or by putting the victim in fear. Among businesses, convenience stores and gas stations have always been principal targets and—thanks to ubiquitous CCTV and caught-on-tape TV shows—they’re still the stereotypical targets.

However, as noted earlier in this report, as traditional robbery targets such as gas stations have invested in crime prevention and seen a decline in robberies, thieves are hitting general commercial establishments, such as restaurants and retail stores, slightly more often. In a recent report on the quick-serve food industry, for example, security consultant Philip Farina (CEO, Farina and Associates Ltd.) said it is falling behind other industries in robbery...
II. CAUSES/COUNTERMEASURES

prevention and must extend training to workers that includes how to recognize potential warning signs of a robbery.

Things could get even worse, according to consultant and researcher Dr. Rosemary Erickson. The age of the average armed robber is becoming increasingly younger, which raises the likelihood that a robbery will include bodily harm to the victim. Younger perpetrators tend to be more violent than older ones, says Erickson.

Because robberies actually involve relatively small overall monetary losses (the average loss in a convenience store robbery was $712 in 2008, for example) some crime prevention analysts think it is possible that some companies may lose sight of their significance. But unlike other crimes that may have a greater impact on the bottom line, robbery puts employees in physical danger, which demands that companies move it well ahead of others on the risk scale.

There are other reasons that robbery prevention makes fiscal sense.

- Medical payment, when crime is the cause of a worker’s injury, averages $13,882. Only burns and motor vehicle accidents result in higher medical payouts (“Violence in the Workplace—An Updated Analysis,” NCCI research brief, 2008).

- Assault-related injuries are relatively more important as a workers’ compensation matter. Data publicized by the National Council on Compensation Insurance Inc. (www.ncci.com), the nation’s largest provider of workers’ compensation data, shows that average payment in cases where injuries result from acts of crime is $11,381, compared to the overall average of just over $9,000. Only motor vehicle claims cost more on average ($13,2467 per claim).

- The cost of training can be harder to justify since it is difficult for a plaintiff employee to win a lawsuit against his or her employer for injuries sustained during a workplace robbery, but when a robbery occurs at a business where employees have received training, they require less victim assistance or leave time, are less likely to quit within six months, and are more productive more quickly in the wake of the robbery, studies show.

![Figure 24. Large Establishments* Experiencing Criminal Workplace Violence** by Industry, 2006](image-url)

*Organizations with 1,000 or more employees
**In the 12 months prior to survey
Prevention. After an exhaustive review of hundreds of studies of crime at commercial establishments, the National Institute of Justice concluded that robbery prevention is ultimately in a company’s own hands. Its research indicates that crime prevention at the establishment level probably has a bigger impact on crime levels than do increases in penalties or less tangible increases in risks (e.g., quicker police response, increased police presence, or greater numbers of arrests and convictions).

There are numerous security strategies an organization should consider as it searches for solutions that are appropriate for its operation:

1. Employ situational crime prevention. This traditional crime fighting strategy continues to hold up under current crime research, according to Severin Sorenson, president and CEO of Sparta Consulting Corporation, a social science research firm. As a formula for preventing crime at a specific location, it may still cover all the bases better than anything that has come since. The principles:

   • **Increase the effort necessary to commit a crime.** Individuals are less likely to commit a crime at a location that presents barriers to criminal activity—for example, using tough glass and drop-safes, employing additional personnel, and so on.

   • **Increase the risks associated with crime.** The higher they perceive the odds of detection and/or apprehension at a given location, the less likely individuals are to commit a crime there. Some examples of deterrence include: deploying formal surveillance, such as video surveillance, security patrols, and employees trained to spot suspicious activity; and natural surveillance, such as good interior and exterior lighting, removal of shrubs or other obstructions that can provide a hiding place, and eliminating barriers to casual observation of the location.

   • **Reduce the reward of crime.** Criminals, like everyone else, think about their return-on-investment—making it important to reduce what they think they can reap from committing a crime—for example, by minimizing cash-on-hand and securing equipment and property.

2. Employ Crime Prevention Through Environmental Design. Companies should follow the tenets of CPTED (described earlier in this report) and give additional consideration to the countermeasures below:

*Do You Make These Robbery Prevention Mistakes?*

Dr. Corrine Peek-Asa, a researcher at the California Injury Prevention Research Center at the UCLA School of Public Health, says her workplace violence research has identified three primary errors and omissions that businesses make that put staff at risk from robbery-related violence.

1. Tendency to embrace a single aspect of prevention while ignoring others—for example, purchasing a surveillance camera system but not improving cash-handling procedures.

2. Failure to understand what exposures their particular type of business faces and instead reacting to media reports of violent incidents that don’t apply to their risk profile.

3. Failure to use violent events as a catalyst to implement prevention programs.
II. CAUSES/COUNTERMEASURES

- Mind the housekeeping. A clean, orderly place of business is inviting to customers, but not to robbers.
- Abundant indoor and outdoor lighting.
- Windows that offer an unobstructed view of the store’s interior.

3. **Examine each commercial location as an individual.** As we know, a thief on the street picks out his or her victim based on who appears least able to combat their attack, at the same time calculating how much money the attack will likely net them. The idea is to look at the businesses on your street as individuals, and ask whether your business is the “person” on your street that a thief would be most apt to target. If a business finds it is the most attractive target, it needs to immediately improve its security defenses, housekeeping, staffing, and so on, until—at a minimum—it is no longer the easiest target on the block. Longer-term security fixes such as community-based solutions and improving relationships with law enforcement are critical in the long run, but businesses in areas where robbery is on the rise may find that not being the prime target is a good first step to reducing risk. Sometimes, the best short-term answer is to push individuals looking for a place to rob down the block.

4. **Position individuals at primary choke points.** Whether it’s a receptionist at the front of the office or a clerk greeting customers when they enter the store, the presence of an individual eliminates potential perpetrators’ anonymity and raises the risk and effort of robbery. “Psychologically, it’s huge. Criminals hate being noticed, which make employees the very best line of defense,” says Crum. Sorenson agrees, and notes that Wal-Mart has made great loss prevention strides merely by positioning senior citizens at the entryway to greet customers. Although such individuals provide no active security, they have security value by channeling behavior. Research shows that crime occurs most often when there is an absence of visible guardians, notes Sorenson.

5. **Use law enforcement to support your security goals.** Sorenson says that at times in the past he has had to “strong arm” local police to address area crime. His team has gone to great investigative lengths to document crime activity occurring in and around properties in an effort to compel law enforcement to intervene. While not every business will need to

---

**Consider What Crooks Are Reading About Your Security**

Unlikely though it may seem, in recent years there has been a wave of bank robberies in Lancaster County, Pa.: three bank heists in three days, four in two weeks, and five in less than a month. Adding to the confusion of bank security and law enforcement was that each eyewitness reported a very different description of the assailant.

So what was behind the sudden rash of bank robberies? Criminologists and investigators brought in by the FBI believe that news accounts of the robberies sparked a rash of copycat crooks. As the media told tale of each successful bank robbery, a perception took hold in the minds of thieves that local banks were easy targets, and each successful heist hatched the idea in a new crook’s mind.

To adequately assess risk, organizations need to understand what messages the media is broadcasting about potential vulnerabilities at their type of establishment. Even when a company’s actual vulnerability to robbery doesn’t change, its risk can increase depending on the perception of potential thieves.
go to such lengths, all companies should understand how, when, why, and where crime is going on around them, and share that information with police, says Sorenson. Businesses should then identify for law enforcement what assistance they want police to provide in helping to prevent robberies.

6. **Know your crime “times.”** “Does the routine nature of your business create specific crime opportunities? I bet it does,” says Sorenson. To identify the most valuable countermeasures, violence prevention teams should analyze area crime statistics and organizational security incident reports to identify criminal activity by hour of the day, day of the week, and month of the year, he suggests. Companies should also examine if the risk changes due to seasonal factors, such as holidays, prom nights, or nearby sporting events. Also analyze “criminal target data,” such as times when inventories are full or when there is more cash on hand.

7. **Employ a robust video surveillance program.** CCTV systems in retail establishments have a reputation of producing grainy video, and that is if they are in working order. They typically offer little in the way of deterrence as a result. But the price has dropped substantially for color cameras with better resolution, and high-resolution video surveillance systems trained on transaction areas and outside the store can provide meaningful deterrence. To ensure companies get the prevention benefit from their CCTV investment, they should take steps both at the corporate and location level. These include:

- Conduct an annual operational review of all aspects of CCTV operation and management. The review should include CCTV operation, videotape handling, and equipment maintenance.

---

**Companies Join Forces to Deploy Violence Prevention Measure**

The Philadelphia media turned their attention in 2007 to the issue of workplace violence after a gunman fatally shot three men and then himself at a business center in the old Philadelphia Navy Yard. The examination of security measures revealed a novel approach being used by a group of industrial companies. For the safety of workers traveling to and from work (as well as to catch individuals dumping garbage), the firms joined forces to install high-resolution cameras in the neighborhood. To maximize their value, the system feeds video to local police, which officers can access from computers in their cruisers.

---

**Assume Thieves Will Learn Your Vulnerabilities**

Some stores employ phony CCTV cameras to deter robberies and violence, but since robberies often have an insider component, such “false” security may offer no security at all.

Consider the experience of a Staples store in Valley Stream, N.Y. Near closing time, robbers hid inside. They emerged soon after, gained control of the store, and bound and locked a dozen employees in the basement. The robbers planned to get away with roughly $20,000, but when one hostage managed to place a cell phone call to police, the heist was up—and the siege ultimately ended six hours after it began.

Although the robbery went bad, the primary security question is what made the crooks think they could get away with it? According to reviews of police and court reports, the four robbers had an accomplice—a former employee who mapped out the store’s floor plan and provided details about its alarm system. But the primary reason the robbers expected to get away clean was the insider’s tip to his accomplices that the store’s CCTV system wasn’t working.
II. CAUSES/COUNTERMEASURES

- Audit maintenance companies to ensure they meet schedules and follow guidelines to ensure the integrity of CCTV images.

- Conduct spot audits of CCTV systems at several locations. The audit should include a check of picture quality and content and a random review of videotapes to ensure that image quality is to the required standard in daylight and darkness.

- Establish personnel at each location who are responsible for monitoring CCTV systems, immediately reporting problems, and following-up to ensure that problems receive immediate attention.

- If not recording digitally, prevent the degradation of image quality by recording on a VHS/SVHS tape a maximum of 12 times.

- Spot faulty recording machines or tapes by designating a staff person—at the end of each recording period—to rewind the tape and carry out three random spot replays to ensure the recording is of a reasonable quality.

8. **Train staff how to react.** About one-third of robbers injure victims during a robbery attempt. In light of the rise of gratuitous violence in robberies, a survey by the Athena Research Corporation asked robbers about the likelihood of their using violence in such a crime. Most respondents said the reason people get hurt in robberies is because “they resist,” “try to be a hero,” or “make sudden moves.” The second most common reason, robbers admitted, is that they are nervous or high on drugs. So teaching staff not to resist and to remain calm may help prevent a robbery from resulting in injury to staff. Depending on the operation, training may also include the following policies:

- Never open the business to anyone after closing. (Beware of callers who say your business has been broken into and ask you to come down. Confirm—by calling back—that the call was from a law enforcement agency or your alarm company.)

- Vary the times, routes, and methods of concealment for bank deposits and don’t use marked “moneybags.”

- Use only one register at night. Leave other registers empty and open and tilt the register drawer to show there is no money in it.

- Greet customers as they enter.

---

**FROM THE FIELD...**

**Violence Prevention Program Reduces Robberies**

Researchers gave 314 small, high-risk businesses in Los Angeles individualized security consultations, printed materials, training brochures, and a video on keeping employees safe from robbery-related workplace violence. Follow-up visits and a study of crime data show that—although crime rates generally increased for all businesses from the pre- to post-intervention periods—businesses with high compliance to the program experienced a decrease in overall violent crime and robbery.

Stores were most likely to implement the employee-training portion of the program, the study found (“Compliance to a Workplace Violence Prevention Program in Small Businesses,” American Journal of Preventive Medicine, 2004).
• Dress presentably. Well-dressed staff appear more prepared, better trained, and less inviting to would-be robbers.

• Periodically check offices and storage, supply, and other work areas for the presence of unauthorized persons.

• Staff should also be given emergency procedures to use in case of a robbery or security breach and emergency contact numbers and a notification policy.

Training experts warn, however, that instruction on how to respond to a robbery can’t be a one-time thing. Companies that decide to instruct employees on how to react in such a situation must also commit to providing periodic refresher instruction. Studies show that employee skills in this regard diminish sharply over time.

9. **Monitor employees and provide feedback.** Regular monitoring helps ensure that employees continue to use proper work practices. Monitoring should include review of the specific procedures in use and their effectiveness, including a determination of whether the procedures actually used are those specified in the company’s policies and procedures. The review should address any deficiencies, changes that have occurred, employee or customer complaints about lack of security, instances of violence or threats of violence, and whether corrective action is necessary. Giving regular, constructive feedback to employees helps to ensure their commitment to the prevention program. Also, for an effective program, the employer should establish employee sanctions for those employees who chronically and/or purposefully violate administrative controls or work practices. An employee who has been properly trained and consulted after such a violation, but who continues to violate established written work practice, should be disciplined accordingly.

10. **Deploy security measures that will spoil a robber’s plan.** Although CCTV can help catch criminals and may deter some, research shows that crooks are generally more shortsighted in their approach to crime. Their focus is typically on getting the money (or asset) and getting away. Therefore, anything that spoils that plan, such as the lack of money or the lack of an escape route, is a good deterrent. Some ideas:

• Working alarms.

• Time-lock safes.

---

**Does Limiting Cash on Hand Truly Work?**

The strategy has long been considered a best practice, and there is solid evidence that it is effective in cutting robbery rates, according to data from the parent company of 7-11, one of the strategy’s pioneers. The corporation studied incident data pre- and post-implementation and attributes a 65 percent reduction in robbery to the initiation of a $50 cash restriction policy.

Businesses should establish a store policy that sets a limit on how much cash can be in a cash register at one time, and a stricter limit during high-risk time (at night). It also helps to discourage robbers by advertising—through signage—that the store limits the amount of cash in registers.
II. CAUSES/COUNTERMEASURES

• Limit the number of solitary workers, especially at high-risk stores and high-risk times.

• Curtail available cash. During evening and late night hours of operation, cash levels should be kept to a minimal amount per cash register ($50 or less) to conduct business. Transactions with large bills (over $20) should be prohibited.

• Armed security guards.

• In-store panic buttons.

11. Examine modern geographic information systems (GIS). GIS has been a staple of public law enforcement since the 1990s, helping it to map and analyze crime data, identify hotspots, and implement strategic policing. Today’s mapping technology, computer software, and aerial and satellite imagery can also help private companies target security countermeasures and assess whether they work.

For example, some commuting students at Temple University were being victimized in a dodgy area near the rail station closest to the school, so security officials constructed a permanent security kiosk near the station. Although the kiosk seemed to help, the school didn’t know for sure until it used a GIS to reliably evaluate the impact on area crime and found the kiosk reduced crime events by 80 percent in the surrounding radius.

12. Develop an after-incident plan. Preventing robberies must include learning from those incidents in which when prevention fails. A complete plan will include procedures for dealing with robbery events, such as establishing a relationship with a crisis-counseling firm, a process for reviewing incidents and identifying necessary new security measures, debriefing staff, and reporting incidents.

Parking area crime

Workplace violence prevention teams need to make parking facility security assessments a priority. A parking lot is the most common location of a domestic violence assault that occurs at work and the most common site of assaults leading to negligent security lawsuits; violent crime is more likely to occur in a parking facility than in any other commercial facility, according to research by the National Institute of Justice (NIJ).

It’s also critical that parking area security assessments become a regular part of an organization’s security program. Changes can easily occur, such as the improved safety of adjacent areas, that will alter the risk of parking area crime and the security measures that are necessary to prevent it. Organizations should evaluate their parking area security plan every year or, at a minimum, every two years.

In addition to their traditional position as a source of great risk, good reasons have arisen recently to give these hotspots additional scrutiny.

More theft opportunities. An employee who comes across a thief in a parking area is at substantial risk of being assaulted—or worse. That risk is growing now that vehicle theft includes car parts. Companies have always had to deal with the threat of car theft and
vehicle break-ins, but they now must contend with thieves targeting car valuables that can’t be locked up; namely, catalytic converters. This part of a vehicle’s exhaust system contains precious metals that have risen sharply in value, making them desirable targets. It’s not a few isolated incidents, as theft patterns now indicate that thieves have become cognizant of which vehicle makes and models have vulnerably positioned catalytic converters.

**OSHA considers parking areas part of the workplace.** An interpretation letter released in 2008 by the Occupational Safety and Health Administration said that injuries in company parking areas to workers coming and going from work are work-related and thus must be recorded under the agency’s injury and illness recording and reporting requirements (if they meet injury criteria, including whether medical treatment is sought and work days missed). In its interpretation letter, OSHA defined the “work environment” as the establishment and other locations where one or more employees are working or are present as a condition of their employment—and that company parking lots and access roads are included within the definition of “establishment.”

**Parking areas are a flash point in the battle over gun rights.** As previously noted in this report, there is a battle being waged between employers and state legislatures wanting to expand gun rights to include the right of employees to keep guns in their personal vehicles at work. Practically speaking, not much is known about whether these laws have any effect on workplace safety. However, it is a legitimate concern. “If employees have access to firearms stored in their vehicles parked at work, then the potential for workplace disagreements to become lethal increases,” according to Dana Loomis, Ph.D. (“Preventing Gun Violence in the Workplace,” CRISP Report, ASIS International, 2008).

**Solutions.** Workplace violence teams should examine a risk and vulnerability assessment—based on both internal incident data and area crime statistics—to derive appropriate security measures for preventing violence in parking areas.

1. **Design.** In the event of construction or re-design of a parking facility, security or workplace violence prevention representatives should provide input into the design. A design with security in mind can greatly reduce the risk of attacks once the facility is in use, according to NIJ researchers. The NIJ and other experts in crime prevention through environmental design recommend the following security elements for parking structures:

---

**FROM THE FIELD...**

**A Secure Parking Area Is a Good Investment**

Parking lots and security lawsuits too often go hand in hand. Recently, for example, a jury ordered Hahnemann University Hospital in Philadelphia to pay the family of a parking lot attendant $5.5 million in connection with a robbery in which he was shot and killed.

The verdict, in addition to highlighting the inherent threat of parking areas, reminds security departments to follow recommendations made during security audits and reviews. The jury doled out the substantial award amount in part because it came out during trial that, six months before the shooting, a security company had reportedly recommended to the hospital that it install bulletproof glass in the parking booth or automate its parking garage.

The attorney for the victim noted publicly that—in light of the large award—the hospital could have paid off a new automated parking garage in three months.
II. CAUSES/COUNTERMEASURES

- Elevator lobbies and stairs in open parking garages should be open to the parking areas except at roof levels where glass enclosures may be provided for weather protection.

- The ideal solution is a stair and/or elevator waiting area totally open to the exterior and/or the parking areas. If a stair must be enclosed for code purposes or weather protection, glass walls can reduce or eliminate the incidence of both personal injury attacks and various types of vandalism.

- Close off potential hiding places below stairs.

- Access control and perimeter security should always be considered in the initial design stage. CCTV for parking facilities that is implemented as a retrofit is typically twice as expensive.

- Maximize flat parking areas and minimize ramps. Openness enhances natural surveillance. Long-span construction and high ceilings create openness and aid in lighting the facility.

- Pedestrian paths should be carefully planned to concentrate egress. For example, bringing all pedestrians through one portal rather than allowing them to disperse through numerous exits improves the ability to see and be seen by others.

- Concentrate vehicular entrance and egress to a minimum number of locations.

- Locate attendant booths, parking offices, and security stations where attendants can directly monitor activity.

- Avoid dead-end parking areas as well as nooks and crannies in the general design of the parking facility.

- Plant shrubbery away from the facility and keep trimmed to eliminate hiding places.

- Provide security screening or fencing at points of low activity that discourages individuals from entering the facility on foot yet still maintains openness and natural surveillance. A system of fencing, grilles, and doors also may be designed to completely shut down access to the entire facility during unattended hours.

FROM THE FIELD...

Give Parking Area Patrol Officers BOLO Reports

Be-on-the-lookout (BOLO) reports are typically targeted at building entry posts to deny entry to individuals who have been harassing or stalking employees. But it's worth noting that 20 percent of violent crimes that occur in parking facilities are committed by individuals who know the victim, according to the NIJ.

Bonnie Michelman, director of police, security, and outside service at Massachusetts General Hospital, says they are careful to include officers who patrol parking lots and parking lot attendants in BOLO reports and that the strategy has reaped security benefits.
• Ground level pedestrian exits that open into nonsecure areas should be emergency exits only and fitted with panic bar hardware.

• Help orient patrons and allow them to move quickly in and out of the parking facility with careful placement of signs and graphics.

• Use color coding and/or unique memory aids to help patrons easily locate their parked vehicles.

2. Lighting. Lighting is the most important security feature of a parking structure, and one of only a few facility features that has conclusively shown in case studies to reduce crime, according to the NIJ. Workplace violence prevention teams should consult “Lighting for Parking Facilities” guidelines from the Illuminating Engineering Society of North America (IESNA, www.iesna.org) and ensure the company meets its standards.

Companies must remember that the type of light is critical. Parking lots may have plenty of illumination, but brightness isn’t the only important thing. In fact, too much light can create glare that actually reduces visibility. The top three and most critical mistakes in lighting design are (1) lack of understanding of industry standards, (2) inadequate vertical luminance, and (3) poor lighting uniformity. Some things for the team to consider:

• There have been significant improvements in the quality of outdoor lighting, and new products can keep parking areas safer than what many organizations are currently using.

• Consider switching to the white light of metal halide lamps. While its lumen output is slightly lower, it’s spread more evenly over the whole visual spectrum, helping to improve what people see under it. Looking straight ahead, the effective lumen output is 100 percent higher for metal halide lamps than for high-pressure sodium sources. For peripheral vision, detection and reaction to visual stimuli is six times higher. White light also improves color identification and CCTV is far more effective when used in conjunction with the white light of metal halide or fluorescent lamps.

• Use fixtures that emit high levels of vertical illumination.

• Select lighting to optimize performance of outdoor security cameras.

• Work closely with facilities and building managers to make sure security is a primary consideration in choosing lighting.

• Decide on how many lighting fixtures you need and then add 15 percent. This “buffer zone” will compensate for the number of fixtures that may be out of service at any given time.

3. Hard solutions. There is a wide range of security technology and other physical security measures that can improve the safety of parking areas and garages. For example, companies can:

• Limit access by installing automatic gates and card access systems. There are more available than ever to choose from and they can be used to create important safe areas when risks change, such as during a major corporate layoff.
II. CAUSES/COUNTERMEASURES

- Use a white concrete stain on ceilings in parking garages to reflect light and increase lighting uniformity.

- Erase signs identifying parking stalls and spaces. For example, it is not a good idea to have a “Reserved for Director of Human Resources” sign above a parking space.

- Deploy video surveillance cameras. Consider mobile CCTV cameras that ride on tracks back and forth down the length of parking aisles or megapixel cameras that can provide high quality images for a large area. Don’t put up false signs or false cameras, as they give parking patrons a false sense of security and can increase your liability.

- Deploy emergency call systems. Strategically position emergency systems (such as call buttons, blue lights, and so on) to permit an individual in trouble to call for help. These should be tested and verified as working on a regular schedule—once a week if possible. Provide officers on security patrol with a check sheet or handheld electronic device to keep track of tests.

- Distribute personal alarms. Make these available to any employees who feel unsafe walking to their car. Employees can pick one up before they leave so they have a direct link to the security office to report trouble.

4. Soft solutions. In addition to technology, companies should deploy administrative and “people” solutions that are appropriate for their parking areas’ level of risk. Options to consider:

- Coordinate with the maintenance or environmental services department to create a housekeeping plan that promotes security and safety in parking areas. Trash and other signs of wear promote undesirable behavior.

- Provide visible patrols. Studies show that a visible officer presence in parking areas is the security measure that employees most appreciate. Security vehicles with flashing lights offer enhanced deterrence. Alternatively, consider providing uniformed guards with bicycles. There is no better way to get around a parking structure and they are cheap compared to vehicles and can also raise some officers’ level of job satisfaction.

- Use unscheduled security patrols of parking areas with varying routes. In high-risk situations have check-in stations at key locations or use a guard patrol system to record that patrols are being performed, suggest parking security experts at the NIJ.

- Ask new users of a parking facility to assess its security. Security staff and longtime users of a parking structure already know where everything is, whereas new users can point out deficiencies, such as inadequate signs pointing the way to exits, stairs, or emergency call centers.

- Link the location where employees park to employee schedules. For example, a company might assign all third-shift workers to one parking garage level or parking area. This will make workers safer as they go to and from the facility to parking areas because it ensures other workers will be in the same area of the parking facility at the same time.
• Take aggressive steps in the wake of an incident. If a thief knocks down and steals the purse of an employee in the parking garage, a company could try to keep the incident quiet, but this is usually a bad idea since news about the attack will generally spread among workers. A better option may be to respond aggressively via a memo about the incident and the steps the company is taking to make sure it doesn’t happen again. A company might also suggest to workers they use the “buddy system,” and always leave the office with a coworker. Offer security escorts to any employee who feels unsafe walking alone to the garage, and increase the frequency of parking area security patrols.

• “Deputize” employees. The eyes and ears of the average employee are valuable security assets. Encourage them by providing feedback anytime employees make a report to the security department. Ask yourself: If an employee spots someone in the bushes near the employee parking area and calls security to report it, what happens after officers investigate? Would our security department give the employee feedback on what they find? For example, if the “suspicious person” turns out to be a contract maintenance worker installing new outdoor lighting, would you call and let the employee know?

• Audit for the “little things.” Conduct a fresh facility survey to note small things that may be making your parking areas more dangerous. For example, small bushes planted years ago around the parking area may now be big enough to provide cover for an assailant.

• Set up an emergency alert tree with security representatives from other appropriate organizations. Companies in the same industry or in the same geographical area often face similar threats, and an alert tree system can keep you informed of security problems to watch out for, such as a surge in parking lot car break-ins.

Store theft

Retailers must walk a fine line when addressing theft from stores. Stores need to utilize staff as a loss prevention tool. If not, they risk developing a reputation for lax security, which will only encourage other criminals to target the store. However, a thief trying to steal an item from a store shelf may become violent when confronted and assault a store associate, an incident of far greater consequence than the loss of a little merchandise.

The risk to store personnel has increased alongside store theft, which has spiked during the recent period of high home foreclosures, credit defaults, and unemployment. Although other types of crime have decreased as the economy sagged (surprising many experts), opportunistic theft from retail stores has increased sharply.

In a recent survey by the Retail Industry Leaders Association, 78 percent of retailers reported an increase in amateur and opportunistic shoplifting over the previous year (“Current Crime Trends Survey,” January 2010). Large retailers are among the victims, but small and upscale boutique shops are being hit especially hard. With few employees, they are proving vulnerable to grab-and-run thefts.

In commenting about the recent rise in shoplifting, Richard Hollinger, professor of criminology at the University of Florida, said he believes it is being driven by the economy. “A lot of
people are on the financial edge,” he said. Simply put, said Mark Zandi, chief economist of Moody’s Economy.com, “When the economy is down, shoplifting goes up.” So, too, does the risk of a violent clash with store employees.

Retailers often approach workplace violence and loss prevention as separate issues, perhaps even administered by different teams or departments, but most incidents of workplace violence in this environment actually stem from loss prevention activities, according to research by the British Retail Consortium and Maybo, a leading British firm in conflict management. It’s critical for companies to consider the connection between the two issues during strategic planning. Otherwise, it’s possible that the two programs may work against one another.

**Solutions.** The link between violence and loss prevention warrants several considerations.

- Review your current loss prevention policy and assess how it is influencing your number of workplace violence incidents. Do your internal records show that shoplifting stops are resulting in employee victims of violence? If your records mirror national statistics, it is a clear call for loss prevention and workplace violence teams to work closely with one another.

- Make sure your policy is clear—and communicated—regarding who should and should not approach a suspected shoplifter. Audit stores for whether managers and staff groups are being drawn into arrest and detention activities for which they do not have guidance or training.

- Give all employees something to do when they see someone shoplifting (tell a supervisor, call a hotline, write down a description, and so forth). Most often it’s when store associates are unclear on what action to take that they take action for which they do not have training.

- Focus on preventing and deterring shoplifting more than arrests because these strategies will have the value-added benefit of reducing the number of workplace violence incidents. “If businesses wish to reduce assaults and to protect their reputation they need to work on alternative loss prevention strategies that will be more effective in deterring thieves and thereby reducing exposure to physical confrontation,” recommends a Maybo report (“Workplace Violence: A Review of Retail Training Needs”).

- Review the training program for store associates. All employees should receive basic instruction in communicating with potentially violent individuals, conflict management, and personal safety awareness.

- Where arrest is a legitimate option, ensure that staff to whom you give the authority have more comprehensive conflict management training, understand the legal aspects of detention, and possess physical intervention skills in case situations escalate. They should also receive detailed training in how to conduct stops to minimize the risk to nearby employees or shoppers.

- Security personnel, equipment, and training are all necessary parts of a loss prevention policy, and retailers must understand the danger of focusing limited resources on just one or two aspects.
• Provide clear guidance to loss prevention staff on the role of restraint devices, such as handcuffs, and on pursuing suspects.

• Raise line managers’ awareness of how to best support staff in the aftermath of a violent incident. It’s helpful if employee assistance professionals handle such instances.

• Consider how you might be able to improve the incident reporting database to red flag discrepancies between store employee activities and training. For example, a database field that asks for the name of individuals involved in an apprehension could link to a training database indicating whether those individuals have also received training in apprehension and detention.

• Whenever you are developing loss prevention strategies, keep in mind that the majority of assaults on retail staff occur when staff confront, arrest, and detain thieves. “Retailers should first focus on reducing staff exposure to the risk,” Maybo consultants insist.

B. Customers/Clients

The Bureau of Labor Statistics conducted a national study of workplace violence in 2006, examining the types of incidents that occur and what measures companies take to prevent them. In examining the data for discrepancies between incident data and company security measures, one lesson shouts out above all others: Service companies must make dealing with customers a greater focus of their workplace violence prevention program.

The data show that 98 percent of large service companies (those with more than 1,000 employees) specifically address coworker violence as part of their violence prevention program or policy; 84 percent specifically address domestic violence; and 82 percent address client or customer violence. However, clients and customers are actually the most common source of incidents for these establishments, according to the data.

“Workers most likely to experience a violent act on the job do not sit at a desk, they are interacting with the public,” according to Lynn Jenkins, senior scientist at the National Institute for Occupational Safety and Health (NIOSH). Because of it, NIOSH launched an awareness campaign to inform the private sector that retail trades and service industries suffer more than half of workplace murders and 85% of non-fatal assaults.

There are also indications that the risk to public-facing employees is growing. Social scientists’ recent research and surveys suggest a general weakening of the boundary between

The Customer Is (Not Always) Right

A survey of American workers finds that roughly one-quarter suffer the screams, insults, and threats of clients and customers. While not as ripe for catchy “going postal” headlines, “exposure to aggressive behavior at work is associated with a wide range of negative consequences,” according to one of the study’s researchers, Aaron Schat (DeGroote School of Business, McMaster University, Canada). Aggression costs businesses by fostering negative work attitudes, hurting productivity, and increasing absenteeism and turnover.
acceptable and unacceptable behavior in society. Shouting, cursing, name-calling, and other inappropriate behavior by members of the public are increasing—and they can spark a physical altercation if not effectively handled. So organizations need to examine whether deteriorating societal behavior requires expanding employee training for dealing with difficult individuals.

While all employees who have public contact face some risk, five factors tend to define the greater risk to employees in service occupations: handling money and valuables; providing care, advice, or training; carrying out inspection or enforcement duties; working with mentally disturbed, drunk, or potentially violent people; and working alone. Certain characteristics of public contact place some individuals at particular risk, such as dealing

Customers and Clients: Most Commonly Underappreciated Threat

Researchers studying the experiences of 866 Midwestern municipal government employees found that perpetrators of verbal and physical abuse were most commonly outsiders. A study by the Bureau of Labor Statistics also highlights the problem with outsiders—finding that service companies are less likely to train workers on the threat from outsiders than from coworkers, while outsiders account for a greater percentage of incidents. The fact is that customers and clients are a bigger workplace violence problem than many companies think, and more focus should be put on protecting customer-facing workers.

Three Out of Four Doctors Unlikely to Recommend Their Violence Prevention Team

A study of the experiences of 171 ER doctors in Michigan found that 76 percent had been exposed to at least one violent incident during the previous year. Additionally, 12 percent faced confrontations outside the emergency department, and 3.5 percent were victims of stalking away from work (“Workplace Violence: A Survey of Emergency Physicians in the State of Michigan,” Annals of Emergency Medicine, 2005).

The finding that healthcare professionals face workplace violence is nothing new, but the survey’s discovery that ER docs often take security into their own hands is. As a result of facing a violent incident, 20 percent of doctors said they bought a knife and 18 percent bought a gun.

The American College of Emergency Physicians, in the wake of the findings, recommended hospitals to provide adequate security personnel, physical barriers, surveillance equipment, and other security systems, and to educate staff about preventing, recognizing, and dealing with potentially violent situations.
with frustrated customers because of long waits for service, for example, or who take away certain rights, such as prohibiting cell phone usage.

Hospital employees are a prime example of a workgroup that fits the profile for high-risk workers, so it is little surprise that some research studies have estimated that they suffer up to one-quarter of workplace violence incidents worldwide. Assaults occur during times of high patient or family interaction, when patients or family members feel frustrated, vulnerable, and out of control. And they often take place when hospital staff must admit a patient involuntarily, or attempt to limit eating, drinking, or alcohol or tobacco use.

Organizations also need to examine the threat to workers by considering the level of service they provide to outsiders. Crime research by Ryerson Polytechnic University proves that poor service leads to client frustrations—and that these frustrations play a significant role in contributing to threats and attacks against employees.

In light of this fact, risk assessments must look beyond the existence (or absence) of security controls and crime deterrents, such as mirrors, CCTV, access control, duress buttons, and the like. Assessing the risk of violence “must also address the causal factors that give rise to these threats,” says Stephen Schneider, a research consultant and professor of crime prevention.

**Solutions.** As in all areas of violence prevention, protecting staff from customers requires collecting data about incidents (against whom, time of day, cause, and so forth). Adequate data collection allows organizations to conduct trend analyses of threats and incidents. By combining what is known generally about the threat from customers with facility-specific data, organizations can better assess whether their first line of defense is environmental (such as better lighting), administrative (such as more staff), or behavioral (such as training on dealing with intoxicated individuals). Appropriate solutions may be to:

1. Provide staff the training they need to handle potential conflicts with customers or clients. All organizations that have employees with public contact should examine each employee’s job duties, assess what threats they may face as a result, and then arm them with the necessary training (see recommendations for training content for direct service staff in Section I of this report).

**Should At-Risk Workers Have Weapons So They Can Defend Themselves?**

The answer to that question is “no,” according to research of workplace homicides in North Carolina. The study showed that employees in workplaces that allowed guns were seven times more likely to be killed in a workplace homicide than individuals working in places that prohibited all weapons. Workers who were allowed to carry other weapons, such as chemical sprays, bats, and knives, were three times as likely to be killed. (“Employer Policies Toward Guns and the Risk of Homicide in the Workplace,” *American Journal of Public Health*, May 2005).

“I know there are lots of people with guns, especially in retail businesses, [but] I don’t know that they offer any benefit of increased worker safety,” said Dana Loomis, professor of epidemiology at the University of North Carolina at Chapel Hill and the study’s lead author.
II. CAUSES/COUNTERMEASURES

In addition to training elements identified earlier, employees need training to know when to remove themselves from a situation and the organization’s procedures for calling for help. They also need specific guidance on how to spot potentially aggressive individuals and how to respond. Train workers to:

- **Watch for signals.** Watch for: any individual who verbally expresses anger or frustration; threatening gestures or other body language suggesting anger; indications of drug or alcohol use; and the presence of weapons or objects that individuals might use as a weapon.

- **Diffuse anger through behavior.** Exhibit a calm, caring attitude; don’t match a customer’s threats; acknowledge the person’s feelings (for example, “I know you have been waiting a long time…”); and avoid any behavior that individuals may interpret as aggressive (for example, moving rapidly, getting too close, touching, or speaking loudly).

- **Take safety precautions.** Evaluate each situation for potential violence when entering a room or beginning to relate to a client, visitor, or customer; remain vigilant throughout the encounter by looking for signals of escalating frustration; never isolate oneself with a potentially violent person; and never let a potentially violent person stand between you and the door.

2. Ease tensions through addressing environmental factors, such as noise and overcrowding, that can spark tempers (see the “Physical Security” segment in Section I).

3. Improve customer service and response time to minimize customer frustrations that can lead to violence.

4. Examine the facility’s peak crowd periods and evaluate if the physical space is sufficient to minimize personal interaction among members of the public and between public and staff.

5. Arrange furniture so members of the public cannot easily trap employees should a confrontation occur. Also, assess whether furniture poses an unnecessary risk. If so, consider lightweight furniture and fixtures that have a minimal number of sharp edges, and assess which fixtures or furniture should be anchored.

6. Place employees behind protective barriers, if necessary.

7. Make sure signage is clear and easy to understand (even for individuals with limited English language capabilities). Visitors should intuitively understand where they can and cannot go, where restrooms are, and what they can and cannot do in certain areas.

8. Keep waiting rooms, lobbies, and other public areas clean and in good order.

9. Focus on isolated workers whom angry clients may perceive as easy targets. Bringing these workers into the view of others—by positioning staff nearby, for example—dramatically cuts risk.
C. Coworkers

Workplace shootings

As noted at the outset of this report, workplace homicides have decreased steadily over the last decade, and that includes worker-on-worker rampages—one of an organization’s worst nightmares.

But the threat remains, and although media reports may sensationalize the risk from workplace shootings, few corporate events are as devastating. Also, all signs are not good, according to workplace violence consultant and researcher Dr. Rosemary Erickson. She says the number of events may be down, but that a trend toward more deadly multiple-victim incidents may be developing.

Examining workplace shooting data and events reveals the difficulty in establishing a profile of a workplace shooter. One of the most notable recent events, for example, occurred in Goleta, Calif., at a mail processing facility where an ex-worker killed seven employees. But the shooter, Jennifer Sanmarco, hardly fits the profile most associated with rampage events—that of a middle-aged white male military veteran with an interest in guns.

Focusing on employee profiling to spot the next “rampage shooter” is a bad idea, according to Richard V. Denenberg, co-author of *The Violence-Prone Workplace*. And not just because shooters, like Sanmarco, are often “atypical,” but because too many perfectly harmless workers fit the profile, says Denenberg.

Companies must guard against assuming that shootings only happen in blue-collar work environments, like manufacturing or mail facilities. One-third of workplace shootings occur in “white collar” job settings, and when they do they are no less deadly. There is also no evidence that workplace shootings are more or less likely depending on geographic area.

**Common characteristics of worker shooting events.** While the large number of exceptional incidents demonstrates the general futility of trying to profile incidents or employees

---

**Beware of Button-Pushing Supervisors**

After examining aggression among moonlighting workers, researchers concluded that aggressive behavior among workers more often stems from a perception of supervisor mistreatment than the individual’s history of aggressive behavior, low self-esteem, or propensity for violence.

In other words, specific workplace conditions are more often at the source of the problem than the worker’s personality. So while it’s critical to perform background checks and educate supervisors to spot and calm an employee who is ready to explode, it’s equally critical to ensure supervisors don’t light the fuse.

The researchers say to balance your efforts to weed out potentially violent workers with leadership training for supervisors, hiring supervisors with strong interpersonal skills and not just individuals who have the technical skills for the job, and to never assume supervisors know how to treat people fairly.

Be warned: The employee may be the one who blows, but research shows it’s often preceded by both employees and supervisors exchanging abusive and provocative behavior (“Understanding Supervisor-Targeted Aggression: A Within-Person, Between-Jobs Design,” *Journal of Applied Psychology*, 2005).
II. CAUSES/COUNTERMEASURES

likely to explode, common threads often run through workplace shootings. “People who shoot and kill their coworkers share a number of similar characteristics,” according to one study (“Terror Nine to Five: Guns in the American Workplace,” 1994-2003). Some considerations:

- Offenders are likely to be employees who have recently experienced a negative change in employment status, including those who have been fired, whose contracts have not been renewed, or who have been suspended because of a dispute with management.
- Most workplace shootings are committed with handguns.
- The majority of offenders are 40 years old or older.
- An overwhelming majority of workplace shooters are male.
- In roughly one in 10 cases, the shooter has a publicly known history of mental health problems.
- Although study findings vary greatly (from 10 percent to 80 percent), shooters often display well-known warning signs before a shooting incident, including showing guns to coworkers, making threats, or discussing attacks in advance.

Supervisors play a critical role in preventing these types of events. Many companies are making an effort to conduct more rigorous and sophisticated threat assessments and increasingly employing the services of accredited experts to conduct them. But Anna Winningham, vice president of operations at Risk Control Strategies Inc., warns companies that an assessment of a potentially troubled worker requires, first, identifying the threat, which often depends on how aggressively companies recruit supervisors into the violence-prevention mission.

Subtle signs, such as a worker removing all family pictures from his or her cubicle, can sometimes be all the warning a company will get before a workplace rampage. Similarly, the extent to which supervisors piece together warning signs with knowledge of personal stresses, such as divorce, custody battle, bankruptcy, or foreclosure, determines whether they are likely to notify the security department or violence-prevention team of the need for a detailed threat assessment.

Bullying

The last extensive study of workplace bullying—a survey of nearly 8,000 adult U.S. workers in September 2007 by Zogby International—indicates that 12 percent of workers are currently being victimized or have been in the last year.

A separate survey, conducted in 2007 by the Employment Law Alliance (www.employmentlawalliance.com), found that if you ask employees whether they’ve seen or experienced supervisors conducting specific behaviors often characterized as bullying, more than half say they have. “Only an employer in a state of denial would ignore the poll results and not re-examine their personnel policies, supervisor-employee relations, and management training,” said Stephen J. Hirschfeld, Employment Law Alliance’s CEO.
There are indications, however, that some companies do not yet treat the issue seriously as a form of workplace violence. Surveys show that, when reported, most companies do nothing about bullying behavior (see Figure 26).

Some companies not only ignore but may even encourage bullying, according to David Carr, an attorney with Ice Miller LLP (www.icemiller.com) and moderator of a recent American Bar Association panel discussion on the subject. He suggests that some companies continue to cultivate a “rough and tumble” workplace culture—believing it brings better results—which fosters bullying behavior.

The costs and liability associated with bullying are more fully described later in this report, but there is clear evidence that employers pay a hefty price for it. At the company level, workplace bullying links with a lack of trust of management, a poor organizational climate, higher absenteeism and turnover rates, reduced productivity, and higher litigation costs, according to a study by NIOSH. On a worker level, it “increases symptoms of depression, anxiety, and psychosomatic complaints in those victimized and sometimes in those who were not victims themselves but were witnesses present in the work environment” (“Workplace Bullying: What Organizations Are Saying,” NIOSH).

In addition to diminishing company productivity, abusive behavior in the workplace can light the fuse to more severe acts of worker-on-worker violence. Each case of workplace violence is unique, but many incidents that culminate with a violent act of worker-on-worker violence have bullying behaviors at the beginning, according to an FBI report. “It is the threats, harassment, bullying, domestic violence, stalking, emotional abuse, intimidation, and other forms of behavior and physical violence that, if left unchecked, may result in more serious violent behavior,” the report concluded (“Workplace Violence: Issues in Response”).

The FBI notes that “these are the behaviors that supervisors and managers have to deal with every day” and suggests companies must possess a mechanism so that issues and threats are communicated to everyone in the company with a role to play, including security. As the Virginia Tech massacre so tragically illustrated, when institutions keep issues of conflict and warning signs within silos and fail to alert others who need to know, it is harder to appropriately intervene, prevent, and respond to an actual violent incident.

**Definition.** Workplace bullying is repeated, health-harming mistreatment that could involve verbal abuse; threatening, humiliating, or offensive behavior or actions; or work interference.
There is a distinction between workplace “violence” and “bullying.” One research report draws the distinction this way: Workplace violence centers around behavior—that if committed outside the workplace—could be considered criminal (assault, threats, damage to property, verbal obscenities, and so on). Bullying is less likely to have such a “criminal” component.

While intra-organizational workplace violence refers to threats or actual violence, bullying refers to the escalation of aggressive behaviors that result in the victimization of the subject of the bullying—without the threats or violence. Some examples include persistent criticism, withholding information that is vital for effective work performance, spreading malicious rumors, undervaluing effort, humiliation, and “freezing” (isolating) employees out of the workplace.

The definition suggests one of the difficulties in addressing bullying. Supervisors and managers are frequently the perpetrators, but they are the very people to whom many companies ask employees to report incidents of workplace violence.
Policy. Companies should not assume that a strictly worded or zero tolerance workplace violence policy is sufficient to curb workplace bullying. The term “violence,” even when broadly defined in a zero-tolerance policy, may be insufficient. A supervisor would likely not see repeated book slamming as a violent act, and employees are not likely to report the behavior for the same reason. If companies want to curb bullying behavior—and avoid the losses it causes—they need to educate employees about bullying and make a clear declaration that they will not tolerate such behavior.

Workplace bullying is filtering into corporate workplace violence prevention via the language of employment relations, say experts, but there is disagreement on how explicit employers should be in trying to address it. In an address to the annual conference of the Society for Human Resource Management in 2007, Michael Fox, an attorney with Ogletree Deakins, said he thought that a policy would be better off avoiding the words “workplace bullying” and warned that wording that is too specific can set up a company for a cause of action. “Essentially say, ‘Our policy is that you’re entitled to a workplace where you are not harassed for any reason,’” Fox said.

Many violence prevention experts disagree, however, and say that the more explicit the policy, the more effective it is likely to be at preventing the behavior. They also note defining workplace “bullying” makes it easier to adopt anti-bullying policies.

Regardless of how a policy is worded, one thing that all companies must promote is an open-door policy on harassment so that employees feel free to voice their concerns, advises management attorney Caroline Jacobsen Berdzik (Buchanan Ingersoll & Rooney).

And one thing is very clear: Unless a company includes bullying behaviors among those they ask employees to report, it is not likely to learn when it happens. Most victims of workplace bullying suffer silently until they quit, and when they do complain it is usually just informally.

According to a national survey by IOMA/SDR in October 2009, most organizations address bullying behaviors in their workplace violence prevention policy. Overall, 85 percent of organizations do, including a higher percentage of large companies and government and public service organizations (see Figure 29).

Risk factors. The workplace violence prevention team should review the company against workplace bullying risk factors to assess which departments are most likely to be experiencing
II. CAUSES/COUNTERMEASURES

bullying and who is being victimized. Look for the following:

- Where there are deficiencies in leadership behaviors managers and supervisors are at risk of becoming bullies.
- Where employees are physically isolated from coworkers they are at greater risk for being victims of bullying.
- Where workplaces have low morale workplace bullying is more likely to take place.
- Where employees have less ability to control their own work they are more likely to be victims of bullying.
- Where managers work increasing numbers of hours or fear for their job security they are more likely to bully employees.
- Where an employee’s job has conflicting goals or priorities they are more likely to be a victim of bullying.
- Bullies have usually been bullied in the past.
- Bullies often target more than a single victim.
- Men and women are victimized almost equally.

Solutions. Single incidents of bullying are usually not sufficiently severe to punish, and it is difficult to write a policy that can encompass the myriad forms of abusive behavior. (A

Preventing Sexual Bullying Requires Targeting Supervisors

Researchers examined incidents of workplace violence affecting a group of state employees in the Midwest. “While perpetrators of verbal and physical abuse were more likely to be organizational outsiders, perpetrators of sexual violence were more likely to be organizational insiders,” they concluded.

Specifically, the problem is supervisors. Superiors were the source of 62 percent of abuse, harassment, or violence of a sexual nature, compared to 25 percent caused by coworkers, and 13 percent by customers (“The Enemy Is Not Us: Unexpected Workplace Violence Trends,” Jenny M. Hoobler, Ph.D., and Jennifer Swanberg, Ph.D., Public Personnel Management, Fall 2006).

In light of victim interviews, the researchers suggest that three failures are contributing to incidences of sexual misconduct by supervisors:

1. Conflict avoidance (failing to confront superiors who act improperly).
2. Improper and insufficient management training.
3. Failure to recognize early warning signs and intervene (a supervisor who verbally abuses a worker is more likely to sexually harass her or him).
One Company’s Policy Response to Bullying

Goodwill of Southern California has 1,600 employees, and in early 2004 implemented an “interpersonal misconduct” policy. The policy in part notes: “Interpersonal misconduct is an individual’s behavior that bullies, demeans, intimidates, ridicules, insults, frightens, persecutes, exploits, and/or threatens a targeted individual and would be perceived as such by a reasonable person.”

The policy grew out of its four values stipulated in its strategic vision: respect, integrity, service, and excellence. “I felt we should inject those values through a policy rather than just preach the values,” says Douglas Barr, president and CEO. Its policy also has teeth—a Goodwill SoCal employee can be terminated or moved to another location for a violation—although it is more common for individuals to get coaching or training in management techniques.

During the first year of its policy, the organization fired employees who violated it at the senior level in retail, in the business office, and at the store-manager level, according to Barr. However, he noted that the organization is primarily targeting patterns of negative behavior rather than looking to punish single incidents of bullying, unless they are extremely severe.

supervisor who invites his entire team to lunch except for a single individual is clearly engaging in mistreatment, but it is an insidious act that is difficult to specifically address in a policy or sanction.) So it is critical for organizations to address bullying culturally.

An important part of civilizing the workplace culture is to reign in abrasive, difficult managers who get a free pass because they are also “star” performers. The 2007 Zogby survey suggests this is common: Witnesses to bullying said that in 43 percent of cases, the perpetrator of bullying had the support of one or more senior managers or executives. Other lessons from the data and recommended practices:

- Educate workers about unacceptable “bullying” behaviors and the company policy for addressing them.
- Establish a tracking system for the purposes of documenting cases of workplace bullying to assist in the review and improvement of your workplace violence prevention activities.
- Encourage employees to report violations of company anti-bullying policies (make assurance of non-retaliation and confidentiality). Nearly 54 percent of worker mistreatment occurs in front of others. (Note: Male bullies are more likely than female bullies to conduct their mistreatment in view of others.)
- Give workers a place to report behaviors besides their supervisors. Most workplace bullies are bosses (72 percent), which is likely a contributing cause as to why more bullying victims quit than make a complaint.
- Audit the company for the existence of authoritarian managerial styles.
- Assess management competency in dealing with employees.
- Provide sensitivity training and other “people” skills to managers and supervisors.
II. CAUSES/COUNTERMEASURES

• Encourage supervisors and managers to take available time off.

• Audit the company to assess whether workers are working increasingly long hours, and try to keep staffing at optimum levels.

• Examine work autonomy issues in areas of high risk.

• Regularly survey employees or enlist the help of focus groups to gauge the prevalence of risk factors (low morale, job insecurity, conflicting goals and priorities, and so on).

• Ask employees in exit interviews about workplace tension and conflict. Departing employees may be more forthcoming than existing employees—who may fear rocking the boat—about bullying.

• Document all investigative steps and incidents completely. In 31 percent of cases, bullies are themselves a member of a protected class and enjoy civil rights protection. The Workplace Bullying Institute said that from its anecdotal experience, “they are also the ones to threaten employers with lawsuits to stop investigations or attempts to curb the mistreatment.”

D. Domestic Violence

Several presenters at the 2009 ASIS International annual conference in Anaheim said they’ve witnessed the “growing” problem of workplace violence arising from domestic relationships.

“I see violence stemming from personal relationships increasing,” says consultant Richard Sem. Dr. James Madero, president of Violence Prevention International, issued a similar warning, and added that he believes companies generally underestimate the threat.

The sagging economy isn’t helping. “Given the current 10-plus percent unemployment, high rate of foreclosures, personal bankruptcies, and economic uncertainty, domestic violence is on the rise. The workplace becomes an easy access point for violence,” warned Jim Satterfield, president and COO of Firestorm, a crisis-management consultant firm.

Companies pay a particularly high price for not addressing the threat from domestic violence. Not only are they vulnerable to domestic violence spilling over into the workplace, but in the absence of a targeted effort to raise awareness about it, companies are unlikely to ever know that an employee is the victim of domestic abuse at home and yet will suffer

FROM THE FIELD...

Until You Address Domestic Violence, You Won’t Know the Extent of the Problem

One hundred companies in Columbus, Ohio, including JPMorgan Chase and Limited Brands, joined forces to promote workplace strategies to combat domestic violence, including policies, training, and victim assistance.

When it implements a prevention program, a company is likely to be surprised at the number of employees that seek assistance, suggested a Chase representative speaking at a regional forum on workplace violence. She said a pilot program caused requests for assistance to increase 400 percent, suggesting that the company had been missing a considerable opportunity to improve worker productivity and safety.
its consequences. Among them:
low employee morale, lost workdays, increased tardiness, higher medical costs, and costs from hiring temporary employees or paying overtime to make up for absent workers. Job abandonment by victims who are fearful because they are being stalked is also a significant but often unknown cost that companies are paying, according to Robin Runge, a director of the American Bar Association’s Commission on Domestic Violence.

Lost productivity is also a price that companies pay. A Department of Labor guide on preventing domestic violence cites research that found 96 percent of domestic abuse victims have suffered workplace problems as a result. Seventy percent said it impacted their ability to perform their job.

Because of the cost and greater awareness, more companies today are focusing on helping employees with domestic violence and stalking issues, according to Eugene Rugala, a Beaufort, S.C.-based consultant on workplace violence and former supervisory special agent with the FBI’s National Center for the Analysis of Violent Crime. However, although more companies are taking on the issue, data show that the majority of companies fail to treat domestic violence as a workplace issue. Most companies do not include domestic violence during workplace violence training, according to data from the Bureau of Labor Statistics (see Figure 30).

Released in 2009, a study conducted by researchers at the University of Arkansas and funded by the Department of Justice took a comprehensive look at intimate partner violence in two

Companies Tackle Domestic Violence to Boost Productivity

“Traditionally, people felt domestic violence only affected the workplace if there was an actual violent incident in the workplace,” says Steve Heldstab, a specialist in corporate security for State Farm Insurance Companies, which is a member of the Corporate Alliance to End Partner Violence (CAEVP).

Experts put the number of days of work missed each year in the United States from domestic violence at eight million, and absenteeism is just a fraction of the total cost that companies pay for domestic violence. Heldstab and other members of CAEVP say hidden costs of domestic violence include a drop in productivity because victims struggle with the physical and emotional challenges of the abuse.

To examine what more than one dozen companies are doing to address domestic violence, see the “best practices” section of the CAEVP Web site (www.caepv.org).
phases—including examining 2,400 employed men and women in three companies (in the education, health services, and transportation industries) in 39 states (Study of the Effects of Intimate Partner Violence on the Workplace, Carol Reeves, Ph.D., Anne O’Leary-Kelly, Ph.D., June 2009). From the results, several lessons emerge:

1. **It’s likely that more employees are victims than you think.** The detailed study called the high rate of intimate partner violence (IPV) victims “startling.” More than 10 percent of both male and female employees are current victims of IPV (within last 12 months), experiencing at least one of five types of violence: threats, stalking, physical aggression, being hurt, or sexual abuse. Furthermore, an additional 30 percent of women and 19 percent of men reported experiencing IPV sometime during their working life. “Our results provide strong evidence that IPV victimization is prevalent in work organizations,” the study concluded. “When current and lifetime victimization rates are combined, we find staggering prevalence rates—over 29% of men and 40% of women in our sample of employed individuals report having been abused at some point.”

Note: It’s surprising that as many men as women report being “current victims” of IPV. It is significant, however, that women reported a higher degree of victimization.

2. **It comes into the workplace.** The report drives home the point that domestic violence doesn’t stay at home. “Our findings demonstrate that a large number of IPV incidents occur at work.” Overall, 18.8 percent of employees who reported currently being victimized indicated that some form of IPV (threats, stalking, physical aggression, being hurt, or sexual abuse) had occurred on their work premises.

Victims who had experienced threats of physical harm reported a fairly substantial percentage of work occurrences, with nearly 9 percent of those who experienced this form of IPV indicating that it had occurred at least once on work premises, the study concluded. Two percent of victims of IPV who suffered physical aggression endured it at work, and over 50% of victims experiencing stalking said it had occurred at least once at their place of work (see Figure 31).

3. **Victims are unlikely to formally report their victimization.** Workplace violence teams may underestimate the risk because when victims tell someone at work—which is only 55 percent of the time—they very rarely tell security or human resources. Usually, it’s only a coworker they confide in (see Figure 32). “From a practical standpoint this means that organizations should not expect policies and procedures that require formal reporting to be entirely effective.” From a security standpoint, it’s clear that basing workplace violence mitigation on formal reports to security or HR will not adequately address the risk.

<table>
<thead>
<tr>
<th>Figure 31. Current IPV Victims Reporting Victimization at Work, 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of Abuse</strong></td>
</tr>
<tr>
<td>Threats</td>
</tr>
<tr>
<td>Stalking</td>
</tr>
<tr>
<td>Physical aggression</td>
</tr>
<tr>
<td>Being hurt</td>
</tr>
<tr>
<td>Sexual abuse</td>
</tr>
<tr>
<td>Overall</td>
</tr>
</tbody>
</table>

(Source: Study of the Effects of Intimate Partner Violence on the Workplace)
workplace incidents to look for useful threat information. Because an incident can happen anytime, anywhere, and to anyone, profiling is dicey. Still, the study reveals some useful data for violence prevention teams to consider as they examine the threat and choice of countermeasures, particularly when a company is made aware of a high-threat situation involving an employee victim of domestic violence.

The study examined 500 assaults that occurred in the workplace as a result of domestic violence. Just over half of the incidents they studied ended in at least one homicide (Domestic Violence Assaults in the Workplace Study, Peace at Work, October 2009). The greatest risk occurs after employee victims have left an abusive relationship, because one of the easiest places to find them is at their workplace, notes the report. From these 500 case studies, data indicate the following:

- **Other victims are not typical but not uncommon.** In 42 percent of the workplace assaults examined, someone in addition to the target victim of domestic abuse was caught up in the violence. Most often, the additional victims were coworkers, often injured during an attempt to help the victim.

- **The position of the employee in the organization doesn’t seem to be a factor.** Most victims of domestic violence assaults in the workplace are line workers, but individuals in management positions (supervisors, managers, and directors) were also numbered among the victims. The rate of victimization was generally consistent with division of labor in the general workforce, the study notes.

- **Hired perpetrators are not typical but not entirely unlikely (especially when the victim of domestic violence is male).** When a perpetrator is threatening an employee victim of domestic abuse, security teams typically issue BOLO (Be-On-The-Lookout) reports to key staff. It’s a wise countermeasure, but it’s worth noting that in 6 percent of the 500 assaults
II. CAUSES/COUNTERMEASURES

studied, the aggressor had hired or enlisted someone else to commit the actual workplace assault. Similar to domestic violence rates in general, most victims of domestic assaults at work are female (92 percent). However, female aggressors are much more likely to hire or enlist someone else to commit the workplace assault on their behalf (29 percent of the time).

- Any type of relationship can spark a workplace assault. The random study of assault cases reflected a fairly even spread regarding the type of relationship between the abuser and victim. In some cases they were married, in slightly more cases they were separated or divorced, but even more frequently the two were dating (involved but with no marital status). Even “online” relationships can spark assaults at work because it is the attitude of the perpetrator—rather than the objective seriousness of the relationship—that fuels the aggression.

- In the parking lot at the start of the shift is especially dangerous. Security teams that know an employee is being threatened need to provide support as soon as that employee arrives at work, the study emphasizes. Most domestic violence assaults in the workplace occur in the parking lot at the start of the shift (see Figure 33). It’s one of the key takeaways from the study, according to its authors. “A frequent occurrence is when the abuser was waiting in the parking lot for the victim to arrive or leave work. Victims are more vulnerable here, as the assailant would have more difficulty hiding a rifle or shotgun as they entered a facility.” Companies with limited security resources should focus their spending on extra parking lot patrols at the start of a shift, according to the report.

Solutions. To manage intimate partner violence in the workplace, the Study of the Effects of Intimate Partner Violence on the Workplace points to four basic requirements.

- Management must demonstrate to all employees (both victims and coworkers) that IPV is an issue it thinks is important and relevant to the workplace.

- The organizations must communicate support for IPV victims through training, security support, and policies.

- If a worker discloses victimization, the organization must communicate concern by offering help (including safety measures) and making certain the victim knows that his or her job is secure.

Figure 33. Where & When Domestic Violence Assaults in the Workplace Occur

(Source: Peace at Work, 2009)
• An organization should communicate expectations for coworkers who become aware of the victimization of another employee through training and organizational policies.

Complicating prevention is the reluctance of employees to alert supervisors to potential problems. Complaining to a boss about issues outside of work such as an abusive spouse is not viewed as a smart career move, especially as layoffs increase and workers suspect supervisors are looking to identify those whose productivity is lagging.

Violence-prevention awareness needs to be particularly aggressive in promoting the security services it offers to employee victims of domestic violence. Workers need to feel their company will support them if they face safety issues away from work rather than consider the issues a problem; otherwise companies may never learn about a threat until it shoots its way through the front door.

There are two important sides to addressing the domestic violence issue in the workplace:

1. **Awareness promotion.** When The Body Shop first tackled the issue years ago, it did so by kicking off a “Shatter the Silence” program to reach out to employees. The program included posting information about domestic violence along with crisis numbers inside bathroom stalls and hiring expert trainers to provide each employee with two hours of education on domestic violence, including the “power cycle” that characterizes it. Other activities may include:

   • Hold a workshop on domestic violence or designate a “domestic violence awareness week.” Hold such seminars during business hours to show workers you’re serious about the issue.

   • Collaborate and coordinate resources with area battered women’s shelters.

   • Write an article for your company’s newsletter on security and safety issues surrounding domestic violence.

   • Ask a senior executive to raise the issue’s profile by getting him or her to participate in an event, such as volunteering at a shelter for battered women or by sending out a letter explaining to workers your commitment to helping employee victims of stalking or domestic violence.

---

**DTE Takes Aim at Domestic Violence**

DTE Energy Co., an electric and gas utility company in Detroit that employs 11,000 workers, is addressing domestic violence and its impact on the workplace.

“We’re not trying to [delve] into their personal lives but we try to help them out,” says Michael Lynch, the company’s chief security officer. “We change work locations for the employee, change their hours, and create a safety plan so the person knows where the emergency exit is.”

DTE also provides employees threatened with domestic violence with protected parking spaces at work and time off for court appearances, and company officials offer to escort employees to court.
II. CAUSES/COUNTERMEASURES

• Contact the National Workplace Resource Center (NWRC) on Domestic Violence to get additional materials, including examples of corporate domestic violence prevention programs and employee education materials (NWRC, http://endabuse.org).

• Educate supervisors on how to look for indicators that an employee is experiencing trouble at home. Though most companies train their supervisors to stay out of workers’ personal lives, managers should be educated about warning signs and receive training in how to skillfully address the issue with workers. Supervisors shouldn’t be unnecessarily intrusive and should respect workers’ privacy, but they should know enough about their staff to be able to spot signs of trouble at home and offer assistance.

• Foster a positive environment in which employees will report victimization and be supportive of them. Make employees aware what resources are available to them to help with domestic situations, such as workplace counseling, police protection, or help with filing restraining orders. Studies show that providing support has many positive consequences for both the organization and for the victimized employee. Positive outcomes include minimizing work absences and productivity problems that often afflict victims.

• Because victims of intimate partner violence usually inform coworkers, procedures and training that help these colleagues understand their role in IPV reporting is critical.

2. Security assistance. Companies also need to take security and safety measures in specific cases of domestic violence to prevent it from spilling into the workplace.

• Develop a safety plan for any employee who tells you they feel threatened at work. Investigate all legal remedies you have at your disposal. For example, in California, under its Workplace Violence Safety Act, employers can seek a temporary restraining order and injunctive relief “on behalf of the employee” if the employee has received a credible threat of violence that could reasonably be carried out at the workplace.

• Do not rely on the surveillance and monitoring infrastructure to provide deterrence of this type of workplace violence. Perpetrators of domestic violence assaults at work aren’t worried about evading recognition.

• Provide employee victims with specially assigned parking spaces and/or provide escorts to take them to the bus, subway, or whatever type of transportation they take home from work.

• Change a victim’s parking area to one closer to an entrance.

• Counsel victims about the various civil and criminal options available to them, such as obtaining a restraining order to keep the perpetrator off of company property.

• Assist victims with legal action such as filing charges with the police or obtaining a restraining order.

• Assess the feasibility of providing “panic buttons” so employees can call for help.

• Provide a safe place in your facility where you can hide a worker who is the victim of domestic violence should his or her abuser come to the workplace.
• Provide advance warning and photographs to security guards and receptionists in case the stalker/partner tries to gain access to the worksite.

• Obtain identifying personal information about the partner (e.g., date of birth, Social Security number, etc.) and a copy of any restraining order (critical if you need to place an emergency call to the police).

• Conduct a criminal background check of the abuser to assess any tendency toward violence and assess the appropriateness of different workplace countermeasures.

• Don’t believe that securing a “Trespass Restriction Order” provides employee victims of domestic abuse significant protection against a workplace assault. Studies show that although a TRO bans abusers from firearm possession, perpetrators are rarely mandated to relinquish their weapons.

• Provide a temporary cell phone to the employee for emergency calls.

• Screen the incoming phone calls of employee victims.

• Discuss the feasibility of other actions with HR and supervisors, such as fluctuating the employee’s work hours, changing their phone extension, relocating them to another workstation, or providing a leave of absence if the threat is acute.

• Establish personal contact with local law enforcement and ask their help in enforcing any restraining order.

• Educate employees to limit the information they disclose about coworkers over the phone. They shouldn’t release information that would help a stalker/partner locate the employee or, if the employee is out of the office, inform them of when she or he will return. (This is a good policy to have in place at all times for all employees.)

• Make employees aware of actions to take if they see someone who poses a threat on the premises (such as in the parking lot as they arrive for work). Establishing and carrying out a response plan—calling law enforcement, notifying security and management, locking facility entrances, and warning targeted victims—may be the best chance to prevent a tragedy when a situation of domestic violence spills into the workplace.
III. CONTRIBUTING FACTORS/MITIGATION

In addition to the sources and causes of workplace violence examined in Section II, there are specific events, issues, and conditions that raise the potential for violence and conflict in the workplace that violence prevention teams need to address. And although it may be a challenge, the goal should be to address these contributing factors before an incident occurs.

“Intervention before is much better, but this means putting money in something where nothing is apparently happening,” says Vittorio Di Martino, an international consultant in Switzerland on stress and violence and co-author of Violence at Work. “Companies may question why they should spend money to tackle violence before,” he says. “But after is too late, and extremely costly.”

A. Adverse Employment Actions

The risk of violence is particularly acute when a negative work event (real or perceived), such as termination, demotion, or reprimand occurs to individuals who:

- have a tendency to blame others for their own deficiencies;
- possess a small social support network; and
- place extraordinary emphasis on their job.

Although this is a useful profile of which to be mindful, it is not a robust strategy for violence-prevention teams to attempt to identify which individuals might take bad news badly. Rather, companies should strive to improve their overall process for delivering news that could potentially trigger violent response.

A national survey of 752 workers in June 2007 by Harris Interactive for the Marlin Co. reflects
the difficulties that some companies have in facing up to this difficult task. Some 10 percent of employees say their company has used e-mail to fire or lay-off staff. And 17 percent said their boss had used e-mails to avoid other difficult face-to-face conversations.

“E-mail has become the new shield of today’s business. Companies hide behind it to avoid the negative reactions of unhappy employees,” says Frank Kenna III, president of the Marlin Co. “While e-mail works fine for day-to-day communication, the last thing you want to do is use it for something as sensitive as layoffs,” Kenna notes. “That risks turning former employees into disgruntled ones.”

Managers and supervisors who deliver bad news, such as denying a worker a promotion or delivering a poor performance review, need management training to handle the situation in a manner that reduces the possibility that the employee will respond violently to the negative news. Organizations also need a mechanism so that when bad news is going to be delivered to a worker with a problematic history, the situation is first reviewed by the threat assessment team so that any necessary precautions can be taken.

Terminations
Corporate belt-tightening and high unemployment remain fixtures of the economy even now that the recession has technically ended. This fact means companies will continue to trim payrolls and replace underperforming workers into the foreseeable future.

Managing Bad News Is Critical to Prevent Ugly Incidents

When a worker turns a gun on a coworker, the odds are better than 50 percent it’s because he or she has recently received a pink slip, a demotion, a pay cut, or suffered some other negative work-related event. That is why a threat assessment should precede the delivery of all such reports.

A Tuesday morning shooting in March 2010 at Ohio State University is just one of the recent cases in point. A janitor entered a campus maintenance building, walked to an office suite, and shot two supervisors, killing one. The search for an answer to the community and media firestorm of “why?” yielded the spark—a university letter sent a few days earlier had informed the worker that because of performance problems his last day of work would be Saturday.

Nothing in press reports suggests the university invited the tragedy. A standard employment background check failed to turn up a stint in prison for receiving stolen property, but to be fair, it was more than a decade earlier and not typically a disqualifier for the type of job he was hired to perform. He was also still a probationary employee, hired only a few months earlier, so when supervisors complained he was late for work and caught sleeping on the job, it was routine for the university to send out a sorry-but-things-aren’t-working-out letter.

In the wake of a shooting, alternative approaches might seem smarter—maybe a more personal approach or immediate termination rather than letting him finish the week—but it’s not clear (it never is) that it would have made a difference.

However, one opportunity to prevent trouble always exists no matter how, where, or when a termination takes place—the watchful eye of security staff. It’s unclear if Ohio State University security personnel were notified of the worker’s status, but the description of his arrival to work after he received notification that his employment was to end—in dark clothing, a hooded sweat shirt, and a backpack—suggests that security personnel might have had some small chance to spot potential trouble if they had been instructed to watch for his arrival to work that day.
A job termination is an especially delicate task—one that should follow a specific security game plan every time it happens. In a survey by the Society for Human Resource Management, 4 percent of companies said that an employee termination at their workplace caused a violent incident in the previous year.

Although the danger is rather obvious, Richard Sem, a consultant and regular expert witness in workplace violence cases, says he still sees employers mishandle these events. “I still see the ‘perp walk,’” says Sem, in which a fired worker is paraded past his coworkers with a box of belongings from his or her desk. “Helping workers preserve their dignity is important, so they still have something left to lose,” he says. Sem says it’s when a worker feels he or she has lost everything that a violent incident is most likely.

Risk assessment. Prior to delivering bad news to an employee, organizations need to spend sufficient time reviewing the individual’s employment history to look for signs that special security measures might be necessary. For example, employees with a history of violence or threats represent a higher risk, and termination of such employees should follow the strictest of the security measures outlined in this section. If the employee’s record shows he or she has a history of filing grievances or lawsuits, companies should also be on high alert, as studies show that such individuals pose a greater risk of future violence. Finally, long-term employees actually present a greater threat in the wake of job terminations. Studies show reliable “company” employees with many years on the job are more likely to react violently to a perceived unfairness (being fired or passed over for promotion) than shorter-term employees. The more value an employee attaches to the job, the more stressful he or she finds a disruption in job status.

While it is wise for companies to conduct careful reviews of employee records and interview supervisors to gauge the potential for violence, there will be no red flags in some violent situations. All terminations, even ones that are expected to go smoothly, should follow the relevant security recommendations outlined below. Some terminations may demand an extra security presence, but all bad news delivered to employees in the work setting should be recognized as high-risk situations.

Furthermore, the threat from violence associated with terminations does not end on the day of discharge. The mean length of time for acts of workplace violence following termination is six months, as resentment toward the previous employer often intensifies when a fired employee can’t find new employment. Unfortunately, many companies only remain on high alert for one to two months following terminations.

FROM THE FIELD...

A Troubled Employer Devises a New Strategy for Terminations

The United States Postal Service (USPS) has certainly had its share of high-profile problems with disgruntled ex-workers, but they’ve worked hard to address the risk by implementing a “soft exit program” to provide managers with a support system when they have to fire an employee. An HR representative joins the supervisor during a termination and speaks with the employee about any unresolved issues, such as benefits, pay, etc. The employee is told to address any further questions to HR. “We’ve taken the supervisor out of the communication link,” says Bradley Johnson, an HR specialist with the USPS. It’s critical that a relationship that is likely bad already not be allowed to get worse through additional contact between the parties, he notes.
Security procedures. The mechanics of a termination (location, time, and so on) can minimize risk by removing the opportunity for violence. Workplace violence prevention teams should help their organization to develop a written policy on how to conduct layoffs or terminations, including the identification of all individuals who need to be notified in advance of the event. “Sometimes line managers, the HR department, security, and legal departments find themselves at cross-purposes. We urge each client to seek a cross-disciplinary, team-based solution to these problems with guidance from a qualified mental health professional,” says Frederick Foster, executive vice president for Seventrees Corporation (www.7trees.com), a specialized protection services company. “It is important to limit the effect of personal feelings and arrive at a consensus decision on a course of action that everyone can live with,” he advises.

Although the recommended practices described below are not universally applicable, they have been shown to be effective for reducing violence during terminations.

1. **When to do it.** On Fridays, according to William Abney, a researcher on workplace violence and professor at Eastern Kentucky University. Abney says that not having a job to go to the day after a termination can be a trigger for violence. Friday pink slips can be less traumatic in the short term because workers do not normally go to work the next day anyway. If termination must come on other days, do it at the end of the shift or the end of the business day to minimize embarrassment to the discharged employee.

2. **Where to do it.** Terminations are best conducted in a neutral setting. Don’t do it in a supervisor’s office, Abney warns, because it can heighten the employee’s feelings of anger. Instead, use a conference room or some other neutral setting that is less familiar to the worker. The room should also be private. Don’t fire a worker in a cubicle-style office because they don’t afford privacy and, if violence erupts, it will unnecessarily endanger other workers. The selected location should also be as close to the entrance as possible, with minimum glass, few furnishings, and two or more doors that lead in and out, according to Foster.

If a risk assessment does not indicate that security staff need to be positioned outside the door, it is a good idea to use a setting that is equipped with a silent alarm or has some other means of allowing security to quickly receive notice that there is trouble (such as

---

**A Worker’s Revenge Can Take Many Forms**

Workplace tragedies are often sparked when a worker, perceiving some sort of injustice, strikes back in violent retribution. But one threat that can’t be overlooked is “logic bombs” (malicious software bugs) planted by individuals with network access angry at being laid off.

Case in point: An IT contractor terminated by Fannie Mae apparently retained his systems access long enough to plant a virus on the company’s network. Had it not been discovered—and had it executed on schedule—it would have destroyed and altered massive amounts of data on Fannie Mae’s 4,000 computer servers nationwide, according to a federal indictment handed down in January 2009. Security executives should take special care to examine the threat from fired contractors because they are handled differently in the payroll system, and fall through the cracks in the account deprovisioning process.
video surveillance). Note: If the employee has issued threats of violence before termination, plainclothes security professionals should always be present or nearby at the time of the termination.

3. **Who should do it.** Generally speaking, the employee’s supervisor is not the best person to notify an employee of termination. Preferably, someone higher up in the company hierarchy and slightly removed from the situation should handle it. Additionally, this individual needs to have training in how to de-escalate violent situations or be accompanied by someone who does.

Training supervisors in workplace violence prevention is critical in this regard because, although supervisors should not typically fire employees directly, they are in the best position to assess the violence potential of individuals prior to termination. If supervisors are well trained in the warning signs exhibited by potentially violent employees, they can act as a vital security asset by recommending when your company needs to take extraordinary security precautions during a dismissal. Supervisors may also need to occasionally deliver other types of unwanted news to employees, making it important that they have the skills to do so effectively.

4. **How long it should take.** The entire termination process should last no longer than 15 minutes, according to Foster, and difficult terminations should be as brief as possible. Notification of the firing should be in the first sentence of the conversation rather than building up to the news. The dismissal must be direct and leave no room for confusion, adds Foster.

To expedite the process, have all the materials necessary to complete the termination process at hand, including a written explanation of any severance benefits or counseling or outplacement services and the name of the specific company manager with whom they need to make any necessary future contact. Also, never take a break during the termination, warns James Madero. He says he’s seen cases in which employees have asked for a break during the firing, gone to their desk to retrieve a gun, and returned firing.

And although terminations should not be a drawn-out process, companies shouldn’t appear in a rush; they should display as much humanity as possible. “We need to remember that terminations are devastating,” says Bonnie Michelman, Director of Police, Security and Outside Services at Massachusetts General Hospital. “I think that it is a tough balance

---

### Keep Track of High-Risk Workers After Termination

How long do you keep on alert for fired workers? As a result of erratic behavior in 2003, Jennifer Sanmarco was escorted out of the postal facility in Goleta, Calif., where she worked. Armed with a 9-millimeter pistol, she returned later—three years later—and killed seven people.

That’s a long time to hold a grudge (and longer than “high alert” status can be maintained), but it’s a tragic reminder to companies that former workers can pose a threat for a long time after being fired. In fact, because resentment often intensifies when fired workers can’t find a new job, they are statistically as likely to return and commit workplace homicide six months after the fact as six days.

---

**FROM THE FIELD...**
because we need to ensure security but treat people with incredible dignity.”

**High-risk terminations.** Depending on the conclusions reached after a threat assessment, other security measures may be necessary during terminations.

- Have security staff stay with an employee you believe might be dangerous until he or she leaves the premises. After discharging a disgruntled and potentially violent employee, do not allow him or her to return to their desk unescorted to retrieve personal belongings—they could have a weapon stashed there. Only use quality officers for this detail, suggests Foster, ones whom you trust to handle the dismissal quickly and smoothly without unnecessarily confronting or humiliating the exiting employee.

- Anytime an organization is firing an individual for behavioral problems, it should position security staff in or just outside the room, advises Michelman.

- If the employee being terminated has previously issued threats of violence, a protection team of security professionals in plain clothes should be available during the termination and at any subsequent hearings, says Foster. They should also remain onsite for a reasonable period of time to ensure that the individual does not return. Organizations need to inform all “gatekeepers,” such as receptionists and those at security posts, not to allow the terminated worker to return.

- If the worker has previously made lethal threats, security should be armed, wear protective clothing, and have detailed training in disarming, weapons retention, “takedown,” and restraining techniques.

- Consider soliciting help from local law enforcement during high-risk terminations and large-scale layoffs.

**Aftermath.** The security department or individuals with security responsibilities should be alerted prior to termination to help with threat assessment and to assist with the actual

---

**In Praise of a Strict Termination Protocol**

Experts in workplace violence prevention often warn that the differences between the goal of supervisors and that of security is often to blame for firings that trigger violent events.

When workers seemed troubled or aggressive and are making others feel uncomfortable, managers can be quick to want to remove them to get rid of the problem and get their department back to running smoothly. But from a security point of view a quick termination may seem unwise if it’s likely to trigger a violent response. Because their mission and priority are different, supervisors—perhaps subconsciously—may not make a point of communicating potential warning signs for violence. If raising such issues seems like it will slow down the process—sparking team meetings, threat reviews, and so on—supervisors may simply avoid bringing them up.

As a result, it may be helpful to require that all employee terminations, without exception, go through the same initial process of including notification to the security department. That way, a classification that an upcoming firing is not an “at-risk termination” will be a justified, fact-driven decision and not an effort to simply push the process through more quickly. Ensuring that the security department is notified in every case, not just in those deemed at-risk, gives the department an opportunity to keep watch for fired employees as they arrive to work to finish out their time at the company—and acknowledges that threat assessments are an inexact science.
III. CONTRIBUTING FACTORS/MITIGATION

termination. They also need to follow basic precautions of revoking access and retrieving property—e.g., control cards or keys, company credit cards, network access, computer and communications equipment, telephone services, sensitive company information, company books and materials, customers lists, and any other company property assigned to the individual. Additionally, Bonnie Michelman suggests that companies have an employee from HR check in with ex-employees a few weeks following termination to see how they are doing.

In addition to these basic measures, companies need to review less obvious issues. Specifically:

- **Duty to warn.** Depending on the jurisdiction, companies may need to warn employees if the employee being fired makes threats against them. A company’s legal team needs to review the situations and a determination needs to be made as to what information should be shared with employees.

- **Additional security precautions.** Companies should assess whether they need to take additional security precautions for threatened coworkers. The risk may warrant providing additional security services, such as a home security survey, changing their phone number, loaning them a cell phone, providing them with a quick response distress button, or providing them a security escort to their vehicle.

- **Be-on-the-lookout (BOLO) notices.** Analysis of workplace homicides indicate that a fired worker is as likely to return to the workplace and fire a gun at coworkers a day, a week, or a month after the dismissal. Because frustration can mount when a fired employee doesn’t find new work, workplaces need to remain on alert for a minimum of six months following the dismissal of a clearly disgruntled employee. This extended threat timeline requires security teams to be vigilant with respect to personnel changes. For example, upon termination a security team may issue a BOLO to the front desk receptionist, asking him or her to contact security immediately if the disgruntled ex-employee returns. But what if there is a change in front desk staff four months after a dangerous worker’s termination? In your workplace, would the new receptionist receive a briefing on individuals for whom he or she should be on the lookout?

**Downsizing/Restructuring**

In addition to addressing the threat from individual terminations, workplace violence prevention teams should work with management during corporate downsizing and restructuring to minimize the risk of violent incidents.

- **Be strategic in allocating resources and focusing attention.** When companies lay off many workers at once from many locations, corporate security executives must be particularly mindful to assess where to focus attention based on a location’s type of business operation, security measures in place, and past and current threats. Generally, security teams will have at least a couple of months to plan as companies make an effort to comply with the federal Worker Adjustment and Retraining Notification Act, which requires employers to provide 60 days’ notice of a mass layoff (or provide 60 days’ pay).
• **Advise management on improving the odds of a safe layoff process.** You’ll have to administer workplace protection regardless of how well or poorly management handles a layoff, but the senior team should at least hear from its violence prevention team on mitigating the threat of violence. Layoffs are safer when a plan is followed and employees are treated respectfully, including thoroughly explaining the reason for the layoff.

• **Consider providing more warning.** Companies may invite unnecessary risk by giving employees little or no warning before termination. While companies often have other reasons why they provide little or no notice, advanced notice reduces the threat that the layoffs will get out of hand. Additionally, when employees think the company provides sufficient notice, morale tends to be higher among the remaining workforce, which may encourage a corporate climate in which the seeds of violent incidents are less likely to be nurtured.

• **Get input from supervisors and managers on employees who may not handle the news well.** Most employees will resign themselves to the news, but a select few may react with aggression. So while great effort should be taken to preserve workers’ dignity during a layoff, problematic employees need to be watched more closely and their movements followed, such as making note of the make and model of the worker’s car so that security is on alert if he or she returns to the workplace. Although personnel records will indicate which employees have a track record of disturbing behavior, managers and supervisors can also suggest more generally the employees who may have trouble with the news, such as individuals who may be experiencing recent financial troubles, for example, or a spouse who was also downsized recently.

• **Advise key staff not to hold meetings with groups of laid-off workers.** Paul French, senior director at Threat Management & Protection Inc. (Huntington Beach, Calif.; www.threatprotect.com) warns that hostilities can arise if workers see it as a chance to negotiate and get frustrated at management’s lack of give.

### Consider Court Protection Against High-Threat Ex-Employees

Brian Allen worked at Scios Inc., a California biotech company, and abruptly resigned after getting “a message from God,” and warning two managers that three employees were going to die from using the company’s product in the near future. He also left 18 phone messages for a coworker who had turned him down for a date.

Under California’s Code of Civil Procedure Section 527.8, the company sought and was issued a two-year injunction against the worker on behalf of the managers and the recipient of the phone calls. Allen appealed the case, arguing that he was never proven insane and had not made any threats to specific individuals.

The California Court of Appeals, First Appellate District, affirmed the injunctive orders, ruling that the request made by the company did not have to be supported by evidence that the worker had made threats of violence to particular employees.

“The express intent of the author of the legislation was to address the growing phenomenon in California of workplace violence by providing employers with injunctive relief so as to prevent such acts of workplace violence,” the court said. There was, the court said, a “credible threat of violence,” and that was sufficient to warrant the issuance of the injunctions (Puthukkeril v. Allen, Cal. Ct. App., No. A114069, unpublished opinion; Oct. 25, 2007).
III. CONTRIBUTING FACTORS/MITIGATION

- **Ramp up security during the week after a firing with additional security on-site and changing access codes.** After a round of layoffs in 2009, a spokesperson for energy company Dynergy said they warned workers remaining after a layoff against lending former coworkers their access badges or inviting them back to the workplace.

- **Make sure that downsizing does not move at a pace beyond the security department’s ability to keep up with it.** Security, IT, and HR will need to remove passwords, block facility access, and take other measures to ensure that terminated employees do not have the ability to return to the facility and cause harm. If security personnel are included in the layoffs, consider staggering security and general employee cuts, as Starbucks did in 2009 when it cut 40 jobs in human resources and asset protection departments. In a statement, the company said, “These two specific areas have unique job responsibilities supporting internal client groups during a workforce reduction so we felt it was more respectful to inform these partners now, prior to the remaining organizational changes.”

- **If you’re planning security staff cuts, examine how “they seem.”** See if they create an appearance of affecting one group of security workers more than another. “[Conduct] reorganizations in a way that avoids discrimination claims, whether they are intentional or unintentional,” said Mark Wiletsky, a management attorney at Holland & Hart (Boulder, Colo.; www.hollandhart.com). “More often than not, when we deal with this, we see issues arise in terms of age discrimination.”

- **Plan for the pickup.** While any company may face the need to conduct a mass layoff, one place to avoid cuts is in the manpower infrastructure that the company needs to conduct adequate background checks on new hires. Most times when the economy dictates a substantial cut in personnel, it also requires a quick ramp-up when the situation improves. As the economy rebounds, “there will be a lot of hiring going on, and they’ll need to hire quickly,” said John Challenger, chief executive officer of Challenger, Gray & Christmas, an outplacement consulting organization (Chicago; www.challengergray.com).

**Aftermath.** Psychological problems that can lead to violence are somewhat common in the wake of downsizing, warns James Campbell Quick, Ph.D., co-author of *Preventive Stress Management in Organizations*. Downsizing contributes to:

1. **Declining morale.** When employees don’t feel appreciated, they are less likely to follow rules—even those in their best interest.

2. **Rising fear.** Even after a corporate downsizing project is complete, workers will fear losing their jobs.

3. **Declining accountability.** Management tends to be less available during reorganization activities. Additionally, downsizing in manager-level positions can create a supervisory vacuum.

4. **Sense of being overwhelmed.** Not all employees react positively to changes in their work structure or workload. Some workers resist change and will resent company management.
Downsizing and large-scale layoffs are not the only types of stressful change that can increase the risk of violence. Some research indicates that rapid expansion, as well as corporate restructuring, can cause workplace upheaval that can alter the risk of violence. In general, companies should approach any large-scale organizational change as a possible precursor to problems. The rationale is that the loss of predictability in the workplace induces stress and worry, which can foster aggression.

**Solutions.** Companies should consider the following approaches to reduce the negative impact of dramatic change, especially downsizing:

- Increase communication during times of upheaval. Open communication and responding to employee questions provide the best opportunity to combat the fears that can lead to anger and violent outbursts.

- Frequently assess worker attitudes toward safety accountability in transitional times.

- Limit unnecessary changes during downsizing and, where possible, implement changes over time.

- Ensure that the lines for reporting, tracking, and responding to incidents of workplace violence remain open. It is possible for changes in the personnel and organizational structures to disrupt procedures relative to the workplace violence prevention program.

- Conduct and evaluate staff interviews during and after downsizing to monitor an increase in stress, anger, and other precursors to violent incidents.

- Ask managers to evaluate the potential effects of downsizing on workplace violence, and ask management to signal to managers that this is a priority and that they must not use additional burdens as an excuse to disregard this important assignment.

- Make sure that remaining personnel are not being assigned additional duties to the point that they will be unable to effectively perform their role in the workplace violence prevention process.

- Maintain an accurate record of the number of hours that staff work in the wake of staff reductions to ensure that overtime is not being used to dangerous levels.

**Make Terminations the End of It**

There is also nothing to be gained—but much to lose—by allowing laid-off or fired workers back into the workplace for meetings with company managers, say experts.

**Case in point:** In November 2008, executives at SiPort Inc., a software company in Santa Clara, Calif., agreed to meet with a terminated engineer. During the meeting, the ex-employee shot and killed three company executives.

If terminated workers are allowed to return to the workplace, they should be subject to the same strict security requirements as any visitor.
III. CONTRIBUTING FACTORS/MITIGATION

• Review to make sure all employees have a clear understanding of their revised responsibilities relative to the workplace violence prevention function.

• Direct supervisors to be on high alert for employee behaviors that are characteristic of increased risk for potential aggression or violence.

• Implement fair HR strategies for those employees whose jobs will be eliminated, such as identifying severance packages and outplacement support. Treating exiting employees honorably will lessen the negative impact that layoffs have on remaining employees.

• Try to implement a period of organizational stability in the wake of downsizing. This will help ease the stress associated with layoffs.

• Address rumors rather than ignoring them.

B. Organizational Culture

Although it can be more difficult for the workplace violence team to address, an organization’s “culture” can foster workplace violence or make it more unlikely. In fact, violence prevention interventions may only be as good as the culture in which an organization implements them, agree many security professionals.

A corporate culture that promotes respect can ease the frustrations that lead to violent outbursts, while a conflict-driven management style can easily raise tensions, according to a report on workplace violence in the healthcare industry by the National Institute for Occupational Safety and Health. Companies that ignore employee frustrations may actually spark violence, particularly among workers for whom their job is everything, warn NIOSH researchers. In order for the specific elements of a workplace violence prevention program—policies, training, and the like—to attain maximum effectiveness, organizations need to work on the corporate culture to make sure it isn’t sabotaging the program’s efforts and to alter employee attitudes toward aggressive behavior.

A study by the Massachusetts Legislature—sparked by a shooting of seven employees at a Wakefield, Mass. technology firm—concluded that employers could better prevent violent incidents by promoting civility, respect, and humanizing the workplace. As a model,

FROM THE FIELD...

Without Considering Cultural and People Issues, Security Measures Provide Less Value

An organization must understand that when an employee exhibits unwanted security behavior, it’s often because of the organization’s own structural failing.

On reason companies ignore this fact? The effectiveness of security hardware. It can actually cause companies to forget how important it is to pay attention to organizational issues and human factors needed to support it.

That is crucial, notes new research on organizational behavior. “Without question, the use of well-designed physical-related security systems to prevent security threats is vital to ensuring security at work. Nevertheless, the expected positive effects could be drastically undercut if human-related systems are not taken into consideration” (“Security in Organizations: Expanding the Frontier of Industrial-Organizational Psychology,” International Review of Industrial and Organizational Psychology, vol. 24, 2009).
companies should consider following the same path they took to reduce sexual harassment in the workplace, according to Lynn Jenkins, senior scientist at NIOSH in an interview with IOMA. “[Companies need] to devise and promote a policy that tells workers it’s not okay to threaten and intimidate. It’s not okay to use violent images. It’s just not the way we do business,” Jenkins says.

Corporate programs that focus on promoting civility in the workplace and train management, supervisors, and workers to deal more civilly with one another can help a safer workplace to evolve, according to Larry Chavez, founder of Critical Incident Associates. Chavez told IOMA that he believes protecting workplaces hinges on such “soft” strategies, and said truly “healthy” organizations do the following:

1. Place a high value on human dignity and emphasize, by example, respect for all employees without regard to rank or position.

2. Have a management that sets the tone by establishing an atmosphere of dignity and civility in all human interactions.

3. Develop civility policies, complete with sanctions that make rules on civility enforceable.

Dr. James Madero agrees that the “tone” of a workplace makes a critical difference. “You can have toxic management styles, or have a blame orientation at the top, and that flows down and can lead to more violence,” he says. For example, a company may have a culture that permits a supervisor to dress down an employee in front of his or her coworkers. “You might get away with that with 100 workers, but the 101st might be like, ‘I am not going to take that.’ ”

**Solutions.** In addition to corporate civility policies that spell out an organization’s expectations for the treatment of coworkers, customers, and others, a company should consider other culture improvement activities to reduce the risk of violence.

1. **Learn about the culture.** In order to assess whether the corporate culture is supporting or inhibiting violence prevention initiatives, organizations should understand what their culture is. Perception surveys and employee exit interviews provide two opportunities to ask employees about cultural issues, such as coworker support, respect, and stress. Analysis of the results will indicate which areas of the organization and issues require intervention.

2. **Critically examine whether your company’s supervisors feel pressure to gloss over incidents.** Acts that undoubtedly would be reported if they occurred at home, at school, or on the street are not addressed at the workplace because of denial, company culture, and worries about corporate image, according to the Massachusetts Joint Committee on Public Safety. Supervisors need to get the message that the company wants to address small incidents, not sweep them under the rug.

3. **Provide updated manager training.** “Unfortunately, today’s managers were schooled in yesterday’s techniques and woefully lack the skills needed for today’s environment,” according to Frank Kenna III, president of the Marlin Co., a consultant firm specializing in
workplace communications. To take aim at tensions that lead to violence, companies need to write new policies, promote these policies to employees, and train workers, managers, and supervisors on how to interact in ways that promote respect and make violence less—not more—likely. “They [need the skills] to listen and respond to what their employees are feeling if they want to have any chance of defusing the stress time bomb,” says Kenna.

4. **Assess the message that you send to employees in corporate actions.** Company leaders who demonstrate to workers that they are running their companies honestly and ethically engender employee trust and minimize tensions. Even actions on a personal level play a role in shaping employee attitudes. For example, companies that demonstrate empathy in handling terminations—by offering job placement services, severance pay, and extension of medical coverage—provide remaining employees a greater sense of security and well-being, which can reduce stress and conflict.

5. **Remove stigmas.** Supervisors and managers can play a key role in dealing with behavioral issues in the workplace by providing workers with a “safe place” to report problems or concerns. However, NIOSH research and independent surveys have found that managers and coworkers often consider overly stressed, depressed, or anxious workers as weak, incompetent, or even lazy. Managers who are aware of behavioral health issues and respond appropriately can lessen the stigma and prevent negative outcomes that occasionally result from untreated mental health issues. Companies should try to reach the same goal on an organizational level by promoting and encouraging all employees to make use of assistance programs and support programs available to their workforce. Companies that discourage workers from seeking help only raise the risk of pressures building until employees explode in a violent act.

6. **Employ a robust employee assistance program (EAP).** Trying to save money by not offering professional assistance to employees in need of counseling or psychological support is a shortsighted mistake, according to former ASIS International President Bonnie Michelman. Companies should give employees an outlet for seeking help to prevent issues of stress or personal difficulties from escalating into threats or acts of violence in the workplace.

7. **Improve worker trust.** Recent occupational health research has found that when workers trust management they experience fewer symptoms from job strain, including less burnout and psychological strain—both frequent precursors in workplace violence incidents (“Trust in Management as a Buffer of the Relationships Between Overload and Strain,” *Journal of

---

**Workers Behave Like Their Peers (Not Necessarily the Way a Policy Says They Should)**

Research proves that the norms and beliefs that surround a worker (in the form of coworkers) exert a social influence. “These social influences can then [have an impact on] an individual’s perceptions, as well as behaviors, related to security.”

In an effort to address this security climate issue, workplace violence prevention teams should ask: 1) What are the group norms? 2) Where (and whom) do they come from? 3) Can they be positively influenced? How?
Occupational Health Psychology, 2003). The study identified effective ways for companies to promote trust:

- Keep promises to workers.
- Communicate the organization’s vision and values to staff.
- Seek out and respect worker input.
- Work toward shared goals.
- Develop mechanisms to increase the personal interaction between management and workers.

8. **Confront all forms of incivility.** “Though many people consider gossip an amusing pastime, in reality it is a disruptive and damaging phenomenon,” warns Kenna. “Most people engage in it, but they don’t realize its consequences. Add to this backstabbing, cliques, and rudeness, and we see a huge opportunity for companies to reduce stress and interpersonal friction by addressing these issues.”

9. **Confront management lip service.** Management may promote their commitment to zero tolerance and civility, but unless they actually mean it, a culture in support of the workplace violence prevention program will not flourish. If a star employee’s tantrums are allowed to persist unabated, for example, workers will think management is insincere about its effort to crack down on workplace violence, which can stifle the reporting of incidents. Words and symbols matter when trying to drive the message of workplace violence prevention into the organization, but attitude and actions matter more.

10. **Cultivate workplace violence prevention at all levels.** As opposed to top-down or bottom-up workplace violence prevention interventions, an organization-wide workplace violence strategy will apply to all organizational levels at all times. This is the quickest way to disseminate the mission throughout the whole organization.

11. **Assess progress carefully.** In their eagerness to meet corporate goals, companies will often believe their own hype about the extent to which workplace prevention is ingrained into the organization. Often, real levels of civility, respect, and support are much different from the rhetoric. The workplace violence prevention team needs to continually test its assumptions regarding the extent to which respect and courtesy is the workplace norm. When trying to achieve a “soft” goal, such as a “more respectful corporate culture,” it can be easy for companies to claim success too early.

12. **Eliminate conditions that promote aggression.** Workplace violence rules should be accompanied by company efforts to minimize workplace conditions that make acts of violence more likely to occur.

- Presence of chronic labor-management disputes, numerous grievances, a high number of workers’ compensation claims, or layoffs and downsizing.
- Presence of rumors regarding layoffs, downsizing, or company financial instability.
• Significant changes in workload or technology not accompanied by sufficient training.

• Lack of formal channels to respond to employee grievances, or the unresponsiveness of these channels.

• The feeling of unjust treatment or perceptions of unfairness in the workplace—in pay, promotion, or punishment, for example—likely contributes to conflict and negative security behaviors.

• Large amounts of overtime. “Whenever you have a problem with overtime, you have an environment that is highly charged and likely to lead to inappropriate behavior by supervisors or employees or both,” says Thomas Germano, former director of the Long Island District of Cornell University’s School of Industrial and Labor Relations. If a company chronically uses overtime, it may reflect understaffing or improper staffing indicative of an authoritarian management style, Germano adds. Employers that demand large amounts of overtime should consider less stressful ways of dealing with the workload, he says.

C. Stress

Because workplace stress can contribute to acts of workplace violence, stress reduction strategies should be part of an organization’s violence prevention activities. Workplace studies have demonstrated a convincing correlation between the amount of stress workers feel and their anger levels. Stressed workers are nearly three times more likely to have urges to strike or verbally assault coworkers, research shows.

Despite the fact that the mass layoffs that accompanied the recent recession are over, workers are not feeling much better at work, according to a survey by the Marlin Company in March 2010. Thirty-eight percent of 705 workers surveyed said they have seen an increase in stress or anxiety in the last six months (see Figure 34).

“Stress in the workplace can be a silent killer undermining businesses,” says Frank Kenna III, president of the Marlin Co. “Companies believe everything is fine until a stressed, out-of-control worker runs rampant. Rather than wait until a deadly outbreak takes place, companies need to help workers manage stress.”

A chief obstacle facing workplace violence prevention teams is the attitude of executives, who may believe a certain amount of
stress benefits the company. Senior leaders want workers to feel a sense of urgency and typically want staff to feel pressure to do their work quickly and effectively.

To achieve executive buy-in, workplace violence team members should coordinate with other stakeholders, such as company health professionals, to alert execs of the price companies pay for having a stressed-out workforce. James Campbell Quick, Ph.D., an expert on organizational culture, says that stress can manifest itself behaviorally, in the form of workplace violence or accidents, or physically, in the form of heart attacks, hypertension, or psychogenic problems. It also costs companies by contributing to the following:

- Absenteeism.
- Tardiness.
- Low morale.
- Job complaints.
- Turnover.
- Injuries.

**Causes.** On the basis of its research, the National Institute for Occupational Safety & Health favors the view that working conditions—as opposed to personal characteristics—play the primary role in causing job stress. Job conditions that may lead to stress:

- **Design of tasks.** Heavy workload, infrequent rest breaks, long work hours and shift work; hectic and routine tasks that have little inherent meaning, do not utilize workers’ skills, and provide little sense of control.

- **Management style.** Lack of participation by workers in decision-making, poor communication in the organization, lack of family-friendly policies.

- **Interpersonal relationships.** Poor social environment and lack of support or help from coworkers and supervisors.

- **Work roles.** Conflicting or uncertain job expectations, too much responsibility, too many hats to wear.

- **Career concerns.** Job insecurity and lack of opportunity for growth, advancement, or promotion; rapid changes for which workers are unprepared.

- **Environmental conditions.** Unpleasant or dangerous physical conditions such as crowding, noise, air pollution, or ergonomic problems.

**Solutions.** Unlike research into the causes and effects of workplace stress, evaluation data on stress management programs are relatively rare. Nonetheless, there is a body of evidence to suggest that companies can address stress as successfully as other health and safety issues if they deal with the issue logically and systematically.
III. CONTRIBUTING FACTORS/MITIGATION

Companies should start by conducting a stress risk assessment. Familiarize staff with the symptoms of workplace stress, followed by work analysis interviews, group discussions, and surveys of employees to measure their perception of job conditions, stress, health, and job satisfaction. Also, collect and analyze objective data relative to stress conditions. Finally, consider in a risk assessment the company’s existing management controls and employee support systems that help mitigate stress.

Once a company assesses the level of stress in its workplace and analyzes the data for clues as to where workplace stress (which department, which shift, and so on) may be running highest, it can intervene appropriately. Sample stress reduction activities:

- Provide stress management training to employees. In addition to reducing the risk of workplace violence and the intentional infliction of injury, workers who have stress management training available to them also report higher levels of job satisfaction.
- Improve indoor air quality.
- Educate employees about the importance of work/life balance.
- Improve work environment ergonomics.
- Increase recognition of employees for good work.
- Provide additional opportunities for career development.
- Promote an organizational culture that values the individual worker.
- Ensure consistency between management actions and organizational values.
- Ensure that the workload is in line with workers’ capabilities and resources.
- Design jobs to provide more meaning, stimulation, and opportunities for workers to use their skills.

Alternative Benefits Cut Stress, Study Claims

Complementary alternative benefits—beyond those workers traditionally receive—may help companies relieve workers’ stress, reduce health care costs, and possibly reduce the risk of violence, according to a study by researchers at the University of Michigan’s Ross School of Business.

The researchers found less turnover and lower health care costs among companies that offer generous alternative benefits, which can include flexible work hours; telecommuting; subsidized health club memberships or on-site fitness centers; paid leave time and special services for new parent employees; laundry and dry-cleaning services, valet parking, and grocery delivery; and discounted tickets to movies, museums, sporting events, and other activities.

Although they didn’t study a direct link, researchers said they believe the same stress-reduction perks that improved workers’ productivity and reduced absenteeism may also reduce conflict. “It would seem that a healthy, less-stressed, and collegial work force would be less prone to resolve conflicts by violence,” according to professor Cindy Schipani, one of the lead researchers. Certainly, since stress is a principle cause of workplace bullying, anything that an organization does to reduce stress is also a workplace violence prevention measure.
• Clearly define workers’ roles and responsibilities.
• Give workers opportunities to participate in decisions and actions affecting their jobs.
• Improve communications and reduce uncertainty about career development and future employment prospects.
• Provide additional opportunities for social interaction among workers.
• Establish work schedules that are more compatible with demands and responsibilities outside the job.
• When introducing a new task, make sure workers are clear on how to do it before leaving them to it.

Finally, violence prevention teams should keep an eye on the level of workplace stress by conducting periodic employee surveys to monitor environmental workplace stressors such as temperature, lighting, ventilation, and so on. While regular workplace walk-throughs can identify burned out lightbulbs and an audit may tell you if noise exceeds acceptable levels, only an employee survey will inform an organization what workers think about lighting, noise, and other environmental elements. You may find that saving money by turning down the lights at night is costing you in the long run by increasing workers’ stress or that paying for noise reduction equipment will save you money in the long run by reducing stress.

D. Substance Abuse

There is considerable debate about whether concentrating on substance abuse is a very fruitful way to lower the risk of workplace violence.

In testimony before the Massachusetts Legislature’s Joint Committee on Public Safety, Ken Duckworth, deputy commissioner of the Massachusetts Department of Mental Health, said that substance abuse is “without a doubt the number-one risk factor” in employees likely to commit a violent act.

But at the same workplace violence hearing, other experts scoffed at that assertion. James Alan Fox, a professor of criminal justice at Northeastern University, said that substance abuse is “absolutely not a predictor of violence,” and that very few perpetrators of violent workplace acts have substance abuse problems. He and others rejected the contention that steering a drug user toward an EAP might avert a violent incident. Such an attempt is more likely to trigger a violent response, Fox said.
There is little scientific evidence to bolster the bold claims by advocates of either viewpoint, and the truth probably lies somewhere in the middle.

**Drug testing.** Companies with an employee drug testing program probably receive a measure of violence prevention benefit from its existence, but the benefit may be too small to warrant its initiation at organizations that do not otherwise perceive the need for one.

Benchmarks on corporate drug testing programs collected by IOMA in October 2009 show that most organizations conduct pre-hire and for-cause drug testing of employees, but most do not conduct routine or random testing of existing workers (see Figures 35-38).

James Madero, Ph.D., president of Violence Prevention International, thinks drug testing can somewhat lessen the risk of worker-on-worker violence. Companies stand to benefit even if they only conduct drug screening at the pre-employment level, because some potentially violent individuals will take themselves out of the process, Madero says.

However, opponents to company drug testing programs suggest that drug tests, which can lead to employee suspensions and terminations unrelated to work performance, can actually increase the risk that an employee will commit an act of violence. While there are no specific data to support this assertion, it appears plausible when one considers that a change in worker employment status is frequently at the root of violent acts. It is certainly conceivable that an excellent worker who is nonetheless terminated for off-the-job behavior may develop the type of resentment that is often at

---

**Figure 36. Routine Scheduled Substance Testing of Existing Employees, 2010**

(Source: IOMA/SDR Survey on Corporate Security Management, Policy & Practices)

**Figure 37. Random Substance Testing of Existing Employees, 2010**

(Source: IOMA/SDR Survey on Corporate Security Management, Policy & Practices)

**Figure 38. Organizations with a Policy of “For Cause” Substance Testing* by Size, 2010**

*Company will conduct testing “for cause”; e.g., after a workplace accident, for behavior, etc.

(Source: IOMA/SDR Survey on Corporate Security Management, Policy & Practices)
the source of violent acts aimed at “getting back” at the company.

To minimize the risk that drug testing could lead to a violent episode, companies should undertake efforts to ensure that employees perceive that the program is being fairly administered. Poorly run drug-testing programs can undermine the morale and loyalty of staff, which can do more to contribute to the risk of workplace violence than reduce it.

Finally, there is the issue of cost-effectiveness. If a company’s goal is to reduce workplace violence, there are better ways to spend resources than on drug testing, such as an employee training.

**Drug use.** Workplace drug use, as measured by the percentage of positive drug tests, was on a sharp upswing in the early part of the decade. The latest data, however, show that it is again on the decline.

Data from millions of workplace drug tests performed by Quest Diagnostics show that the rate of positive tests for cocaine and methamphetamine declined sharply from 2005 to the first half of 2009. Because methamphetamine use causes irritability, combativeness, and nervousness and can be a contributor to violent workplace incidents, the trend is particularly encouraging.

The rate of positive tests for any substance has also declined, from 4.1 percent in 2005 to 3.5 percent in the first half of 2009.

**Substance use and customer/client violence.** While the link between employee drug use and violent acts is hard to gauge, drug and alcohol use clearly contributes to violent acts inflicted upon employees—from inebriated bar patrons assaulting waitresses to drug-addled emergency room patients assaulting nurses to gun-toting robbers in need of a fix demanding money from store clerks. Drug and alcohol use is a factor in one of four acts of workplace violence, according to the U.S. National Institute on Drug Abuse (www.nida.nih.gov).

Because violent assaults from external sources frequently involve substance use, organizations need to identify drug and alcohol use as a warning sign of violence. During training, employees should receive instruction on how to manage inebriated individuals so as to minimize the potential for violence.

**E. Online Communication**

Online communication provides another avenue for worker-on-worker harassment, as well as for outsiders to reach staff with inappropriate, harassing, or threatening messages. Such harassment has been labeled “cyberstalking,” refers to the use of the Internet, e-mail, or other electronic communications to stalk another person, and involves ongoing harassing or threatening behavior.

The very benefits of new technology—that it is low cost, easy to use, and anonymous in nature—make it an attractive medium for stalkers. Not surprisingly, the majority of cyberstalkers are men and the majority of victims are women, and in many cases the cyberstalker and the victim have a prior relationship, with cyberstalking beginning when the victim
III. CONTRIBUTING FACTORS/MITIGATION

attempts to break off a relationship. Cyberstalking of strangers, however, is not uncommon, and is facilitated by the enormous amount of personal information available through the Internet.

Although cyberstalking may seem more benign than a stalker in the bushes watching a victim’s house, a report by the Attorney General says it may not be. Stalkers can take advantage of the ease of communications and increased access to personal information to harass a victim more frequently and in myriad ways. And, as with physical stalking, “online harassment and threats can lead to more serious behavior, including physical violence,” a study found (“Cyberstalking: A New Challenge for Law Enforcement & Industry—A Report from the Attorney General to the Vice President,” Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice).

In some ways, cyberstalking can be more insidious:

- “Offline” stalking typically requires the perpetrator and the victim to be in the same geographic area. Cyberstalkers may be located across the street, across the country, or in the next cubicle.

- Electronic communications technologies make it easier for cyberstalkers to encourage third parties to harass and/or threaten a victim.

- Cyberstalking is so easy that individuals who would never stalk a victim otherwise may be inclined to do it.

**Prevention and assistance.** Cyberstalking is dangerous both economically, because employee victims are substantially less productive, and physically, because ignored virtual

**Figure 39. Perpetrators of Cyberstalking by Relationship to Victim, 2004**

(Source: Journal of Society and Information)

![Figure 39. Perpetrators of Cyberstalking by Relationship to Victim, 2004](Source: Journal of Society and Information)

E-mails and Online Chatting Ends in Workplace Shooting

Online communication greatly expands the ability of individuals to form “relationships,” thereby increasing the odds that a relationship that has gone sour could erupt into violence at work. A shooting in April 2008 at a temporary-staffing agency in Louisburg, N.C., is, unfortunately, a perfect example.

Amy Calamaco, a 22-year-old worker at the firm, met and chatted online with a man from Little Rock, Ark., and although they had never met in person, the man—after she rejected his advances—traveled to North Carolina and went to Calamaco’s workplace armed with a machete and a .40 caliber handgun. He shot and killed Calamaco, shot and wounded a coworker, and then killed himself, according to police.

“In this case, this gentlemen tracked her to her business,” the police chief told a local television station (WTVD). “Once you send an e-mail or whatever, your IP address is out there and can be tracked back to the original e-mail address.”
threats can turn into actual acts of workplace violence. In response to this growing and costly problem, organizations should consider amending their workplace violence awareness programs to include information about—and prevention tips on—cyberstalking.

It may be even more critical for employers to provide assistance in this form of stalking because the law has still not caught up to the threat, and employee frustration with legal remedies can leave victims feeling helpless, which further impairs their ability to work productively. Finally, the frequent inability to identify the source of harassment or threats can be particularly ominous to an employee who is the victim of cyberstalking. Prevention efforts should entail the following:

- Recognize that cyberstalking is a serious problem—not only as a potential precursor to face-to-face threats or violence—but also as a serious invasion of employees’ lives.
- Include definitions of cyberstalking in workplace violence policy statements, and educate employees on the definition and characteristics of cyberstalking as part of the violence prevention and awareness program.
- If your company contracts with outside trainers for workplace violence prevention training, assess whether cyberstalking is included in their curriculum and ensure that trainers have an understanding of the problem.
- During employee training, include tips on how to minimize the risk of becoming a victim of cyberstalking, including: (1) Do not share personal information in public spaces anywhere online or give it to strangers, including in e-mail or chat rooms. (2) Do not use your real name or nickname as your screen name or user ID. (3) Pick a name that is gender- and age-neutral. And do not post personal information as part of any user profiles. (4) Be extremely cautious about meeting online acquaintances in person. (5) Anytime an online situation becomes hostile, log off immediately.
- Encourage recipients of threatening electronic communications to immediately contact a designated company employee (supervisor, HR, EAP, violence prevention committee member, and so forth). Be sure to share the information with the company security representative to assess whether additional security measures need to be taken to protect the victim. It is advisable to use the same reporting chain for incidents of cyberstalking as for all other forms of harassment at work. This sends the message—to both victims and perpetrators—that the organization regards virtual harassment as seriously as it does other forms of workplace violence.
- Use filtering and e-mail blocking software to prevent harassing messages from reaching employees at work.
- Provide employees with general training about the Internet. In general, the greater a person’s knowledge of Internet communications technology, the less distress they feel as a result of online harassment, studies show. Conversely, workers who are unclear about online technology report significantly higher levels of fear from e-mail harassment.
- If the victim believes the cyberstalker may be a coworker, undertake an investigation. The techniques are similar to those used in investigating other types of computer crime.
III. CONTRIBUTING FACTORS/MITIGATION

Cyberstalkers leave an “electronic trail” that you can follow back to the source.

- Alert workers that most Internet Service Providers have an address to which complaints of abusive or harassing electronic mail can be sent (this address is usually “abuse@[the ISP’s domain].”

- Instruct e-mail users how to use tools that block e-mail from individuals who are attempting to harass or annoy them.

- Instruct victims of cyberstalking to make unaltered copies of all e-mails sent by the stalker and retain them as evidence, and to let the stalker know that she or he does not want to have any further contact.

- Help employee victims protect themselves by changing passwords often, keeping passwords secret, using passwords that do not use identifying information that the stalker could guess, installing a program that requires a password to log on to the computer, and clearing out online history information.

- Provide referrals to available resources that are specifically designed to assist victims of cyberstalking and stalking. CyberAngels is a nonprofit group assisting victims of online harassment (www.cyberangels.org). The National Center for Victims of Crime provides referrals and advocacy services (www.ncvc.org).

F. Solitary Workers

On the list of occupations with the most workplace homicide, one commonality stands out. Employees are at greatest risk when they work outside of a controlled security environment or don’t have security personnel or others watching over them.

More workers than ever are facing the heightened risk of solitary work as a result of new technology and field communication devices that allow employees to work outside of the controlled work environment. Companies must be mindful, however, not to allow the opportunity from work mobility to blind them to its risks.

Solutions. A violence prevention team should examine its company’s handling of employees who work alone and implement appropriate solutions for enhancing their safety.

1. Identify employees who work alone. Thinking of “solitary” workers probably brings to mind a taxi driver, logger, or convenience store clerk. But workplace violence prevention teams should apply the “working alone” framework to any employee who is out of view or earshot of another person and who cannot expect a visit from anyone for an extended period of time. Under this definition, a solitary worker might include a receptionist in a large office building, a traveling sales employee, or an office worker who burns the midnight oil.

2. Assess and address the risk faced by each worker who works alone. Companies should prevent employees from working in isolation whenever possible—especially for jobs with a recognized risk—but that isn’t always practical. Whether or not an employee
working alone faces a high or low risk depends on the type of work, their interaction with the public, and the potential consequences of a security event. There are broad categories of workers who work alone, and there is unique set of violence prevention strategies for each. Specifically:

- **Workers who handle cash and valuables**, such as convenience store clerks, retail food outlet workers, and taxi drivers. These workers are primarily at risk from robberies and assault. Controls include: reducing cash handling, good store visibility, robbery awareness training, and security systems.

- **Workers who travel away from the base office to meet clients**, such as sales staff, home care workers, and social services workers. These workers may face unpredictable client behavior, assault, robbery, and verbal abuse. Controls include: providing workers with a standard security awareness checklist so they can evaluate their own risk before entering a situation, including client behavior, location security, previous experiences, and the presence of other dangerous items (e.g., weapons). Companies should also arrange for a "safe visit plan" in the event a worker feels he or she is entering a potentially unsafe situation. This plan should outline the options they have for making the visit safer, such as the use of an active communication system, switching the meeting place to a safer location, or asking supervisors to assign a coworker to accompany them.

- **Workers who are at risk of violent attack because their workplace is isolated from public view**, such as security guards and custodians. These workers primarily face the risk of violent attacks by intruders. Controls include: site security, safe work procedures, and training. Safe work procedures should direct workers to check the security of the workplace at the beginning and at the end of the shift, and training should include how to behave when confronted with an intruder.

**Solitary Workers At Risk Don’t End with Taxi Drivers**

When thinking of high-risk occupations, one rightly thinks of security guards, police officers, convenience store clerks, and taxi drivers. But workers of all sorts face workplace assaults—or worse. Just a casual search of a single month (June 2010) yielded some horrific examples:

- A teenager working at a community pool in Overland Park, Kan., was sexually assaulted in a pool house;
- A youth counselor at a group home for troubled teens in Lockport, N.Y., was bludgeoned to death during a robbery; and
- A man kidnapped a Cumberland Farms Food Store employee in Shelton, N.H., throwing her in the trunk of his car and repeatedly beating her while high on “angel dust.”

Different jobs and locations, but they had the common risk factor of working alone.

Lone workers—employees who perform activities isolated from other workers and without close or direct supervision—require special security considerations. Organizations need to ask basic questions to assess the risk: What is a reasonable length of time for the person to be alone? Can one person adequately control the risks of the job? Is the person medically fit and suitable to work alone (e.g., age, medical condition)?

Based on a hazard assessment of the risks faced by employees who work alone, organizations should establish procedures and institute security measures to mitigate their risk.
3. **Establish a check-in procedure.** A “check-in” plan helps ensure that your company is making necessary contacts with all employees and should establish ways to account for people—either visually or verbally—while they are working. Considerations:

   - Make sure your plan is appropriate for both regular business hours as well as after main office hours.
   - Decide if a verbal check-in is adequate, or if a coworker or supervisor needs to conduct a visual check.
   - When a solitary worker is traveling away from the office, a main contact person should know his or her destination, estimated time of arrival, return time or date, contact information if staying overnight, mode of travel (public transit, car, plane, and so forth), and alternate plan in the event of bad weather, traffic problems, or other contingencies.

Here is a sample check-in procedure:

   - Prepare a daily work plan so the company knows where the lone employee will be and when.
   - Identify one main person to be the worker’s contact at the office, plus a backup.
   - Define under what circumstances the solitary employee will check in and how often.
   - Stick to the check-in or call-in schedule.
   - Develop a plan in the event that the solitary employee does not check in by the necessary time.

4. **Identify additional opportunities to reduce the risk to employees who work alone.** Ideas:

   - Talk to employees who work alone about their work. Get their input about the work they do; if, when, and why they feel unsafe; and possible solutions to their security concerns.
   - In your security incident database, include a data field that captures whether the worker was alone at the time of the security incident. Security directors can then run reports to see whether working alone is contributing to security incidents and collect evidence for the need to change staffing levels or other changes in company policy.
   - Make sure supervisors make regular contact with remote or solitary workers. For supervisors who oversee solitary workers, this may also be a good performance measure.
   - Within a facility, position a telephone as close as possible to workers who work alone. For workers away from the office, provide a cell phone. If traveling to an area that will be out of cell phone range, have alternative methods of communication available (such as use of public telephones, site visits, or satellite technology).
• Position workers, where possible, in locations of highest visibility.

• Where appropriate, use a security system such as video surveillance cameras, mirrors, observation windows, and so on, to make visible workers who would ordinarily be out of view. Advances in remotely monitoring cameras over the Internet have made this easier to do than ever before.

• Encourage employees to request assistance from police, security services, or supervisors any time they feel unsafe.

• Where appropriate, provide employees with a GPS device that allows supervisors to track their location online.

• Provide additional security to employees who work late. An employee who is the only one on the floor after hours is in a particularly vulnerable situation, especially in buildings that still allow public access late at night, such as hospitals. Helpful security measures may include panic alarms in isolated building areas; instituting a security policy requiring after-hours staff to notify a security representative that they are still in the building and to inform security when they leave; and keying-off elevators to restrict access to certain floors after hours.

Selecting lone worker safety devices and services. Because of the risk and the growing number of workers performing solitary work, the market is particularly robust for personal protection devices and response services. Increasingly, vendors have been offering automatic warning devices that operate if specific signals are not received periodically from the lone worker who is assigned to use them (for example, systems that utilize GPS tracking to follow the whereabouts of security staff) and other devices that lone workers can use to signal trouble or which automatically alarm by the absence of activity.

It may be affordable and effective to rely on a lone worker safety device and monitoring service, but outsourcing this aspect of protection demands careful consideration. In Britain, where protection of lone workers is a specific safety requirement, they have recently developed a new British Standard code of practice (BS 8484:2009) for the provision of lone worker device services. Though it doesn’t carry any regulatory weight in the United States, the safety standard is helpful by defining best practices surrounding security for lone workers when relying on technology devices for their protection.

Suppliers of a device and monitoring. They should be able to demonstrate:

• financial stability and at least two years of accounts;

• proof of necessary insurance; and

• the ability to protect the data it receives.

The device. The lone worker (LW) safety device should:

• be suitable for the LW environment;
III. CONTRIBUTING FACTORS/MITIGATION

- be on the correct communications network for the area in which the solitary employee works;
- have the required functions as defined by a risk assessment;
- have enough battery capacity for the duration of the job task;
- have any special functions as required by the lone work task (e.g., a “man down” function);
- have the ability, in conjunction with the alarm receiving center, to provide the LW’s location; and
- be provided to the LW with full training prior to use.

**The monitoring/response center.** The British standard also suggests that you should verify that the alarm-receiving center can answer “yes” to the following questions:

- Do they meet police requirements for police response?
- Do they have the ability to pinpoint your LW’s location in the event of an activation of the device?
- Can they listen in when the device activates and talk to the LW either directly using the device or by other means, such as a cell phone?
- Do they manage false alerts from the LW device?
- Do they verify where an emergency response is required and manage the incident?

Finally, the new British Standard and the British Security Institute suggest that clarity—among all parties—is critical to ensure the effective response to alarms from an LW device.

- Define the response you require for your LW in your response agreement.
- Consider, where possible, a stepped response, with managers or supervisors being the first option and the emergency services being the last option.
- Understand the response requirements of the emergency services.
- Inform and train LWs in the type of response they will receive.

**G. Open Environments**

After suffering a senseless act of violence, most companies will focus on hardening their security shell, asking, What can we do to prevent violence from ever again leaking in? For those working in a corporate, educational, or some other campus environment, this is not a complete strategy. You may be able to control different parts of an open environment, but you have no real option for completely keeping out an individual bent on violence.
Addressing a recent Governor’s Campus Preparedness Conference in Virginia, George Mason University’s Chief of Police dared to utter the usually unspoken truth—that a campus lockdown isn’t just impractical, it’s impossible. “I know I can’t lock down George Mason,” he said. The comment highlights the unique challenge of managing workplace violence in an open environment.

**Risk.** A college campus is a quintessential example of this security challenge. A gymnasium or lab can have an access control requirement, but anyone can walk onto the grounds. When a campus has both an educational and a residential environment, the risks multiply. Although clearly unique, the experience of colleges is useful for other open environments to consider, and federal-reporting requirements ensure data is available on it. Under the Clery Act, colleges and universities that participate in the federal financial aid programs must maintain and report information about crimes on and around campuses.

Examining that data reflects just how difficult is the challenge facing campus safety officials. Not only is it impossible to fence out violent intruders, but statistics on attacks show they happen all over the campus (see Figure 40). Even when assaults occur inside buildings, they defy the easy targeting of security countermeasures. Data show that violent attacks occur in similar numbers in offices (14 percent); instructional areas (13 percent); common areas (9 percent); and hallways, stairwells, and restrooms (9 percent). (“Campus Attacks: Targeted Violence Affecting Institutions Of Higher Education,” United States Secret Service, United States Department of Education, FBI; April 2010.)

**Not So Random**

Mass killings like the bloodbath at Virginia Tech in 2007 give the false impression that random violence is the principal threat. Although that tragedy has become the event most associated with violence on college campuses, the event itself—in which Seung-Hui Cho went building to building on a random killing spree—is atypical. In fact, only 3 percent of on-/non-campus attackers move between buildings or locations, according to the data. Of the vast majority of attacks that occurred within a single building, only 4 percent moved to different locales within it (e.g., from a classroom to an office or hallway).

“Though much attention has been given to the phenomenon of the ‘traveling’ attacker, in context, it actually is a rare event. This finding may have tactical and strategic ramifications for first responders and emergency management professionals,” according to an FBI report. (“Campus Attacks: Targeted Violence Affecting Institutions Of Higher Education,” United States Secret Service, United States Department of Education, FBI; April 2010.)

Rather than random, mass shooting sprees, the vast majority of violent assaults are singular events in which perpetrators target one or more specific individuals. So, more than the Virginia Tech incident, these other highly publicized incidents in 2010 seem more illustrative of the primary threat:

- The killing at the University of Virginia in which a member of the men’s lacrosse team allegedly beat to death a member of the women’s team with whom he was romantically entangled;
- The murder at Ohio State University of two maintenance supervisors by a janitor after he was told he would be terminated; and
- The shooting by a University of Alabama biology professor who had been denied tenure of six colleagues (three fatally) during a faculty meeting.
Clearly, to eradicate violence from a campus environment, security personnel would need to be everywhere all the time. Since that is impossible—and locking down and fencing off is not an option—where do you look for answers?

Solutions. It’s important for violence prevention team members in these environments to review all of the security recommendations in this report, but because these environment pose a unique security challenge, it’s important to consider and focus on some specific prevention and mitigation measures.

1. Open communication lines. Most violent attackers on a campus environment target specific individuals. This provides security a chance to prevail—if communication lanes are open to capture and share information about triggering events. Most incidents have a specific target and target selections are usually closely related to triggering events (e.g., a romantic breakup, an academic or workplace failure, or a dispute). Most assaults are also limited to the person or persons whom the subject may have blamed for causing the event, according to the FBI.

Concerning behaviors are also frequently observed by friends, family, associates, professors, or coworkers, such as paranoid ideas, delusional statements, changes in personality or performance, disciplinary problems, depressed mood, suicidal ideation, nonspecific threats of violence, increased isolation, “odd” or “bizarre” behavior, and interest in or acquisition of weapons.

These common factors of attacks on campus environments—triggering events, targeted individuals, concerning behavior—demonstrate the need to have a flexible and comprehensive response to the risk of violence and for providing an avenue for communication between those who devise protection strategies and those who may become aware of unreported threats or other warning indicators, such as supervisors, human resources, and employee representatives. For schools these factors indicate the need to improve information sharing between administrators, campus security, faculty, and others.

2. Think broadly about who poses a threat. Reflecting on the data it collected about campus crime, the FBI concluded, “From a threat assessment perspective, the fact that 30 percent of perpetrators were either unaffiliated or indirectly affiliated with the institution of higher learning through students or employees challenges campus and law enforcement personnel to design a threat assessment capability that can also identify and assess threats that go beyond their student and employee populations.” For schools, establishing
connections to community resources ahead of time may enhance campus safety professionals’ ability to prevent a threat from materializing that originated from an indirectly affiliated subject, according to the report. Corporations must treat the issue in a similarly comprehensive manner and incorporate the risk from domestic situations when addressing the risk of violence in the workplace.

3. Maximize your control. Within open environments, there is typically an opportunity for an organization to tighten whatever control it does possess to better mitigate an incident. Some examples:

- By its nature, a college or corporate campus is mostly open, but an organization can restrict access to parts of it by adding or enhancing access control systems or, at a minimum, reducing the number of building entrances (while maintaining a sufficient number of emergency exits).

- If appropriately trained, staff and unarmed security officers may be able to prevent an incident involving an armed visitor or patron from turning deadly by calming the conflict with effective early-incident intervention.

- Representatives from the University of Richmond said they installed locks and peepholes on all classroom doors to permit secure sheltering during a campus emergency. (Peepholes let individuals inside confirm who is knocking at the door; e.g., police, not the shooter.) Some states now recommend that schools equip classrooms with panic buttons. Even if a security department has armed officers, geography makes it unlikely that they’ll be able to contain a shooting in a large open environment once it starts. So part of planning active-shooter response must include an audit of building security and upstream training opportunities that will assist emergency response.

4. Coordinate with police. An active-shooter response plan should include steps for establishing a command center to manage the crisis and awareness training for employees on what to do when a shooter is on company property. A company can also share the plan with law enforcement to improve coordination, and provide active-shooter response maps so police will know where to go to assume control of the situation. Additionally, law enforcement may have resources or programs that can help organizations plan, prepare, and train staff.

5. Coordinate with management. The perception of the safety of schools has been harmed by mass shooting events, but the fact that college public relations departments, administration officials, and security representatives have often seemed on different pages about their degree of vulnerability to shooting events hasn’t helped, either. An institution or organization is better served by close coordination between management and security so it can present consistency in its messages about safety and preparedness.

Security executives should coordinate with management and administrators on the best way to communicate with staff and the media on the issue of active-shooter response. Security professionals should refrain from describing shooting events in open environments as “impossible to prevent” because it ignores the legitimate desire of administrators to make
invitees feel safe. But, at the same time, senior officials must realize that ignoring risks and failing to speak frankly about the limitations of security can complicate crisis response.

Security officials need to present a strong case for why legitimate threats should not be downplayed. One persuasive argument is that general staff members have a critical role in preventing an active-shooter event from resulting in mass casualties. In any large environment serviced by a small security force, a workable response plan needs to include training for managers, supervisors, or faculty on a shelter-in-place response to an active-shooter alert.

Security and management should also periodically negotiate over what is the appropriate mix between visible and invisible security given the current threat level, level of fear, and the public image an institution or facility wants to present.

6. **Choose your words carefully.** A majority of all college campuses have “lockdown” plans on the books, and more than 60 percent of public universities have them, according to the *Reader’s Digest (RD) College Safety Survey*. But there is a growing sense among many experts that the “lockdown” language does more to serve public relations than it does to describe the reality of a security response—and some believe it can hinder the response by providing a false sense of security. At the recent campus security conference, speakers suggested that the focus of the response should be on “seeking secure shelter,” rather than promises of a “lockdown.”

7. **Adopt an emergency mass notification and communication system—but don’t stop there.** The *RD College Safety Survey* found that more than 90 percent of schools have one in place, and since the mass killings at Virginia Tech, they’ve been the focus of active-shooter response planning. As part of reauthorizing the Higher Education Act of 1965, a grant program is now in place under which higher education institutions can apply for money to upgrade emergency communications systems to improve the efficiency of alerting students to a significant emergency or dangerous situation.

Some experts at a campus security conference, however, warned against thinking that active-shooter response begins and ends with an effective mass notification system. Because such systems can create panic, security teams must first confirm information before an alert can go out. Organizations must also have technology accompany education and training for personnel on how the alert system works as well as what to do in case of an emergency—an area in which the campus security survey highlighted a gap. While 95 percent of institutions have mass notification systems in place, only 70 percent said they educate and train students, faculty, and staff about their roles and responsibilities in an emergency.

8. **Test response plans and emergency systems.** Frequently drill security and other functional personnel on active-shooter incidents to improve their response and spot deficiencies. In some locations and for certain facilities, such as academic institutions, it may now be possible to develop drills and exercises with local law enforcement. In New Jersey, for example, the state’s homeland security director noted that more people have died from active-shooter incidents than school fires and said the types of drills and exercises that agencies and institutions conduct need to reflect this new reality. Organizations should
also regularly test emergency notification systems to discover how many individuals don’t receive timely alerts and why.

9. More solutions. Several states have recently examined the safety of their universities against a Virginia Tech-type shooting, and the recommendations are helpful to any security department or workplace violence prevention team that contends with the threat of an active shooter in an open environment. The recommendations are:

- Assess current capability in receiving, processing, and acting upon all emergency phone calls. For instance, review current dispatch operations and technologies to ensure rapid access to critical information.

- Assess staffing levels, safety, security, and emergency response equipment and active-shooter response training to ensure appropriate handling of a violent critical incident. Equipment on hand should include door-breaching equipment for gaining forcible entry into locked buildings.

- Have a communication system that is interoperable with all area responders. For instance, a security department should be able to communicate with local law enforcement, fire, and emergency medical responders through a compatible radio system.

- Adhere to the National Incident Management System (NIMS) and the Incident Command System (ICS) framework. The guidelines define personnel roles and responsibilities during a crisis and standardize emergency operations, which allows for more effective coordination and communication with responder agencies also trained in NIMS and ICS.

H. Racial Conflict

That the United States elected its first black president is surely a sign that racial attitudes in the country have changed, but to say America has become a post-racial society would be more optimistic than real.

In fact, racial hostilities appear to have been a contributing cause in the most deadly workplace shooting in 2010. Omar Thornton, in a meeting where he was being reprimanded for stealing beer from the Connecticut distributor where he worked, pulled out a gun and started shooting. By the end of his warehouse rampage, he had killed 8 employees and injured two, and then he shot himself.

According to his family—and to the shooter himself in a chilling 911 call after the shooting and before he took his life—racial bias drove the black truck driver to do it. “Uh, you probably want to know the reason why I shot this place up,” Thornton said in the call. “This place here is a racist place. They treat me bad over here. They treat all the other black employees bad over here, too. So I just took it into my own hands, and, uh, handled the problem.” He added: “I wish I could have got more of the people.”

Risk. Unemployment remains at a stubbornly high level and workplaces are increasingly ethnically and racially diverse, and that’s a risk recipe that workplace violence prevention teams and security executives need to examine. Some considerations:
• Hispanic advocacy groups such as the Mexican American Legal Defense and Educational Fund have reported a sharp rise in attacks on their constituency. Overall, hate crimes against Hispanics are up 50 percent in the most recent three years for which the FBI has statistics.

• The line recently drawn in the Arizona sand over illegal immigration exemplifies a growing us-versus-them mind-set that may increase the potential for violent attacks on targeted groups or institutions.

• Even President Obama’s election, while certainly a symbol of national unity, has sparked a “fairly major backlash” among white nationalists, according to a Southern Poverty Law Center Intelligence Report. It cited a record number of hate-related incidents in the period immediately following the election. And while Obama secured more than half of the country’s votes and the support of many urban whites, political scientists have noted extraordinary racial polarization in the vote in Southern states.

A government report issued shortly after Obama took office, which drew criticism at the time, now seems increasingly on target. The report warned that the current economic challenges and political climate are similar to conditions in the past when right-wing extremism gained momentum. (“Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment,” Office of Intelligence and Analysis, April 2009).

It specifically (and perhaps presciently) warned that the issue of immigration could be fuel for violent extremists. “Right-wing extremists were concerned during the 1990s with the perception that illegal immigrants were taking away American jobs through their willingness to work at significantly lower wages. DHS/I&A assesses that right-wing extremist groups’

A Risk That Still Needs Watching

It was a tiny little news item from 2009, but a federal discrimination lawsuit filed against the Lansing Board of Water & Light is a good reminder to organizations that racial hostilities at work won’t disappear because the country elected a black president.

Filed on behalf of a black worker in U.S. District Court in Grand Rapids, the lawsuit claims he’s been enduring a hostile work environment for years, including white coworkers’ donning KKK hoods. And it’s hardly the only recent example:

• A former armed security guard at a Connecticut gun manufacturing plant admitted in court that he drew swastikas on the desks of several minority employees. According to detectives, the security officer said feelings of being underappreciated and stress in his home life drove him to it.

• Ethnic slams followed the decapitation killing in January 2010 at Virginia Tech by one Chinese student of another. The school felt compelled to publicly reiterate its support of diversity on campus after it received several dozens of letters and e-mails school officials characterized as “xenophobic barbs.”

• Personal interviews with 327 workers found that workers cited race and ethnicity as the cause for their workplace mistreatment three times as often as workers cited gender, age, religion, or education level as the cause (“Occupational Stressors and Antinormative Behavior,” Sameer Hinduja, Department of Criminology and Criminal Justice, Florida Atlantic University, Security Journal, 2007). “Race—historically a principal basis for discrimination—remains an impetus for mistreatment in the current work [environment],” the study concluded.
frustration over a perceived lack of government action on illegal immigration has the potential to incite individuals or small groups toward violence.”

Unchecked, racial hostilities can result in workplace tragedies, as allegedly happened in 2004 when a white Lockheed Martin employee shot 14 coworkers, 12 of them black, killing five. The employee had a history of making racist comments and investigators from the Equal Employment Opportunity Commission reportedly concluded that the company had failed to quell a growing environment of racial hostility at the Meridian, Miss., plant leading up to the shooting. (State and federal authorities cleared Lockheed of responsibility, however.)

**Solutions.** Many employers embrace the concept of a melting pot of workers with different demographic characteristics, backgrounds, attitudes, ideas, and experiences. “However, they must also make a concerted effort in providing an environment of justice, tolerance, and civility within which a diverse workforce can succeed,” warns Sameer Hinduja, a member of the department of criminology and criminal justice at Florida Atlantic University.

The issue demands a high level of cooperation among company managers. Hinduja says his research finds that discrimination and harassment, coping mechanisms, and security issues are inextricably linked. So company leaders in charge of each area need to cooperate with one another when devising strategies to address the issue.

Perceptions of mistreatment can compromise the security of organizations, and as the workplace continues to become more diverse due to the overall change in American demographics, issues of discrimination and harassment will become increasingly important for workplace violence teams to address:

- Lay the foundation for preventing violence stemming from racial or ethnic tensions with a strict policy, periodic reminders to employees of acceptable and unacceptable behavior (through e-mails or training), and swift discipline for any violations. Some organizations, such as SUNY Cortland, a state university in New York, make special note of the issue in their workplace violence prevention policy: “Any acts of violence directed against individuals based on race, religion, ethnicity, gender, or sexual orientation are especially intolerable and will be subject to the strictest disciplinary actions.”
- Provide diversity training for supervisors and specifically prohibit threats based on race or ethnicity.
- Aggressively address complaints of racial harassment or threats. In the workplace, racial incidents can gain momentum and quickly deliver a devastating blow to the workplace culture.
- Take the temperature of the workplace in the wake of the slumping economy and workers being placed under additional stress.
- Be willing to acknowledge the role that race plays in workplace aggression—something that can be hard for organizations to face—and examine how its culture may lessen or exacerbate tensions.
III. CONTRIBUTING FACTORS/MITIGATION

- Consider appointing different workplace violence team members to represent different worker population groups and liaison with them. The strategy prevents cultural and language barriers from obscuring threats and ensures that any concerns are known to the violence prevention team. The “champion” for each group can also be made responsible for tracking nuances of prejudice it faces and identifying when it may be appropriate to provide updated training to managers to prevent its occurrence.

- Security teams need to track and analyze incidents and investigate complaints of harassment and bullying for any suggestion that race or ethnic discrimination is a contributing cause. Any incident, such as the discovery by security staff of a racist remark written in a bathroom stall, needs to be passed along to the violence prevention team or the company’s multicultural steering committee so that the root cause—and not just the graffiti—is addressed.

- Consider community-based violence when assessing the internal risk from race or ethnic hostilities. The violence prevention team needs to educate itself about the pressures and violence that workers face away from work. There is ample proof that outside stressors—such as the recent videotaped killing in Oakland of a black youth by a white police office that sparked citywide protests—has the capacity to pollute workplace relationships. Race and ethic tensions that contribute to workplace incidents are rarely isolated from the community, so an organization’s attempts to address them may benefit from some sort of community engagement. Studies show that in terms of racial and ethic hostilities, the relationship between the community and the factory is a reciprocal one.

I. Suicide

The number of workplace homicides fell by 18 percent in 2008, and is down 52 percent since 1994. Workplace suicides are following a very different trend line, however. They reached the highest number ever reported by the U.S. fatality census in 2008: 251. That is 28 percent higher than in 2007.

Charles Lattarulo, clinical director for employee assistance program provider Harris, Rothenberg International, told MSNBC that suicides and attempted suicides among the 2,600 organizations and 8 million employees his company’s programs cover have surged after December 2008. “We used to get these types of calls once a week, maybe once every two weeks. Now we get a suicidal call every single day.”

As with workplace violence committed against others, there is no one reliable profile of an individual who will carry out a suicide at work. However, a detailed look at data does point to individuals at higher than average risk:

- Of the workplace suicides in 2008, men account for 94 percent (but they worked only 57 percent of the nation’s job hours).

- Thirty-six percent of suicides were among employees aged 45 to 54 (but they accounted for only 25 percent of hours worked).
Another Side of Violent Acts in the Workplace

In May 2010, a 59-year-old Maryland lawyer shot himself in the head after finding out he was about to lose his job. A Chicago commuter train director—being investigated for an unauthorized vacation payout—stepped in front of an oncoming train and was killed.

Trying to stem the tide of workplace suicide has become a major focus for France Telecom SA, which has suffered 23 employee suicides since the economic downturn started. Most recently, a 32-year-old employee—who had been involved in discussions on restructuring—threw herself out a fourth-floor window of her Paris office building.

In the wake of the event, the media detailed the effort that the company said it was making to prevent future suicides. The company suspended hundreds of employee transfers that were due to take place as part of restructuring; held a conference call with its 20,000 managers, who were to hold subsequent meetings with all employees; and asked employees to watch out for signs of depression and suicidal tendencies among their colleagues.

• White workers committed 78 percent of workplace suicides (but they accounted for only 69 percent of hours worked).

Solutions. Several elements within corporate violence prevention programs can also help protect workers from doing harm to themselves, including educating supervisors on warning signs of troubled staff, opening lines of communication among managers and other stakeholders in workplace violence prevention, and a strong employee assistance program.

Coworkers play a particularly important role in suicide prevention. More than supervisors, coworkers will be exposed to indicators of trouble. Whether these workers have been given some basic tools—for recognizing the signs, knowing how to address the individual and to whom they should relay their concern—will often make the difference in whether managers have an opportunity to intervene before it’s too late. Coupled with the research showing that coworkers are frequently the only individuals in whom victims of domestic violence confide—the increase in workplace suicides suggest that employee education needs to be a significant element in company violence-prevention efforts.

J. Crowds

Technically, perhaps, an incident of workplace violence must involve the infliction of intentional harm. However, intention probably does not matter to an employee victim of aggressive customer behavior. Rushing crowds also present a real threat to the physical safety of employees.

In 2008, a seasonal Wal-Mart security guard was trampled to death by door-rushing holiday shoppers eager for Black Friday sales. Reaction was swift. A New York City councilman promised legislation requiring additional security at retail doorbuster sales. The victim’s family filed a wrongful death lawsuit against Wal-Mart and the Long Island mall where the store is located.

The security worker’s death was rare but hardly unprecedented. Every year there are several stampede and crowd-crush incidents, often with an eye-popping casualty count. Roughly
III. CONTRIBUTING FACTORS/MITIGATION

2,000 people worldwide die each year in uncontrolled crowds on average, according to University of Melbourne professor Roger Hughes, a leading researcher in the prevention of crowd-trampling deaths and injuries. In 2008, 150 died in a stampede at a temple in India and 10 at an Indonesia rock concert. In addition to spectacular tragedies, the Internet is full of amateur videos of crowds at U.S. retailers this past holiday season pushing and pulling over sales merchandise.

Crowds possess enormous destructive power, as the incident at Wal-Mart proved. The worker, who died of asphyxiation due to the rush of holiday shoppers, was 6 feet, 5 inches tall and weighed 270 pounds, according to police.

**Costs.** In pursuing a criminal case, prosecutors have a heavier burden than in a civil lawsuit, in which attorneys would only need to prove that a company should have been able to foresee the potential of a deadly stampede. In crowd-rush incidents, that is a case that attorneys may be able to make, according to several legal and security experts. Curtis Baillie, principal consultant at Security Consulting Strategies LLC, noted that injuries to customers happen every year. There has been enough history to put retailers on notice that they have a “duty” to protect their invited guests, he believes. Complicating a legal defense may be marketing and advertising that are clearly intended to attract a large crowd and create an environment of shopping frenzy.

In addition to the real risk crowds pose to safety, retailers often face the cost of defending themselves against fabricated injury claims by unscrupulous individuals who know that any time a crowd is pushing, there is a lawsuit waiting to be filed. In 2003, for example, a woman claimed door-rushing Wal-Mart shoppers knocked her unconscious on Black Friday, although it later came to light that the woman had filed 15 similar injury claims against retailers in the past. Finally, the hit to reputation when tragedy occurs surely outweighs any marketing benefit of riling up customers with the promise of super-cheap sale items. For Wal-Mart detractors, for example, the Black Friday trampling death provided them fresh ammo in their effort to paint it as an uncaring corporate bully.

**Prevention.** Crowd control is a critical crisis-management consideration for any public or entertainment venue. It is also an issue for many other organizations to consider, such as hospitals, which may need to contend with crushing crowds in a pandemic panic or large-scale terrorist attack.

Contrary to appearances, crowd behavior can be reasonably predicted, according to Hughes’s research into pedestrian traffic and modeling of actual trampling incidents. By anticipating and analyzing the crowd density, speed, and how individuals assess the situation and choose paths to reach their goal, organizers should be able to predict “danger spots” and implement appropriate traffic-control measures. Specifically, his research shows that when crowds reach a density of five people per square meter, people are in danger of being trampled. The risk from crushing occurs at a density of approximately 10 people.

His research also shows that it’s possible to avoid crushing injuries and asphyxiation that results when extreme crowd pressures build up at barriers. Although it may seem too late at this point, his study suggests that several minutes are available for taking corrective action.
(such as collapsing crowd barriers) to prevent high crowd density from resulting in injury (“Prediction of Human Crowd Pressures,” Accident Analysis and Prevention, 2006).

Health and safety experts have also identified general risk assessment factors—both physical and behavioral—that security executives should review whenever crowds are expected. Specifically, assess:

- **The location and layout of the venue and design of circulation routes.** Venues should strive to strike a balance between limiting entrances or turnstiles to control crowd flow into a cramped area and allowing a large crowd buildup outside. Use barriers to help direct crowd flows and, to the extent possible, strategically place desirable areas or amenities in an effort to spread out a crowd within a facility.

- **How much visitors know about the location’s layout and design.** According to the United Kingdom’s Health & Safety Executive, familiar visitors are likely to go to favorite places and travel familiar routes and will try to do so even if their normal route is closed. Unfamiliar visitors can block routes and create a hazard, so it’s critical to have ample signage to help people make their choices quickly. Also, in an emergency, people will escape via the exit they know best, even if it’s not the safest escape route, something emergency planners should factor in.

- **The type of crowd that is expected.** The age, social, and racial makeup of a crowd will affect crowd behavior and suggest appropriate arrangements. Safety also needs to be examined from the perspective of the crowd’s goal; for example, if it’s to gain sight of something or someone, then anything climbable becomes a potential fall hazard.

- **The physical venue features that can contribute to injury.** These include (1) steep slopes, dead ends, and locked gates; (2) the convergence of several routes into one; and (3) uneven or slippery flooring or steps.

- **The potential for hazardous conditions to develop.** These include (1) reverse or cross flows in a dense crowd; (2) crowd flows obstructed by lines or gathering crowds; and (3) large pedestrian flows mixing with vehicle traffic or other hazards.

**Retail solutions.** Below is some specific advice on crowd control for retailers to prevent crowd-rush injuries.

**Before an event:**

- Develop a written plan for the regular analysis, planning, inspection, operation, and review of crowd safety systems.

- Establish an appropriate communication strategy to facilitate teamwork and coordination among staff working the event.

- Train management and security staff in crowd control and ensure contracted security staff members have undergone crowd-management training.
III. CONTRIBUTING FACTORS/MITIGATION

- Research similar past events, comparable events in the area, and consult with marketing and sales to achieve an accurate idea of the numbers and type of crowd expected to attend.

- Inform law enforcement of the event and expected crowd size.

- Assess the arrangements in place to control crowds, such as force level, and assess their adequacy against the expected size/type of crowd.

- Erect sturdy barricades to control the flow of entrants.

- Set targets for crowd management that, if exceeded, will trigger a response (such as opening new service points).

- Locate big-sale items in different areas within the store and use signage to direct shoppers to them.

_During the event:_

- Use snaking crowd lines that lead away from the entrance.

- Consider handing out claim tickets to those in line for the specially priced merchandise.

- Communicate via bullhorn or other means with individuals in line and provide safety precautions, updates, and instructions.

- Attend to the comfort of those in line by providing drinks, snacks, or entertainment.

- Allow entry in stages.
IV. LEGAL/REGULATORY CONSIDERATIONS

At all stages in addressing workplace violence—from wording a policy to assessing a threat—a company needs to consider its legal liability and regulatory obligations. Legal counsel should participate on the workplace violence prevention team and review whether the company’s effort to prevent violence is in accordance with its obligations under the law. The legal landscape is littered with cases in which employers have been found liable in cases of workplace violence. And when they are, jurors are often generous with corporate cash.

Legal and regulatory risks include:

- **Fines from OSHA.** An employer who learns that a current or former employee has threatened violence against another employee may have to take certain preventive steps under federal OSHA and state plans to provide a workplace that is free from recognized hazards that are likely to cause an employee harm.

- **Negligent hiring, supervision, and retention lawsuits.** These tort cases can cost a company millions and are based on the principle that an employer has a duty to protect employees and customers from injuries caused by employees whom the employer knows,
or should know, pose a risk of harm to others. If a company discovers that an employee is prone to violence yet keeps them on, it may be liable under this theory for any harm the employee causes to another.

- **Harassment claims.** Companies may face lawsuits for creating or permitting a hostile work environment to exist.

- **Failure to notify torts.** Again, laws vary by state, but employers may also be liable—and face large judgment awards—if they fail to disclose a threat or conceal hazards from an employee and then an act of violence occurs in which that employee is injured.

- **Inadequate security lawsuits.** Companies may face lawsuits if they fail to take reasonable security precautions given the risk. Judgments usually come down to whether or not the violent act was foreseeable and, if so, whether the company’s reaction was reasonable.

- **“Respondent superior.”** An employer may be liable for an employee’s act when the employee carries it out in the course and scope of his or her job duties.

- **State and local regulation.** Companies may face penalties for violating specific requirements under state and local law. These address a range of issues: from lighting and staffing requirements at high-risk establishments and conducting employee background checks for employees who interact with vulnerable populations to workplace security protections that must be afforded victims of domestic abuse.

Because liability can arise from any number of federal or state statutes, regulations, or judicial decisions, companies would be wise to approach workplace violence prevention with the eventuality of a lawsuit in mind. While state workers’ compensation is intended to provide the sole remedy for injuries arising out of an individual’s employment, legal maneuvering by plaintiff’s attorneys has created myriad exceptions to the rule.

Insurance can help reduce the risk associated with lawsuits stemming from violent incidents. Some policies cover tangible costs, such as medical bills, attorneys’ fees, lost wages, security

---

**Security Burden Now Shifts to Businesses When Crime Rises**

There is a move toward a regulatory reaction to crime, likely due to tight city and state budgets that make it hard to combat rising crime by increasing police presence. When crime spikes, city councils are now less likely to discuss putting more cops on the beat and more likely to craft ordinances requiring businesses to adopt security measures. Some recent examples:

- Anxiety over late-night violence caused Wichita, Kan., to push tougher safety regulations for nightclubs and drinking establishments.

- The Houston police department has started enforcing new regulations that require convenience stores to register with the police, provide safety training to employees, and install security equipment such as drop safes, surveillance cameras, and panic buttons.

- The Dallas City Council passed a series of rules to make convenience stores safer by requiring all of them to install high-resolution cameras, silent alarms, and drop safes.
IV. LEGAL/REGULATORY CONSIDERATIONS

costs, rehabilitation, and property damage; others include coverage of intangible costs, such as lost staff time, staff replacement, training expenses, and absentee wage costs. But while insurance is a helpful risk mitigation tool, it should not be considered a shield against the expenses from lawsuits arising from workplace violence.

In short, if a significant violent episode takes place, a company should expect that its workplace violence prevention activities will go on trial. Therefore, as companies examine risk and implement a prevention program, they should do so with the mindset that a jury might also review it one day.

Again, companies need to consult legal counsel before making any changes and identify the specific liabilities they face given their location, industry, and history of crime. The general information below is solely designed to point workplace violence teams in the direction of legal and regulatory issues that they should examine more fully.

A. General Liability Prevention

Strategies to reduce liability are found throughout this report and included further along in this section. For example, specific information regarding negligent hiring lawsuits and strategies to avoid them are discussed below and in the section on pre-employment background screening earlier in this report. More broadly, however, the labor law firm of Littler Mendelson (www.littler.com) developed a practical seven-step approach in response to the phenomenon of workplace violence in the 1990s and employers’ growing legal obligations to control it. Organizations can go a long way toward reducing liability and demonstrating a good faith effort toward addressing workplace violence if they:

• Make preventing and controlling workplace violence a priority and form a team of key employees to develop, review, and implement policies dealing with violence.

• Talk with employees and supervisors about early warning signs of potentially violent behavior and steps to be followed in responding to and investigating an incident of workplace violence.

• Increase physical security measures and develop a relationship with local law enforcement authorities.

• Develop crisis procedures for responding to an incident of workplace violence.

• Investigate and respond to threats of workplace violence.

• Make efforts to prevent workplace violence by properly pre-screening employees, consistently enforcing workplace rules, and using an employee assistance program and medical care resources.

• Establish clear internal and external lines of communication to avert and respond effectively to crisis situations.
Addressing foreseeable threats

The issue of foreseeability is a cornerstone of lawsuits arising from incidents of workplace violence. If an employee commits a violent act, the courts will seek to determine whether the company should have known the employee was prone to violence and, therefore, should have refused to hire or dismissed the employee. And if an outsider during a robbery attempt hurts employees, the courts will ask: Should the business have known such a crime would occur and, if so, should it have done more to protect employees?

Experts including Daniel Kroop, a representative of CAP Index Inc. (www.capindex.com), a risk-intelligence firm specializing in crime forecasting, identified eight steps in building a data-driven security program that can help an organization demonstrate that it performed its due diligence in assessing the risk of violence to employees.

1. Evaluate your external environment. When you go into court, local police crime records are sure to be introduced, says Kroop. The mistake companies frequently make is to rely on data that is too old. Data based on a site survey from 2004 won’t fly in 2008. External crime data should not be more than two years old, and security directors should develop a mechanism to learn of crime alerts. Data are often free from local police departments, can be supplemented with data from the FBI’s Uniform Crime Report, and are commercially available from consultant firms. Even if you find some data are unavailable, documenting that you conducted a good-faith search for the information is valuable in a court case. Contrary to a persistent security industry myth, companies do not lessen their liability by intentionally keeping themselves in the dark about security risks.

2. Evaluate your internal factors. Examine the nature of your business risk: Do you invite the public in? Do operations, such as handling cash, make it attractive to criminals? Are there attractive nuisances nearby, such as gas stations and liquor stores? Tip: Use employee perception surveys to gauge their perception of area crime. “You can get a lot of valuable insight by polling your employees,” says Kroop.

Workers’ Compensation Can Limit Loss—But Don’t Count on It

Workers’ compensation is the typical remedy for employees if they suffer an injury while at work, including in cases of workplace violence. In July 2005, for example, the U.S. Court of Appeals for the Fifth Circuit (covering Texas, Louisiana, and Mississippi) ruled that the 2003 workplace shooting of 14 employees at a Lockheed Martin plant in Meridian, Miss., was a workers’ comp. matter. The employee’s rampage shooting “cannot be separated from the employment status of his victims,” said the ruling, which limits the damage awards to victims to roughly $150,000 apiece.

But such rulings don’t deter plaintiff’s attorneys—and they don’t always lose. If a workplace shooting occurs, companies can expect a lawsuit regardless of how the state’s workers’ comp. rules are written. For example, there is now a lawsuit making its way through the courts against DaimlerChrysler, filed by a worker who was wounded when a coworker entered its Toledo, Ohio plant with a concealed shotgun and opened fire. The worker alleges that DaimlerChrysler and its security company are liable for damages because the automaker knew that the worker, if allowed unimpeded access to the plant, would pose a risk of violent harm to his coworkers.

Only one thing is certain about the case outcome: Win or lose, the legal bill will be substantial.
3. **Examine an incident history.** This goes beyond having a file cabinet of incident reports. Use an incident reporting database to conduct trend analysis and keep accurate and complete internal incident records. Generally speaking, courts perceive crime statistics relative to the organization’s property as a more important factor in negligent security lawsuits than area crime statistics. The absence of significant incidents can be used in court to successfully defend the security measures you decided to take. For example, the California Supreme Court ruled that California law imposes no duty on an owner of a commercial parking garage to provide security guards or take other measures to prevent criminal acts on its premises if it has a record of no assaults on the property in the past 10 years (*Sharon P. v. Arman Ltd.*, Cal., No. S063612, 12/16/99).

Additionally, organizations must be aware of all corporate documents that address issues of risk. If any department creates a paper trail denoting the risk of violence but fails to share data with the security department or the workplace violence prevention team, a company will probably fail to align security measures with the documented risk. And, in a lawsuit, an organization will have a tough time explaining why.

4. **Consider the experience of other local businesses.** Seek information about the existence of any incidents at similar businesses nearby, and employ security measures that are equal to or better than those of other firms. If you deploy less security than similar neighboring businesses, you will need data to show why you thought less security was adequate. This factor tends to be of particular concern to juries, say legal experts in negligent security cases. Companies should remember that security lawsuits tend to be very “local,” says consultant and researcher Dr. Rosemary Erickson (Athena Research Corporation). “What the Mobile does on one corner can affect a security case against a Shell station around the block,” she says.

5. **Meet the recognized standard of care for your industry.** While doing so doesn’t ensure victory, it’s especially hard to win in the absence of it.

6. **Measure your policies and procedures.** “If you’re not practicing your policies and procedures, either change them or get rid of them,” says Kroop. The first thing an expert witness will examine is your policies and procedures to see if you live up to them, he notes.

7. **Review and evaluate your program against your findings.** Examine them every six months to one year and document what you find and what you did as a result.

8. **Solicit an outside expert to review your program.** Also, have a formal process for conducting yearly reviews of the security program and immediate reviews in the wake of a significant incident.

**Violence prevention documentation.** Employing target-hardening security strategies in line with the threat is key for preventing a lawsuit claiming inadequate security. But it is possible for an organization to win or lose a case over issues that have nothing to do with the actual physical security operation. “Companies may be doing what they are supposed to be doing, but they fail to document it,” says Alan Kaminsky, an attorney with Wilson Elser Moskowitz Edelman & Dicker, LLP (www.wemed.com). “It’s one thing to do your job properly and another thing to prove it to a judge or a jury.”
It’s critical to have a paper trail that includes accurate staffing and training records, and to maintain it for a minimum of three years, notes Kaminsky. “The best defense is to have your information documented to the point that you can produce it in court if you ever need it,” agrees Kroop.

B. Workplace Safety Regulations

Occupational Safety and Health Administration (OSHA)

There is no federal standard addressing workplace violence, and the Occupational Safety and Health Administration (OSHA) has no rulemaking planned in the area of workplace violence. However, the Occupational Safety and Health Act includes a general duty clause—Section 5(a)(1)—under which the agency can issue penalties to companies that fail to address the risk of workplace violence. The general duty clause states that each employer covered under the OSH Act has a “general duty to furnish each employee with employment and places of employment free from recognized hazards causing or likely to cause death or serious physical harm.”

There are many examples of OSHA citing companies for a general duty clause violation for substandard workplace violence prevention. These include: a hospital’s failure to protect its employees from violent patient behavior and a property management firm’s failure to adopt security measures to protect apartment complex staff from assaults by tenants.

In response to a question from an employer, OSHA issued a standard interpretation letter on Oct. 30, 2006 on the intersection of workplace violence and federal safety regulations. The letter, written by OSHA’s director of enforcement, states: “In a workplace where the risk of violence and serious personal injury are significant enough to be ‘recognized hazards,’

A Typical OSHA Investigation of Workplace Violence

In November 2007, an OSHA director described a fairly typical OSHA case involving a 122-bed psychiatric facility in the South.

OSHA was prompted to investigate after receiving a complaint. When it went in, it found that the psychiatric facility had a solid training program and recorded and reported injuries in accordance with OSHA standards. But agency investigators were concerned that the facility was not doing enough to prevent human bites to employees’ hands, arms, and shoulders, which data showed were the most common type of injury to staff.

Another problem OSHA found was unsecured items in the day room of the acute unit that could be used as weapons, including television equipment, chairs, and tables. Elise Handelman, director of OSHA’s Office of Occupational Health Nursing in the Directorate of Science, Technology, and Medicine, says the ceiling also had metal strips, which were taken down by adolescents and used as swords. There were also concerns that staffing ratios were insufficient to prevent injuries.

Following the investigation, OSHA sent the facility a hazard alert letter requesting that it address human bites, maintain staff ratios, and secure equipment. But it assessed no penalties.

“Do these actions do any good?” asks Handelman. “I think yes, overwhelmingly they do begin to move us toward greater protection for employees, and they increase awareness among employees and employers” about workplace violence. In addition, she says, they raise “expectations that if there is a problem, OSHA will come out.”
IV. LEGAL/REGULATORY CONSIDERATIONS

the general duty clause [Section 5(a)(1) of the Occupational Safety and Health Act] would require the employer to take feasible steps to minimize those risks.” The letter added: “Failure of an employer to implement feasible means of abatement of these hazards could result in the finding of an OSH Act violation.”

However, it is difficult for OSHA to cite employers under the general duty clause, according to Elise Handelman, director of OSHA’s Office of Occupational Health Nursing in the Directorate of Science, Technology, and Medicine. In order to issue such a citation, OSHA must prove that: the employer failed to keep the workplace free from the hazard to which employees were exposed, the hazard was recognized, and the hazard was causing or likely to cause physical impairment or death, Handelman says. But the most difficult thing to prove is the existence of a feasible and useful method to correct the hazard, Handelman says. Examples of controls for workplace violence are increasing the number of staff, deploying physical security measures, and providing employee training.

Recently there has been mounting criticism that weak civil penalties and even weaker criminal fines under the Occupational Safety and Health Act are holding back progress in reducing workplace fatalities. In April 2008, at a hearing to examine penalties for worker fatalities under the Act held by the Senate Health, Education, Labor and Pensions Committee, a parade of witnesses decried the infrequency of OSHA inspections and frequent penalty reductions for cited violations.

Serious violations of OSHA standards—those that pose a substantial probability of death or serious harm to workers, are subject to a maximum penalty of $7,000, notes Peg Seminario, director of safety and health for the AFL-CIO. Willful violations and repeat violations carry a maximum penalty of $70,000, and willful violations have a minimum penalty of $5,000. Moreover, Seminario says, the maximum civil penalties provided for under the OSH Act are rarely assessed.

State regulations. Workplace violence can slide down the scale of safety priorities due to the fact that, unlike many other causes of worker injuries, there is no federal standard addressing it (as noted above, it is covered only under the general duty clause that specifies that employers have an obligation to maintain a workplace free from recognized hazards).

While this hasn’t changed, companies should be aware that several state plans place greater obligations on employers to protect staff from violence. For example, several existing provisions of the Washington Administrative Code (WAC) may apply to the hazards of violence in the workplace. It includes one provision that is specific to late-night retail (WAC 296-832, the “Late Night Retail Workers Crime Protection Standard”) and provides specific violence-related direction to retail businesses that operate between 11:00 p.m. and 6:00 a.m.

According to Aaron Trippler, director of government affairs at the American Industrial Hygiene Association, the issue of workplace violence is also a growing safety concern at the state level. Trippler said that workplace violence ranks among the top rulemaking and enforcement issues at the state level (along with mold analysis and safe patient handling). “[States] have become very proactive in taking a look at specific issues within their state
that they think need to be addressed immediately. The states are probably the leaders right now, and federal OSHA is not.”

Additionally, states and municipalities have increasingly been addressing the issue in targeted regulations. Companies need to be aware of their obligations, as some regulations are narrowly defined for specific types of establishments.

For example, some states, such as New Mexico, have specific guidelines that define robbery prevention training requirements for late-night retail workers, a worker population that is frequently victimized in violent incidents. In New York in 2006, Gov. George Pataki signed into law a bill that requires public employers with more than 20 employees to assess risk and develop and implement a written plan of action to prevent potential workplace violence.

C. Policies

Zero tolerance

Companies have broad authority to establish whatever workplace violence policies they deem appropriate, but in some cases courts have found that company policies have gone too far.

Case in point: A Court of Appeals decision, while reiterating the right of employers to enact policies that prohibit verbal threats, violent behavior, and physical conduct that jeopardizes safety—and even restrict speech to protect workers—ruled that employers cannot always enforce policies that are so broad that they include mere expressions that have “violent overtones” but which are not threats themselves. In these cases, it is possible for a workplace violence policy to infringe on an employee’s free speech (Bauer v. Sampson, U.S. Court of Appeals, 9th. Cir., Nos. 99-56964; 00-55408; CV-98-10686-GAF, Oct. 15, 2001).

The Ninth Circuit Court of Appeals made this ruling in the case of a community college professor who, upset over actions by the college’s Board of Trustees, published articles that included violent overtones in a campus newspaper. For example, the professor wrote that,
IV. LEGAL/REGULATORY CONSIDERATIONS

Just How ‘Zero’ Can Zero Tolerance Be?

A hotel restaurant worker had qualms about her employer’s work scheduling policy and complained, which prompted a change that didn’t go over well with everyone, including a 22-year veteran hostess. Jokingly, she placed her hands around the neck of the “complainer” and gently shook for a few seconds while laughingly noting, “It’s all because of you!”

That didn’t go over with the hotel, which fired the hostess for violating its zero tolerance workplace violence policy. The dismissed employee sued and the case went all the way to Hawaii’s Supreme Court. Ultimately, the state’s highest court agreed that the worker was just joking, but it still denied the hostess’s claim. It said joke or no joke, her action “was in deliberate disregard of the standards of behavior which the employer had a right to expect of an employee.”

Organizations need to craft their workplace violence policy carefully and resist the urge to apply it “automatically.” It should prohibit verbal threats, violent behavior, or physical conduct which interferes with employee safety in the workplace (that is wording that courts have suggested is okay). However, employers should be wary of a blanket policy of disciplining every mere expression that has a “violent overtone” if the expression is not a threat. In these cases, a workplace violence policy may indeed infringe on an employee’s free speech. In other words, workplace violence committees should review each case individually and attempt to discern the employee’s intent. They should resist the urge to let certain “workplace words” trigger automatic reprisals.

Companies should also be careful with respect to identifying “threatening language” as a cause for automatic dismissal. Some experts note that people of varying ethnic, racial, religious, generational, or economic groups may use different language and gestures to express themselves, and that natural and harmless expressions by one group may be perceived by another as aggressive and threatening. While companies need to prohibit hostile and aggressive behavior, they need to be careful not to misinterpret innocent behavior or language as having a hostile intent. Furthermore, there have been instances in which zero tolerance policies have been used by management to harass specific employees, and workplace violence prevention teams need to audit how the company applies the workplace violence policy to ensure integrity in enforcement.

Weapons

Companies have broad authority to establish policies banning weapons on company property. However, even this fairly straightforward right is running into complications. Employers
should be wary that state legislatures—unwilling to wait for the federal government to weigh in—continue to press the issue of employer gun bans.

In 2010, Indiana passed a law that allows employees and invitees in the state to keep guns concealed in their cars while at work. Florida passed a similar law in 2008. The list of states that have addressed the issue also includes Alaska, Florida, Georgia, Idaho, Kentucky, Louisiana, Minnesota, Mississippi, Montana, Oklahoma, and Utah.

Each law is different, and organizations should have legal counsel review their state’s law to assess how it comports with their workplace weapons policy. The Florida law is typical of several, however, and includes the following restrictions:

- Employers can’t prohibit employees licensed to carry concealed weapons from keeping firearms in their locked vehicles on company property.

- The law also places several associated restrictions on employers, including a prohibition against asking workers about guns in their vehicle, searching an employee vehicle, and conditioning employment on an agreement about guns in vehicles or whether an employee holds a concealed-weapons permit.

- Exceptions include company vehicles; also, schools, nuclear power facilities, state correctional facilities, and companies whose main business is producing combustible or explosive materials are exempt.

The most notable legal development in the battle over employers’ private property rights and employees’ Second Amendment rights is a ruling by the U.S. Court of Appeals for the 10th Circuit in the battle over an Oklahoma state law that holds employers criminally liable for prohibiting employees from storing firearms in locked vehicles on company property (Ramsey Winch Inc. v. Henry, 10th Cir., No. 07-5166, Feb. 18, 2009).

Although the verdict directly affects only Oklahoma employers, the case is significant. The case is the first court test of the argument that when a state law allows workers to have guns at work, it forces employers to violate federal OSHA rules that require employers to keep workplaces free from recognized hazards. Winning would have reversed the nationwide legal trend and placed decisions about workplace security measures back in the hands of property owners and their security executives, but the reversal by the U.S. Court of Appeals for the 10th Circuit in February strikes a blow to that hope. The verdict went so far as to infer meaning from OSHA’s silence on the issue. “OSHA is aware of the controversy surrounding firearms in the workplace and has consciously decided not to adopt a standard,” said the circuit court.

Indeed, in a Jan. 16, 2010, letter to an Oklahoma state senator, Acting Assistant Secretary of Labor for Occupational Safety and Health (OSH) Thomas M. Stohler said the agency does not believe the general duty clause preempts the state’s law. According to the letter, Stohler said that gun-related violence is not a “recognized occupational hazard in industry as a whole” and “state laws protecting an employee’s right to transport and store firearms in a locked car” do not impede the general duty clause of the OSH Act.
IV. LEGAL/REGULATORY CONSIDERATIONS

The appeals court recognized the possibility that an employer may violate the general duty clause for failing to prevent workplace violence if the risk is clear and recognizable, but it said the district court’s interpretation that guns in employees’ vehicles rose to the level of being a “recognized hazard” was mistaken.

On this issue, the momentum is clearly with state legislatures and the National Rifle Association. In addition to the several states where guns-in-cars laws have recently passed, new laws are under consideration in other states. For example, by a 26-2 vote, the Alabama state Senate recently approved a bill to prohibit companies from restricting employees from keeping firearms in their locked vehicles at work, and it is likely to become state law.

However, when state laws directing otherwise aren’t in effect, employers can enforce bans on firearms at workplaces. In March 2009, the U.S. 6th Circuit Court of Appeals granted summary judgment to an employer in a wrongful discharge case. The employee was fired for possessing firearms at work in violation of company policy. His case was tossed because Ohio does not have a clear public policy of allowing employees to have firearms on the property of private employers (*Plona v. United Parcel Service, Inc.*, No. 08-3512, March 6, 2009).

**Ramifications.** Companies need to be mindful of maintaining policies that are aligned with state laws as they expand the rights of those with permits to carry concealed weapons. Some legal experts warn that these guns-in-car laws create a new breed of protected worker whose rights security teams must be wary of violating with prohibited searches or questioning. Under the laws, gun owners have the same rights as other protected workers to sue if they feel they’ve been discriminated against because they own a gun or keep one in their car.

“We’re now equating people having guns with groups protected for their sex, race, or religion,” said Allan Weitzman, a partner at Proskauer Rose LLP. There definitely will be trumped-up discrimination cases over the issue, he predicted. “Somebody’s going to get fired ‘and it’s because you know that I have a gun. I’m exercising my rights, and that’s the pretext for your getting rid of me.’”

Affected employers should consult legal counsel, take actions to comply with the law, and address the security concerns it raises. Affected companies may need to:

- Revise employment applications, eliminating any questions about whether a job seeker has a concealed weapons permit.
- Remove reference to a blanket gun ban from the employee handbook.
- Train supervisors and security staff on questions that are now not permitted under law.
- Train security staff on new restrictions to vehicle searches.
- Consider issuing a companywide memo expressing a commitment not only to obeying the law, but also to protecting the safety of employees and clarifying the company’s policy against bringing a weapon into the workplace.
Open carry. In addition to the battleground described above, the open-carry movement—licensed gun owners who purposefully test employer policies by visibly wearing their firearms—provide a challenge for workplace violence prevention teams. Organizations should review their state’s law on the matter and determine whether it requires them to take specific actions to protect their right as a property owner to ban guns from their premises. The failure to meet these requirements can affect a company’s liability should an incident involving a weapon occur.

States treat the matter in any number of ways. In Arizona, for example, individuals with a concealed-carry weapons permit can carry their weapons concealed or out in the open. But Arizona business owners can demand that a gun-toting individual leave their premises regardless of whether they have posted a no-gun sign. If the individual refuses to leave, he or she can then be arrested for trespassing.

But some states do require signage to enforce a criminal trespass approach to banning weapons from company property. This approach typically applies to all individuals on business premises including employees, customers, and visitors, note attorneys Garry Mathiason and Jodi Kruger (“Weapons in the Workplace: The Employer’s Response,” SHRM legal report). If an employer pursues this approach, they offer the following general recommendations:

- Post signs prohibiting weapons on the property to place a potential trespasser on notice that bringing a weapon onto the premises is not permitted. Place signs at the restricted entrance so, for example, if an employer desires to prohibit weapons in the parking lot, there’s a notice at the entry to the parking lot. This notifies employees and others of possible criminal prosecution for violations (i.e., that it is not simply an internal policy violation but can be a criminal offense). It may be possible to follow a criminal trespass policy without signage, but usually unlawful trespass will only occur, as in Arizona, if first an individual is asked to leave and refuses.

- Place employees and visitors on notice of a potential search by the company and by law enforcement authorities to reduce privacy expectations.

- Company policy and postings should make it clear that the employer disclaims legal responsibility for enforcement, beyond disciplining employees and requesting individuals to leave the premises. Enforcement of criminal trespass laws should be left to the authorities.

The expansion of state concealed weapon permits has a dramatic impact on security in public spaces, from shopping malls to convention centers, and demands that facilities re-consider their security levels. Companies also need to aggressively reiterate their policies on weapons in the workplace to coincide with a law’s passage so employees remain clear about what the firm expects of them.

D. Hiring and Supervision

In a conference presentation in August 2010, Barry Nixon, president of the National Institute for the Prevention of Workplace Violence, described motivations that are often associated with acts of workplace violence—such as financial troubles, personal relationship issues,
emotional problems, and substance use. He then noted, “Most of these behaviors can be detected in a thorough background investigation,” which is the reason that deficiencies in this area often result in lawsuits.

Negligent hiring claims are a fast-growing area of employment litigation, warns Lester Rosen, an attorney and president of Employment Screening Resource. It is also likely to grow as a cause of action as conducting criminal background checks gets easier. Through corporate data breaches and resulting news coverage, the public has become acutely aware of the wealth of information that is available about individuals with a few clicks of a mouse. Employers that forgo a background check for any individual, even someone being considered for a low-level job, now face a greater risk of lawsuit if that individual has a criminal history and subsequently commits a violent act.

Statistics also suggest that in cases of a violent outburst involving staff, lax oversight or negligent retention is at the heart of an equal number of lawsuits as negligent hiring. A growing number of employers are being forced to defend themselves in costly litigation alleging negligent retention, according to attorney Eric Hobbs (Michael Best & Friedrich, LLP; www.mbf-law.com).

When lawsuits do arise, companies often lose. A study of California jury verdicts in employment cases found that employers lose 60 percent of negligent hiring/supervision lawsuits. Jurors tend to believe the employer had the duty, ability, and resources to perform safe hiring. Today’s legal environment is one of “if you could have known, you should have known,” says Rosen.

Standard defenses, such as claiming the employee lied on the job application, that the organization is also a victim of criminal behavior, or that past employers didn’t warn of

FROM THE FIELD...

**Background Checks on Low-Level Employees Can Be a Worthwhile Expense**

In November 2006, James Ealy quit his job as a maintenance worker at a Burger King restaurant in Lindenhurst, Ill. A few weeks later, police say Ealy went to his old employer’s restaurant after closing, got inside, and strangled to death the store manager with her uniform’s bow tie before emptying the store safe.

Flashback to 1982. James Ealy strangles to death four members of a Chicago-area family, but his conviction is overturned when an appellate court rules his confession was coerced. It taints all the subsequently obtained evidence proving he did it, and Ealy walks on the murders. However, prosecutors were able to make stick a sexual assault charge in an entirely separate case, and on that Ealy serves nine years of a 23-year sentence. Shortly after his release, he returns to jail to serve three years of a 10-year sentence for threatening someone with a gun and a knife.

It’s no surprise that Burger King and the regional dining services company that ran the Lindenhurst franchise were hit with a wrongful death lawsuit in the Ealy case. The victim’s family claimed several security missteps led to her death. She was made to count money while alone in the store. The alarm system wasn’t activated and was inadequate even if it had been turned on. Ealy kept a key to the store after quitting, which is how he likely got into the restaurant on the night of the murder. And at the very core of the lawsuit was the family’s claim of negligent hiring and supervision: If the restaurant had bothered to do a simple criminal check, it would have uncovered Ealy’s track record of murder and sexual assault.

How does the story end? The family of the slain restaurant worker accepted a $2 million settlement. And the restaurant where it happened closed for good four months after the incident because the customer count never rebounded after the murder.
dangerous behavior, are not likely to help your case, says Rosen. And legal experts also warn against thinking that using a vendor to conduct background screening absolves a company of liability. Employers are likely to be a party in a lawsuit whether they conducted the check themselves or hired someone else to do it. Companies are expected to know what checks the screening service conducts and may be liable if they prove to be insufficient.

“It’s the new darling of the lawyers who want to make money off corporations,” reported Carl King, founder and CEO of Selection Management (www.insights-inc.com), in an ABC News report. “If an employee does something bad, then maybe the employer’s responsible.”

To reduce liability, companies need to:

1. **Take action in the hiring stage.** While plaintiff’s attorneys can take aim at a variety of failures in the wake of a violent incident, many cases revolve around an employer’s failure to take basic precautions when hiring the individual who is the cause of a plaintiff’s injuries, says Hobbs. “Generally, negligence in hiring involves failures to act. It’s very uncommon for an employer to be sued for negligence after doing something affirmatively in the hiring process. So we’re talking about hiring someone without looking into their criminal background or failing to check references that would have alerted the employer to a problem,” Hobbs says. David Mendholson, a partner with Piper Rudnick (www.dlapiper.com), agrees that action is the best form of lawsuit prevention. “Uninformed decisions are more vulnerable to legal action [than informed ones],” he says. Companies should examine the recommended practices for background screening detailed earlier in this report. For reducing liability, companies should:

   - Perform thorough pre-employment screenings that include criminal background reviews.
   - Make calls to previous employers and all references.
   - Seek additional references and information from the job candidate if reference checks fail to provide meaningful information or raise additional questions.

---

### When Lax Supervision Is to Blame for Employees’ Poor Judgment, Attorneys Pounce

An appeals court recently upheld a jury’s $1.5 million judgment for a plaintiff who sustained injuries and disability in a fight with an off-duty restaurant employee who felt the customer had made advances toward his girlfriend. The court ruled the jury was reasonable in its finding that the fast food operator negligently failed to train and supervise its staff.

The case highlights the need for companies to document their training so they can demonstrate that any aggressive behavior by staff goes against what they have been told. “The fact that [the worker] apparently felt comfortable in behaving in such an improper manner on restaurant premises raises troubling questions regarding the level of training,” the court wrote.

Furthermore, that another employee joined in the fight and “that a restaurant chef’s instinctive reaction upon learning of the fight was to go witness the altercation rather than break it up or notify management strongly supports a conclusion that there was a general failure on the part of Captain D’s to properly supervise and train their employees at this particular franchise.”  ([Foradori Jr. v. Garious Harris, etc., et al., Captain D’s LLC, United States Court of Appeals Fifth Circuit, No. 06-60030, April 1, 2008.])
• View inconsistencies and gaps in employment with a suspicious eye. Résumé problems require companies to seek additional information and explanation from the job candidate.

2. Conduct performance appraisals and investigate problems. “A plaintiff’s attorney can butcher employers that fail to consistently monitor the performance of their workforce and assess foreseeable risks,” says Hobbs. An appraisal should focus not only on the worker’s job performance, but also on a range of risk factors, such as how they interact with others and conflicts or problems they’ve had dealing with others. Hobbs adds that employers must immediately investigate all suspicious or dangerous behaviors exhibited by their workers. “It sounds so obvious, but some employers don’t do it,” Hobbs notes. If there is a report of an incident, the companies need to immediately examine it, because if an event leads to a lawsuit, companies will need to show that they made a reasonable effort to look into the problem, he adds.

3. Understand your state’s law. To reduce liability, it is critical for an organization to know exactly how each state in which it operates views negligent hiring. The bar is set at various levels in different states. Some states require employers to conduct criminal background checks; some allow cases of negligent hiring to proceed if the violent act was related to the employee’s duties during work hours and work locations; and in a select few, negligent hiring is only recognized if the employee’s act victimized an individual through company objectives, such as during the eviction of a tenant.

Employers must also take note of new laws for background checks that states have enacted to protect vulnerable populations. New requirements for background checks have been passed in Tennessee (childcare workers), Maryland (employees of private schools), Hawaii (youth workers, nursing care service workers, and other healthcare-related employees), Virginia (public school contract employees and care workers for the elderly, children, or the disabled), and other states.

4. Balancing privacy concerns. Various local, state, and federal laws limit an employer’s right to obtain and use information for screening job applicants. Organizations should take several basic precautions to reduce the potential for legal problems.

• Inform applicants in advance of any background checks, secure their written consent to initiate the verification process, and make a full disclosure of the kinds of information you’re gathering and the purpose for requesting it.

**FROM THE FIELD...**

**Check Criminal Records Pre-Hire (After May Be Too Late)**

A Home Depot store in Hawaii hired a sales associate without conducting a criminal background check. Three years later, when the worker was up for a promotion to department supervisor, the store checked his history, found a drug conviction from five years earlier, and promptly fired him. The worker claimed that since he’d been a good worker and had passed several drug tests while employed, his firing was discriminatory and violated a state law that prohibits employment bias based on arrest or court record. The Hawaii Supreme Court agreed, noting that employers must prove that a criminal conviction is rationally related to the duties and responsibilities of the job in order to take a negative action against an employee (*Wright vs. Home Depot U.S.A Inc.*, Hawaii Supreme Court, No. 27190, 9/8/2006).
• Limit inquiries to verifiable job-related information, and ask the same questions about each prospective job candidate for a position. Avoid questions that state guidelines or federal law consider improper.

• Check the accuracy of information before using it to reject an applicant. Make sure your company has a demonstrable, business-related reason for using the information to reject the applicant. Give applicants sufficient time to contest negative information. Take note of estimates that nearly one percent of positive hits in online criminal checks are because of clerical errors.

• Weigh background information in the same way for all candidates of a particular position.

• Make sure that any references that you contact are familiar with the candidate and in a position to provide relevant job-related information.

• Be careful in the wording you use when asking about criminal convictions on the application form. State on the application that a prior criminal conviction won’t necessarily bar employment. Avoid an overly broad question about whether the applicant has been “convicted of any crime.” Also, some states draw a distinction between how you can treat job applicants who have prior convictions for a felony (more serious crimes) versus a misdemeanor. Check with an employment lawyer in your state for specifics.

A comprehensive, written employment screening policy will also reduce inconsistencies that can lay the framework for a lawsuit, according to employment attorney Mark Neuberger (Buchanan Ingersoll Professional Corporation; www.buchananingersoll.com). He notes that employers have the right to refuse to hire a candidate who misstates information on an application so long as they are consistent in such conduct. Similarly, he warns against interview questions that vary widely from applicant to applicant.

E. Threat Assessment

When a company needs to conduct a threat assessment on an employee, legal questions are likely to crop up about the worker’s privacy rights. Such questions could involve asking about an employee’s mental health history or private life. “But it can be done with the right consents and disclosures,” says attorney Rebecca Speer, principal of Speer Associates, an employment law firm in San Francisco that specializes in workplace violence prevention.

Most legal experts also recommend that when the safety of the workplace is a legitimate issue, it should trump an individual’s privacy concerns. “You’ve got to look down the line and say, ‘If I don’t do this, which legal case would I rather be defending,’ ” says consultant and workplace violence expert Mark Braverman. “If you feel the risk is great enough, go ahead and do it and defend your actions down the line.” Speer echoes Braverman: “There is no law I know of that would prevent a company from appropriately addressing behaviors found to be threatening or potentially violent,” she says.

**Americans with Disabilities Act.** Wisely, most organizations tread lightly where the Americans with Disabilities Act (ADA) is concerned. But what impact does the ADA currently
have on a company’s ability to manage workplace threats? Perhaps less than some companies may think. The ADA may protect drug addicts or mentally ill employees, but if such an employee crosses the line, for instance by threatening a co-worker or committing an illegal act, companies do not have to tolerate it. And this applies even if the behavior is the result of the employee’s addiction or illness.

Deciding what to do is a matter of assessing risk, say legal experts. Companies do open themselves up to a lawsuit claiming unfair termination by firing a worker they perceive as disabled. However, the risk associated with such a lawsuit may be significantly less than keeping on an employee who has made a threat of violence.

If such an employee acts on his or her threat, a company would face a lawsuit anyway, one that would undoubtedly be more costly, experts warn. Security, HR, the employee’s supervisors, legal counsel, and others should gather data to make the best decision possible as to whether they can make a reasonable accommodation that will eliminate any significant risk to the health or safety of other employees.

In “direct threat” cases, security teams need to gather as much evidence as possible so they can prove that the risk is significant. According to the Supreme Court, employers need to show that they based their threat assessment on “objectively reasonable” evidence. In other words, a mere belief that an employee may pose a threat is not enough, nor is the word of a single coworker.

**Employee assistance programs (EAPs).** Organizations should employ experts to advise them of the threat potential from individual workers. However, an EAP does not act as a full proof shield from liability in cases of workplace violence. Case in point: Two employers had to pay $8 million to the families of two men killed at an industrial plant in Asheville, N.C., by a fired employee who went on a shooting rampage. The award came despite the fact that a psychologist in the company’s EAP had determined that the individual did not pose a threat. The jury concluded that Union Butterfield and Dormer Tools Inc. should have known the employee was capable of violence and should have taken appropriate precautions in the wake of firing the employee. Crucial evidence included the fact that company management met after the employee’s firing to discuss the situation, including the fact that the worker owned guns and the possibility that he might retaliate violently, but did not take additional security precautions after the EAP psychologist submitted his report (*Allman v. Dormer Tools Inc.*).

**Progressive discipline.** In the wake of a threat made by an employee, a company may face a decision whether to terminate him or her immediately in contradiction to its established progressive discipline procedures. However, courts have repeatedly affirmed the rights of employers to bypass such procedures when other workers’ safety is truly at stake. The U.S. Court of Appeals for the Seventh Circuit noted in a recent ruling that it would be absurd to demand employers follow such procedures in every instance and that an agreement could mean that even if an employee killed a coworker he’d only receive an oral reprimand for a “first offense” under progressive discipline procedures. “Contracts, like statutes, are not read literally when the result would be an absurdity,” the court said.
Members of the public. Companies can face a choice—and potentially a legal battle—when dealing with unruly members of the public. In one case, for example, a hospital refused to allow parents to visit their child because of the couple’s hostile, aggressive, and sometimes violent behavior toward staff. After the child died, the parents sued the hospital for intentional infliction of emotional distress for refusing them entry into the hospital. However, the U.S. Court of Appeals for the Seventh Circuit ruled against the couple and said a hospital could not be held liable for refusing to allow hostile patrons on its premises (Franciski v. University of Chicago Hospitals, U.S. Court of Appeals for the Seventh Circuit, No. 02-4358, 2003).

F. Employee Protection

Bullying

There is no statutory protection for individuals who are bullied in the workplace, notes Eric Matusewitch, former deputy director of the New York City Equal Employment Practices Commission.

Matusewitch observes that federal, state, and local antidiscrimination laws only prohibit harassment and abusive behavior based on an individual’s “protected status”—such as race, religion, sex, age, or disability. Without establishing a connection between bullying behaviors and their protected status, individuals won’t prevail on a harassment claim. Furthermore, typical workplace bullying is generally not perceived as sufficiently extreme to meet the requirements of the tort claim of intentional infliction of emotional distress.

However, while workers outside of a protected class face limited legal recourse in the face of workplace mistreatment, that could change. Workplace bullying could one day be a new area of liability for companies.

Plaintiff’s attorneys are licking their chops at the prospect of opening up this area of liability. And data show that workers also like the idea. In a 2007 survey by the Employment Law Alliance, 64 percent of American workers said an employee who has been abused by a supervisor or employer should have the right to sue that supervisor and the employer to recover damages.

To date, more than a dozen states have introduced proposals for such laws, although none of the so-called “healthy workplace” statutes have yet become law. If one does, “it would represent a fundamental shift in what workplace laws are designed to do,” says Peter Avery, a management attorney at Buchanan Ingersoll & Rooney. He points out that current employment laws don’t regulate general behavior; they prohibit certain behavior against select protected classes. A workplace bullying law, however, would apply to all workers. “So passing a law like this would mean now there’s going to be legislation affecting the way people can behave in the workplace,” he says.

The topic was hotly debated in April 2008 at a meeting of the American Bar Association Employment Rights and Responsibilities Committee. Some argued it could “stop the economy in its tracks.” Others, including management attorney Eric Tate (Morrison & Foerster LLP;
www.mofo.com), say the “free market” should handle the problem of bullying, with companies that tolerate it losing workers and suffering lower productivity due to poor employee morale.

But some argued antibullying laws are necessary, like Maureen Binetti (Wilentz Goldman & Spitzer; www.wilentz.com), who said they would provide recourse for victims who currently fall through the cracks because they are not members of a protected class and because their mistreatment does not fall under other statutes covering assault, false imprisonment, or infliction of emotional distress. And she counters the “free market” suggestion by noting that the victims of workplace bullying suffer as much as employers, yet they can’t recover damages or lost wages. Finally, she suggests that the impact of antibullying laws could be lessened by including an affirmative defense, which would protect employers from lawsuits if they take steps to prevent bullying.

Management attorneys say it is uncertain whether legislation addressing bullying will pass in the near future, but that if it does, it could open a floodgate of employee lawsuits. Matusewitch says he has recently seen things moving in that direction.

Matusewitch points to a substantial verdict against a doctor, upheld by the Indiana Supreme Court, as an indication that the legal line may be on the move. According to the evidence, a surgeon charged at a medical technician with a clenched fist, threatening him. The technician resigned, complained that the incident caused his depression and anxiety and won a $325,000 verdict against the doctor (the hospital was not named in the lawsuit) (Raess v. Doescher, 883 N.E.2d 790, S.C. Ind., April 8, 2008).

The legal debate is sure to continue, and antibullying laws will continue to be introduced—making it clear that companies that begin to address the issue will be positioning themselves ahead of the legal curve. In light of the evolving legal environment, Matusewitch says prudent employers should take the following steps:

1. Issue an antibullying policy statement that defines bullying in common-sense terms and provides examples of unacceptable behavior at work. The policy also should indicate that workplace bullying is a disciplinary offense.

2. Establish a complaint procedure to accompany the policy statement, prohibiting retaliation against those using the procedure.

3. Investigate all complaints of bullying promptly and thoroughly.

4. Conduct employee training to ensure that everyone in the organization understands the policy and their obligation to conduct themselves in a professional and civil manner.

Even absent new laws, it’s still a tricky legal area, according to Michael Fox, an attorney with Ogletree Deakins, in an address at the Society for Human Resource Management’s 2007 conference in Las Vegas. Even though there is no specific federal or state anti-bullying legislation, it doesn’t mean employers can’t be found liable for bullying-type behavior. “Instead of relying on a cause of action custom-made for bullying, plaintiffs utilize harassment related to a protected category, which is a violation of [Title VII of the Civil Rights Act,
the Age Discrimination in Employment Act, or the Americans With Disabilities Act] and the state law counterparts, or utilize common law torts, most often the intentional infliction of emotional distress.” Examples:

- A Kansas psychologist, who was sexually assaulted by a patient, brought a Title VII suit against the mental health center where she was working for failing to take reasonable measures to protect her from a hostile environment created by sexually aggressive patients. The hospital countered that there was no sex-based harassment because male staff also faced abusive behavior from patients, and thus no basis for the lawsuit. But the U.S. Court of Appeals for the Tenth Circuit allowed her lawsuit to proceed, noting that even if conduct affects both sexes, it can constitute sexual harassment if it disproportionately affects female members of the staff.

- A judge recently upheld a $275,000 damage award against GTE Southwest (now Verizon) in a lawsuit won by three employees against the company and a former supervisor. The employees claimed a department supervisor frequently abused them verbally and engaged in bullying activities such as asking an employee to wear a post-it reminder on her shirt so she wouldn’t “forget her paperwork.” The jury found the company liable for permitting the hostile work environment. Workers’ compensation didn’t protect the company from the large monetary award because the injuries were psychological in nature.

**Domestic violence**

No agreement has emerged for how the law can best protect employee victims of domestic violence—whether it’s smarter to model protection on employment law accommodation mandates, such as those provided by the Family and Medical Leave Act or the Americans with Disabilities Act, or the model used in criminal justice, unemployment insurance, and public health, which seeks to spread costs among all employers. But the lack of consensus has hardly slowed down state legislatures from enacting new rules, and the result is a hodgepodge of obligation.

There has been rapid growth in state legislation aimed at protecting and helping employee victims of domestic violence. For example, a Florida law passed in 2008 to help victims of domestic violence exposes employers to liability if they don’t hold their jobs open as required. Florida’s Domestic Violence Leave Law says victims of domestic violence can take up to three unpaid days off from work in any 12-month period to do things like obtain legal help or file an injunction for protection (although employers can require employees first exhaust sick leave and vacation time). Employment law experts recommend that Florida firms update their workplace violence policy or employee handbook to reflect the new law.

A New York City ordinance, enacted in 2004, requires employers to provide “reasonable accommodation” to stalking and domestic abuse victims. The law demands that employers give employees time to pursue legal action against attackers or stalkers and outlines other possible accommodations, such as providing them with a security plan and changing their work location or contact information. The law also prohibits companies from dismissing or rejecting job applicants because of their status as a victim of stalking or abuse. And Maine now requires employers to provide paid or unpaid leave to victims of crime and domestic violence.
IV. LEGAL/REGULATORY CONSIDERATIONS

Additionally, Congress recently held hearings on the issue and has considered several bills that would provide protections such as those being adopted by various states. One bill that has come under consideration would allow all victims to take time off from work without penalty to make court appearances, seek legal assistance, and get help with safety planning, as well as provide unemployment compensation, insurance benefits, and protection from workplace discrimination.

State legislators feel that the traditional avenues for dealing with domestic violence—through criminal and family law—have reached their limits. Consequently, there has been a “migration of domestic violence legislation into employment law, [opening a] dramatic new landscape of legislation [and] an explosion in new laws,” according to a new study. (“Domestic Violence and the Workplace: The Explosion of State Legislation and the Need for a Comprehensive Strategy,” Brooklyn Law School Legal Studies Research, August 2008).

For state legislatures—and perhaps the federal government, in time—moving domestic violence into the realm of employment law represents a new and potentially effective way to make inroads against a stubborn problem. Of course, doing so places the onus on employers, who now must measure whether their workplace violence protections and investigations are adequate.

All the recent laws try to solve the same conundrum: that victims of domestic violence—at a time they rely most on their job’s income for helping them get out of an abusive relationship—often find it difficult to maintain their jobs because of it. So laws have variously mandated that employers avoid employment discrimination against victims, provide job-protected leave to victims, and empower employers to take legal action against perpetrators of domestic violence to protect employees at work.

Some businesses may be purposely turning a blind eye to the problem out of fear that learning about employee victims puts them on the hook if something should happen. A survey of CEOs found several who cited the “legal ramifications of becoming involved” as the primary obstacle to implementing domestic violence prevention (“Corporate Leaders and America’s Workforce on Domestic Violence [CAEPV] CEO and Employee Survey 2007,” Corporate Alliance to End Partner Violence). However, increased protections that states are affording victims of intimate partner violence have altered this equation in favor of being proactive.

Lawsuits. Companies that fail to beef-up security when they’re aware an employee faces a threat from an acquaintance may face civil or criminal penalties if a violent act occurs at work. And the price tag in such cases has been as high as $5 million, notes Susan M. Corcoran, Esq.

Domestic situations can also lead to claims against employers for allowing a hostile work environment. The Supreme Court has ruled that domestic violence can be a form of sexual harassment and it is possible for it to infiltrate the workplace, says Corcoran. She uses the following scenario to illustrate the point: Mary is a victim of domestic violence and, while she is at work, her spouse faxes her letters containing sexually explicit and intimidating language. She tells her boss that these faxes make her uncomfortable and that she doesn’t
know what to do. In such a scenario, the employer has a legal obligation to investigate the employee's concern and determine what, if any, corrective measures it should take to prevent the incident from happening again. Doing nothing leaves a company wide open to a lawsuit, she suggests (“Limiting the Risks of Domestic Violence in the Workplace,” Specialty Technical Publishers).

Additionally, a verdict just handed down by the Washington State Supreme Court shows that a specific domestic violence statute need not exist for an employee victim to win on a wrongful discharge claim. In the case, a worker who was fired after missing work to deal with the fallout from domestic violence successfully proved that there is a mandate to protect those subjected to it inherent in the state of Washington’s expressions of public policy, such as its constitution, its crime victim amendment, and an executive order directing state agencies to provide workplace environments that help victims of domestic violence (Danny v. Laidlaw Transit Services Inc., Wash., No. 78421-3, Oct. 3, 2008).

Solutions. Key to meeting many of the new obligations that states now put on employers is to improve coordination and communication between stakeholders.

- **Between supervisors and the workplace violence prevention team (or the department in charge).** Several jurisdictions have enacted laws making discrimination against victims of domestic violence specifically illegal. So just as new laws forced companies to train supervisors on sexual harassment policies and how to handle incidents, companies must do the same on the topic of domestic violence in affected states (California; New York; New Jersey; Pennsylvania; Oklahoma; New York City; Westchester County, N.Y.; and Illinois).

- **Between supervisors, employees, human resources, and the workplace violence prevention team (or the department in charge).** The Brooklyn Law School research found that several states have enacted a form of “domestic violence leave legislation.” Although they vary in coverage, employee victims are able to take time off work to deal with aspects of domestic violence (e.g., attend a court proceeding or relocate to a safe location) in California, Colorado, Florida, Hawaii, Illinois, Kansas, Maine, New York, North Carolina, Oregon, Washington, and Washington D.C. Additionally, at least 34 states now have laws that protect the jobs of crime victims.

- **Between security, employee victims, supervisors, and human resources.** Illinois and New York City have enacted legislation that requires employers to make reasonable accommodations for employee victims of domestic abuse. The Illinois law specifically identifies that this may mean anything from changing the employee’s telephone number and reassignment to “installation . . . or implementation of a safety procedure in response to actual or threatened domestic or sexual violence.”

- **Between security and employee victims.** Ten states (Arizona, Arkansas, California, Colorado, Georgia, Indiana, Nevada, North Carolina, Rhode Island, and Tennessee) now have laws permitting employers to apply for restraining orders (similar to personal protective orders that domestic violence victims may seek) “against an individual who has harassed, threatened, assaulted, or stalked an employee on the employer’s worksite or while conducting the employer’s business,” according to the report.
The laws generally provide immunity to employers from civil liability for obtaining the order, but the report cautions that the action poses a real risk and security needs to undertake it in consultation with the employee who is the subject of the threat. “The perpetrator of violence will typically understand the order as coming at the individual victim’s behest and may take his anger out on the victim outside the workplace or may respond to such an order by actually attacking the workplace. Thus, a business taking steps to address domestic violence by seeking a protective order without consulting the individual victim may actually increase the danger to the victim and, potentially, to her coworkers.”

- **Between security (or the workplace violence prevention team) and senior management.** As noted earlier, some CEOs see a perverse incentive to remain clueless about domestic violence afflicting workers (out of fear that knowing will raise the company’s liability). However, the rash of new domestic violence laws described above change the math of such an equation, and there is less legal exposure from getting involved than from turning a blind eye, according to the research. It notes that because some businesses are voluntarily taking steps to address domestic violence, it’s a clear sign that employers can do more under existing legal standards. “Indeed, any increased tort risk stemming from taking proactive steps is purely speculative. More likely, as long as an employer could show that it acted reasonably in light of any perceived threat, it still would not be deemed to be liable under a tort framework for third-party violence; in fact, taking appropriate precautions would decrease the likelihood that an employer would be held responsible.”

- **Between the workplace violence prevention team (or department in charge) and employees.** Many employers, such as Verizon, go the extra mile to support employee victims of intimate partner violence. “We have moved an employee from one location in the country to another overnight,” said Verizon’s public affairs manager Debra Lewis. However, there is often a gap between the help companies will provide and employees’ awareness of the help available. For example, the CAEPV survey found that 72 percent of CEOs say their firms offer counseling to their employees, but only 48 percent of those firms’ employees said they knew about the services.

### Parking areas

As noted earlier in the report, parking lots, garages, and structures are frequently sites of assaults on employees. They are also the most common sites of attacks that lead to lawsuits alleging inadequate security.

Studies suggest some common errors leave companies open to lawsuits as the result of violent incidents in parking areas:

- **Failure to evaluate their parking safety plan every year, leading to deficiencies in patrols, use of CCTV, and other failures.**

- **Failure to document their process for repairs, resulting in inoperable CCTV cameras.**

- **Failure to test and verify emergency “call” systems weekly.**
• Failure to provide visible, random patrols.

• Failure to maintain housekeeping that is consistent with the appearance of a safe and secure location.

In addition to following recommended practices identified earlier in this report, there are specific steps companies can take to reduce liability from workplace violence cases that arise from assaults in parking areas:

1. **Benchmark with other parking structures in your area when determining your security strategies.** In the event of an assault and a lawsuit, an organization will need to provide documentation that it considered local crime statistics and the experience of similar structures in the area, as well as the general risks to businesses in its industry.

2. **Document your process for repairs.** A parking garage CCTV camera that is out of service for a couple of days won’t be legally damaging so long as you can show that you follow a timely process of identifying problem cameras and having them repaired.

3. **Have a video strategy to accompany your cameras.** Many experts believe it is the single most important consideration when installing cameras. A “video strategy” defines the purpose that each camera will serve. For example, is it to provide visual evidence? Is it for remote assessment? Using a camera for evidentiary purposes is a legitimate use, but it can help to win a lawsuit later if you define that purpose up front. Otherwise, you will have to defend in court why you had a camera that you weren’t actively monitoring, and the reasoning may look like an excuse in the wake of an assault.

4. **Document patrols.** In the event of a security incident in a parking facility, it is useful to have records indicating that security officers were patrolling the area as necessary. A guard patrol system can help systematically document officer rounds.

---

**A Lesson in Liability From a Parking Lot Assault**

A driver for a trucking company providing services to a FedEx facility in San Diego was assaulted and robbed in the company’s parking lot and filed a premises liability action, in which FedEx won summary judgment. In the appeal, the plaintiff’s attorney contended, among other things, that FedEx was liable under the negligent undertaking doctrine because it didn’t adhere to the security measures it had taken to protect the safety of the parking lot. Failing to do so, the plaintiff’s attorney argued, increased the risk of harm to the contract worker, who had come to rely on those measures for his safety. ([Ericson v. Federal Express Corporation et al.](http://example.com), Court of Appeal, Fourth Appellate District Division One, Calif., Super Ct. No. GIC849702, May 14, 2008.)

At particular issue were FedEx’s written protocols, which called for “perimeter patrols once every hour when two security officers are present for duty and other times as the traffic volume at the gate permits.” The plaintiff’s attorney argued the contract worker reasonably relied on those security patrols—which FedEx had voluntarily undertaken—and suffered an injury as a result.

However, the appeals court flatly rejected that it was a triable issue because there was no evidence that the contract worker had been told the protocol for conducting parking lot patrols (and affirmed summary judgment). It makes the point that when there is no security value from informing invitees of protocols, doing so may only increase a firm’s liability by helping to establish an expectation of security.
Finally, the liability of a company to protect employees from parking area violence may extend further than it thinks. Naturally, companies have a duty to provide “reasonable” measures to protect against parking area crime and to keep the property in good repair, but the courts have shown they can take a broad view of company obligations. For example, an organization’s duty may extend beyond parking facilities over which it has direct control for security. If a company subsidizes employee parking at another facility, it could be held liable if an employee suffers an injury at that facility, according to security consultant Steve Kaufer (Inter/Action Associates, Inc.; interactionassociatesinc.com). Companies should conduct their own security assessment of any parking facility in which they direct employees to park. Even if an organization simply suggests to a new employee where he or she can park for work, security officers should assess the area to make sure it is a place where the employee can park safely.
V. PROGRAM ASSESSMENT

Management will demand to see results from any program it funds—and that will include the workplace violence prevention program. Although protecting employees from violence is clearly the “right thing to do,” management will surely demand concrete signs that its money is being well spent, goals are being met, and progress is being made.

A. Auditing

Workplace violence committees or teams must audit elements of the prevention program and measure compliance with company policies and procedures designed to keep the workplace safe. However, prevention teams must be wary that yearly audits and other examinations of the program aren’t used to rubber-stamp the company’s effort while obscuring problems.

“Compliance is often about developing rules to say you’ve met something you haven’t. Compliance programs provide management with evidence to show that the company is meeting its targets, something it then uses to justify squeezing more out of the system,” notes Dr. John Bircham, director of Bircham-Global Ltd., an international risk and compliance management firm (www.bircham-global.com).

The result is a dangerous downward spiral. As long as a company can show it is complying with its internal policies and procedures or meeting its performance targets, it can demand more from fewer resources. “Soon, shortcuts start to emerge, and the integrity of the entire process is threatened.” Violence prevention teams or personnel need to be careful they are not participating in this type of dangerous misdirection up the chain of command, nor directing it within their own program.

Reviews. A chief responsibility of the workplace violence prevention team is to make the board and senior management aware of their own appetite for risk. The team needs to examine whether the reports they deliver to management create transparency—and thus
accountability—by revealing the true consequences that management’s actions have on the risk of workplace violence, or whether they are simply delivering reports that provide evidence of compliance and continuous improvement. To that end, violence prevention teams need to make sure they themselves are gathering information aimed at seeking truth and not just validation.

It’s the natural tendency of people to provide the answers the questioner wants, and “yes and no” auditing allows it to happen, says Bircham. For example, a workplace violence team might audit the program at a particular business location by asking: “Has your workplace violence plan been reviewed during the last 12 months? Yes or No?” “Has the plan been updated during the last 12 months? Yes or No?”

Such cursory auditing is just a way to be told what you want to hear, Bircham warns. Instead, workplace violence reviews should examine activities by asking open and directed questions, such as: “When was your workplace violence plan last reviewed and what aspects of the plan were updated as a result of the review? Briefly describe the processes used to identify those aspects of the plan that were updated.”

Violence prevention teams need to thoroughly review the internal auditing process for whether it is truly intended to identify gaps in the protection of employees or if it is more directed toward validating the current safety effort.

**Investigations.** Because compliance can be used to actually ignore risk and brush aside shortcomings, examinations of noncompliance—in the form of incident analysis and investigations—are a good hedge against corporate unwillingness to face the truth. Thus, a post-incident analysis to identify lessons learned is a fundamental component of workplace violence prevention.

Investigations of incidents of workplace violence, or inquiries into failures to comply with workplace violence policies, play a critical role in assuring that the company is facing up to its risk. They do so by:

- Providing evidence of how policies are actually being implemented on the ground.
- Providing a source of information on vulnerabilities that exist of which the violence prevention team may not be aware.
- Being a source of meaningful performance metrics. An investigation should identify how the incident unfolded and what failed, and companies can use that knowledge to develop metrics to identify similar weaknesses in the future.

**B. Performance Measurement**

To gauge success and drive improvement, sales departments have sales numbers and production has production numbers, but what numbers should the violence prevention team use? The number of verbal threats and violent acts provides one critical measuring stick, but these figures demonstrate the outcome of the program; they do nothing to indicate whether the program is on the right track to reduce future incidents. While these figures may be the
most important program statistics, they only provide a trailing indication of the program’s effectiveness. To make sure the program is on the right track, violence prevention teams also need to establish leading indicators.

Additionally, for small organizations or businesses where violent acts are rare, a graph in a report to management that depicts, say, “the number of violent acts in Q4” will provide little useful information. In these businesses, a single episode of violence may mark a 100 percent increase, something that imparts no useful information. There are, however, four steps your team can take to effectively track and report performance.

1. **Develop performance metrics.** The workplace violence prevention committee should identify sources of data it can use to derive performance measures, such as security department emergency call reports, security officers’ daily logs and patrol reports, training records, customer satisfaction surveys, and employee perception surveys.

Each source of data can provide several upstream performance indicators. For example, call reports can show how long it took security to respond to a call for assistance and an employee survey can determine how safe workers feel. Examples of performance indicators:

- Percentage of new employees briefed on workplace violence policy within first two weeks of employment.
- Length of time to issue employee identification badges.
- Percentage of security audits conducted on schedule.
- Staff awareness of the workplace violence incident reporting system (as measured through random interviews).
- Percentage of employees complying with corporate badge/identification policy.
- Average wait time for customers.
- Percentage of workplace violence retraining completed on schedule.
- Number of safety/security complaints from employees.

There are myriad performance measures that workplace violence teams can select, and the recommendations and best practices included in this report provide a good source for most of them. Teams should select measurable performance indicators that, if they improve, should ultimately reduce the number of threats or violent acts.

2. **Monitor.** For each performance indicator of the violence prevention program, the committee should develop a performance-monitoring plan. It should detail:

- What types of data it will collect.
- How frequently it will gather results.
- The individual(s) charged with gathering the data (for example, it may ask a guard supervisor to compile and report data on the percentage of parking area patrols completed on time).
• Who will receive the data.
• How frequently it will issue reports and to whom.

3. Threshold-setting. Once a team settles on performance indicators and a performance-monitoring plan, it should establish thresholds based on industry and organizational standards. When a threshold is consistently achieved, the team can raise it in order to demonstrate improvement. For example, many hospitals set an identification badge compliance threshold of 85 percent. If a quarterly audit shows compliance at 80 percent, the hospital may need to embark on an awareness activity to boost compliance. If compliance is always closer to 90 percent, it may choose to establish the higher percentage as a new threshold—and detail the performance improvement in the annual review of the workplace violence program sent to management.

“Customer” satisfaction reports are a critical part of developing a workplace violence program that is driven by continuous improvement. Numbers-only performance indicators do not capture intangibles relative to violence prevention. For example, a team can measure the percentage of new employees that receive workplace violence awareness training in the first month of employment, but unless it receives feedback that the quality of that training is sufficient, the company may be meeting goals that give a false impression of performance.

4. Develop a performance-reporting plan. The workplace violence committee doesn’t need to report on every indicator to everyone—especially not to senior management. Senior management will still focus on the broad progress of the workplace violence program. The annual or quarterly report for senior managers may be limited to:

• Frequency comparison reports that compare workplace violence data showing the percentage of increase or decrease in the frequency rate of occurrence.
• Incident classification reports that list the number of incidents (including total loss and amount recovered) broken down by category, severity, and type.

On a monthly and quarterly basis, however, the workplace violence committee should use the performance indicators to decide where it needs to focus improvement activities, such as more timely training, raising workplace violence awareness for the night shift, or promoting awareness of the security department’s car escort program. The goal is to make improvements in the leading indicators so that when the final incident data are shared with management they will like what they see.

C. Return-on-Investment

The first step in appropriately allocating resources and measuring a return-on-investment is to track costs, but most private companies fail to calculate basic costs associated with workplace violence, according to a study by the Bureau of Labor Statistics in 2006.

Large companies—those with 1,000 or more employees—are the most likely to keep track of workplace violence costs. Yet 76 percent do not track absenteeism costs related to workplace
V. PROGRAM ASSESSMENT

To demonstrate the value of violence prevention, management needs to be made aware of the costs of workplace violence. These include both direct and indirect expenses:

- **Legal bills from negligent hiring, supervision, and retention lawsuits; claims of inadequate security; and failure-to-notify torts.**

- **Indirect costs from lower productivity, wasted time, increased absenteeism, management distraction, and increases in turnover and stress.**

- **Workers’ compensation and medical claims.**

A simple cost comparison model—between the cost of the violence prevention program and the cost of an incident—can help put the situation in perspective for management, according to Dr. James Madero, president of Violence Prevention International. See Figure 43.
Figure 43. Comparing the Cost of Violence Versus Prevention

<table>
<thead>
<tr>
<th>Homicide</th>
<th>Ongoing Harassment</th>
<th>Workplace Violence Prevention (WVP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual event: Two managers murdered</td>
<td>Hypothetical event: Six months</td>
<td>Sample company—Union Butterfield, 500 employees</td>
</tr>
<tr>
<td>by a disgruntled fired employee</td>
<td>of ongoing harassment of one manager</td>
<td></td>
</tr>
<tr>
<td>Lawsuit: Allan vs. Union Dormer Tools</td>
<td>Lost wages due to manager’s two days</td>
<td>Threat reported to Butterfield/</td>
</tr>
<tr>
<td>(May 1999)</td>
<td>of absenteeism per month ($3,600)</td>
<td>workplace violence prevention</td>
</tr>
<tr>
<td>Warning signs: Threats made to “take</td>
<td>Loss of productivity of 10 minutes per day in manager’s</td>
<td>Early intervention resolves threat</td>
</tr>
<tr>
<td>management with me”</td>
<td>department of 10 employees ($5,000)</td>
<td></td>
</tr>
<tr>
<td>Verdict: Jury award of $7.9 million</td>
<td>Loss of major contract due to poorly prepared proposal</td>
<td>Ongoing annual cost of WVP program: $14,000</td>
</tr>
<tr>
<td></td>
<td>($30,000)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stress related to poor performance of manager leads to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>his dismissal ($20,000 severance; $100,000 to hire/train</td>
<td></td>
</tr>
<tr>
<td></td>
<td>replacement)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total cost: $158,600</td>
<td></td>
</tr>
</tbody>
</table>

Average of out-of-court settlement in workplace homicide case: $500,000
Average jury verdict: $3 million
Total estimated annual losses to American businesses from workplace violence for legal costs, jury verdicts, court settlements, and productivity losses: $4 billion to $36 billion

Tracking costs

To calculate costs associated with workplace violence, demonstrate progress in reducing incidents, and figure money saved, companies need to capture all incidents—no matter how small—in a central database.

In addition to helping aim solutions at the problem, companies that collect workplace violence data possess the surest method for convincing management that money put toward violence prevention is money well spent, according to Madero. “The greater the number of small incidents that a company has, the more likely it is to have a serious incident of workplace violence,” he says. This is logic that management can easily understand, and it is why—just as companies should capture every accident near-miss—companies must capture every incident, including arguments, threats, bullying, intimidation, outbursts, and domestic violence issues. Such data collection provides evidence that the workplace violence prevention program is helping to minimize the threat of a major incident capable of disrupting production and harming an organization’s brand and value.
V. PROGRAM ASSESSMENT

In addition to tracking hard financial costs associated with incidents, the workplace violence team should educate management on the costs associated with “minor” incidents. Safety professionals are used to the concept of the “soft costs” associated with workplace accidents. Workplace violence is similar. Companies can suffer financially from workplace violence even without a tragic fatality. Threats, harassment, bullying, and stress are expensive, too. “If you have two people quit because of a negative work environment, the replacement costs are more than the cost of a comprehensive violence prevention program,” notes Madero.

Many factors may need to be included in the accounting when examining the price paid for workplace violence:

- Cost for subsequent increases in security.
- Building repair and cleanup.
- Business interruptions with customers.
- Loss of productivity.
- Lost work time.
- Turnover of employees and associated recruitment, hiring, and training costs.
- Increase in absenteeism of both the employee who is the victim of a violent act and other employees.
- Salary continuation for those who are injured or traumatized.
- Valued employees with institutional knowledge quitting or retiring early.
- Increase in insurance premiums.
- Cost of attorney fees, medical care, and psychological care for current employees.
- Lost opportunities or sales.
- Harm to employee-recruiting efforts.
- Harm to the organization’s reputation and/or stock price/profitability.

**Spending $9.27 Per Nurse Can Prevent Assaults, Study Shows**

According to data presented at an OSHA conference on reducing workplace violence at psychiatric facilities, researchers at the University of Minnesota’s School of Public Health estimated that employers could prevent serious injuries from workplace assaults by spending just $11 per employee annually on interventions ranging from architectural changes to staffing strategies.

They based the per-employee prevention costs on a formula that examined the number of workplace injuries to healthcare workers in Minnesota, the cost of injuries, and the average cost per injury claim where assaults were the cause ($14,479). Their conclusion: Preventing serious injuries from workplace assaults would cost $9.27 per registered nurse; $16.91 for each licensed practical nurse; $36.19 per nurse’s aide; and $100.42 per health aide.

“The way a person could use that [formula] is a kind of a back-of-the-envelope benchmark. It’s to say, ‘If we want to end these serious, non-fatal assaults, if we want to eliminate them,’ it would not be inappropriate to target that amount per person in that industry,” said the study’s principal researcher, Patricia McGovern, an associate professor of environmental and occupational health at the University of Minnesota’s School of Public Health.
Once management understands that the costs of workplace violence go beyond assaults and fatalities, it will be less likely to pull the plug on programs after they’ve directed improvements, according Richard Lefler, vice president of worldwide security for American Express. He says he’s seen instances where effective corporate programs have been cut because they reduce major incidents to the point that senior management starts to question if the program is still necessary. If companies only track major incidents, management may see only the cost of programs—not the benefit.

If leaders of the violence prevention effort find themselves working in an environment where violence prevention is not a management priority, they should seek partners—among human resources and legal counsel—to bolster their case. If violence prevention advocates can convince legal to sign-on to their call for additional resources, they are on their way to getting them, suggests Madero. Lefler said that partnering was the key to success for his program. He worked closely with business management at each office location, and these managers became extremely supportive of the program because it prevented disruptions and enhanced their ability to deliver on their performance goals. Once business managers are on board, funding for the program is secure.

Injuries. Cost of crime-related workers’ compensation claims are more than 60 percent higher on average than for noncriminal-related claims. Medical costs associated with crime-related claims are 36 percent higher, and indemnity costs are 48 percent higher than for claims with other causes. The only type of workers’ compensation claims that costs more on average are those involving motor vehicles, according to data from the National Council on Compensation Insurance, Inc.

Workplace injuries from violence also put workers out of commission longer. Oregon, which has been particularly aggressive in tracking hard costs associated with violence-related claims, discovered that its average violence-related claim results in 69 lost days; significantly higher than for other claims.

Bullying. If you have an employee who is a victim of domestic violence, it is almost certainly hurting his or her productivity. According to a growing body of social science research, it is extremely common for perpetrators of domestic violence to purposefully interfere with victims’ ability to work by harassing them at work, limiting their access to cash or transportation, or sabotaging their child care arrangements.

Government studies indicate that between 35 percent and 56 percent of employed battered women were harassed while at work by the abuser, and batterers can be extremely creative and dogged in their efforts to disrupt victims’ employment, including calling in false reports of drug use or stealing. On average, research
indicates that a victim of domestic violence loses 137 work hours per year (almost four weeks).

Workers who witness it also suggest the fallout is significant. Zogby International polled 8,000 workers and a majority said the victims of bullying they’ve seen have suffered stress-related health complications. Witnesses also said that 40 percent of bullying victims quit their jobs. “That represents the preventable loss of 21.6 million workers,” the Workplace Bullying Institute (WBI) noted in its analysis of the results.

Bullying—or the associated “desk rage”—has been shown to cause psychological and physical trauma to workers, according to mental health experts. They’ve discovered that an oppressive work atmosphere causes depression, anxiety, and even illness through the suppression of the immune system. All of these consequences can have a substantial impact on bottom-line company productivity.

Additionally, a research study of 700 workplace bullying victims found that they are more likely to consume drugs at work. It found that 20 percent of bullying victims take drugs because of job problems, compared with 4 percent of other employees (“Psychosocial Factors at the Workplace—Do They Affect Substance Use? Evidence From the Tyrolean Workplace Study,” Pharmacoepidemiology and Drug Safety, 2004).

All told, workplace bullying is a significant drain on the corporate bottom line, more so than many other employee-related issues. A report by the Conference Board Inc. (www.conference-board.org) released cost estimates from interest groups, consultants, and government agencies that put dollar figures on the annual cost to businesses for different workplace

---

**Aggression as Harmful as Sexual Harassment**

In March 2008, at the Seventh International Conference on Work, Stress, and Health in Washington, D.C., researchers from Queen’s University in Ontario revealed results from their review of 110 scientific studies on the consequences of workplace aggression and sexual harassment. The researchers examined workers’ health; level of stress, anger, and anxiety; and job turnover, satisfaction, and commitment. Their surprising conclusion: Workplace aggression has more severe consequences than sexual harassment. Especially noteworthy is that victims of bullying are less committed to their job and are more likely to quit, thereby causing employers to incur the substantial cost of filling job vacancies.
issues. The group said consensus estimates put the cost of workplace bullying at $400 billion annually, the same as employee fraud, three times as much as employee alcohol abuse, and nearly four times as much as ergonomic disorders.

**Conflict.** Companies can use the workplace violence prevention program to reduce organizational conflict—and demonstrate cost savings from doing so. “Unmanaged employee conflict is perhaps the largest reducible cost in organizations today,” according to Daniel Dana, Ph.D., Mediation Training Institute International (www.mediationworks.com). Dana estimates that a full 65 percent of performance problems result from strained relationships between employees—not from deficits in individual employees’ skill or motivation.

By measuring the financial costs of a single organizational conflict, companies may be able to cost-justify interventions and training for supervisors on managing organizational conflict. Not only will the risk of conflict festering into an act of violence wane, but productivity will increase. For an example, see Appendix Q, “Conflict Accounting Tool.” It shows how a single unresolved conflict can result in a large bottom-line loss.

**Residual benefits.** Interventions that successfully reduce the risk of workplace violence are bound to have other benefits—from reducing monetary loss from robberies, to improvements in employee retention rates to reducing healthcare costs. Workplace violence teams should keep track of successes, their ROI, and residual benefits to keep funding strong for the violence prevention effort.

For example, many of the security measures that can reduce the likelihood of violence—adding patrols, increasing visibility of security, training employees to be on the lookout for suspicious individuals—are the same ones that can reduce the likelihood of a successful terrorist attack—something that many businesses find hard to fund because of the small likelihood of an event.
VI. APPENDICES

A. Glossary of Workplace Violence Terms

For an organization to effectively fight workplace violence it needs to identify specific procedures for staff to follow to report an incident. To that end, it needs to instruct employees on what exactly constitutes a reportable incident. A glossary of terms as an adjunct to the workplace violence prevention policy can help get all employees and management on the same page. Definitions of various forms of workplace violence:

- Bullying: repeated intimidation, slandering, social isolation, or humiliation by one or more persons against another.
- Coercion: to force to think or act in a certain manner by use of pressure, threats, or intimidation; to dominate, restrain, or control forcibly.
- Degradation: to reduce in status, dishonor, disgrace, or debase.
- Disrespect: lack of respect or courteous regard.
- Harassment: systematic persecution by repeated annoyances, threats of demands, unrelenting pursuit to gain a desired end, to nag or tease, taunt or ridicule persistently. Interfering with fellow employees on agency premises or creating discord or lack of harmony in the work environment.
- Humiliation: to lower the pride or dignity.
- Insubordination: defiance or opposition to established authority.
- Intimidation: to make timid, frighten.
- Manipulation: to influence deviously, to falsify for personal gain.
• Physical harassment: assault, impeding or blocking movement or any physical interference with normal work or movement when directed at an individual.

• Stalking: to pursue a prey, e.g., following, unwanted phone calls, communications, e-mails.

• Verbal harassment: name calling, derogatory comments or slurs based on sex, race, ethnicity, religion, sexual orientation.

• Visual harassment: displaying derogatory posters, cartoons, or drawings that are offensive.

Other forms of workplace violence include:

• Use of abusive or threatening language toward another employee, a supervisor, or any other person on agency premises.

• Conduct that unreasonably interferes with an employee’s performance of his or her job or that creates an intimidating, hostile, or offensive work environment.

• Inducing another employee to violate agency policy.

• Insubordination or uncooperative conduct, including refusing to follow a supervisor’s or manager’s requests, instructions, or orders.

(Source: The State of Connecticut Department of Veterans Affairs)
B. Model Policy Statement

It is the policy of XYZ Company that each of our employees has the right to a workplace free from violence. Furthermore, every employee has the right to seek assistance through the EAP to deal with any issues of violence, wherever they happen, including outside of the workplace. For purposes of this policy, violence is defined as any act in which one person seeks to hurt or intimidate another through the use of physical contact or verbal harassment or manipulation. This includes actions of employees, supervisors, customers, suppliers, or any other person.

XYZ Company shall:

• Seek to eliminate the potential for violence in and around the workplace.

• Seek to eliminate the potential for violence by affecting the attitudes and behavior of our customers and suppliers.

We will use a variety of methods to accomplish the above, including:

1. We will disseminate to all employees/supervisors/managers a statement against all acts of violence, including family violence. This statement will be posted in prominent locations accessible to customers and suppliers.

2. Our opposition to all forms of sexual harassment will be made clear by disseminating to all employees/supervisors/managers our policy prohibiting sexual harassment. Copies of the policy, informational posters, or other media will be prominently displayed in areas accessible to our customers and suppliers.

3. We will provide information to all employees about services available through our EAP, including those designed to help employees deal with any issues related to workplace or family violence.

4. We will regularly review our workplace environment and minimize wherever possible physical attributes which may expose our employees, customers, or suppliers to violent acts.

5. Employees with questions or complaints about workplace behaviors that fall under this policy may discuss them with ________________. Concerns will be investigated, and appropriate action will be taken. This may include disciplinary action for an employee who is a perpetrator of a violent act.

Everyone with whom we come into contact in our work deserves to be treated with courtesy and respect. This means that we treat each other, our customers, our suppliers, and all others in this fashion and that we can expect the same treatment in return.

(Source: Minnesota Department of Labor and Industry)
C. Model Weapons Policy

Policy statement

In order to ensure a safe environment for employees and customers, our establishment, XYZ Company, prohibits the wearing, transporting, storage, or presence of firearms or other dangerous weapons in our facilities or on our property. Any employee in possession of a firearm or other weapon while on our facilities/property or while otherwise fulfilling job responsibilities may face disciplinary action, including termination. A client or visitor who violates this policy may be removed from the property and reported to the authorities. Possession of a valid concealed weapons permit authorized by the state is not an exemption under this policy.

Definition

Firearms or other dangerous weapons means:

- any device from which a projectile may be fired by an explosive
- any simulated firearm operated by gas or compressed air
- sling shot
- sand club
- metal knuckles
- any spring blade knife
- any knife which opens or is ejected open by an outward, downward thrust or movement
- any instrument that can be used as a club and poses a reasonable risk of injury

Exemptions

This policy does not apply to:

- any law enforcement personnel engaged in official duties
- any security personnel engaged in official duties
- any person engaged in military activities sponsored by the federal or state government, while engaged in official duties

Notification

“No Firearms or other Dangerous Weapons” signs shall be conspicuously posted within all XYZ Company facilities and in parking areas and grounds surrounding our facilities. These signs will clearly indicate that firearms and other weapons are not to be carried onto our property or into our facilities.
VI. APPENDICES

Reporting

Staff or security personnel will request any visitor found in possession of a firearm or other dangerous weapon to remove it from the facility, and local law enforcement authorities will be notified promptly.

Special instructions for employees

Any employee concerned about personal safety may request an escort (e.g., to a parking lot off premises) or other appropriate intervention by security personnel. Educational materials will be made available on request regarding the magnitude of the workplace violence problem in the United States and the role of firearms and other dangerous weapons in this violence. Training will be provided to employees on this and other workplace violence prevention measures that XYZ Company has implemented.

(Source: Minnesota Department of Labor and Industry)
D. Sample Violence Prevention Program Report

A Workplace Violence Prevention Team will be established and part of their duties will be to assess the vulnerability to workplace violence at our establishment and reach agreement on preventive actions to be taken. They will be responsible for auditing our overall Workplace Violence Program.

The Workplace Violence Prevention Team will consist of:

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Smith</td>
<td>Vice President</td>
<td>555-1212</td>
</tr>
<tr>
<td>Jane Doe</td>
<td>Operations</td>
<td>555-1234</td>
</tr>
<tr>
<td>Frank Jones</td>
<td>Shop Steward</td>
<td>555-1233</td>
</tr>
<tr>
<td>James Brown</td>
<td>Security</td>
<td>555-1456</td>
</tr>
<tr>
<td>Susan Dean</td>
<td>Treasurer</td>
<td>555-1567</td>
</tr>
<tr>
<td>Tom Jones</td>
<td>Treasurer</td>
<td>555-1678</td>
</tr>
<tr>
<td>Sally Field</td>
<td>Personnel</td>
<td>555-1789</td>
</tr>
</tbody>
</table>

The Team will develop employee training programs in violence prevention and plan for responding to acts of violence. They will communicate this plan internally to all employees.

The Team will begin their work by reviewing previous incidents of violence at our workplace. They will analyze and review existing records identifying patterns that may indicate causes and severity of assault incidents and identify changes necessary to correct these hazards. These records include but are not limited to, OSHA 200 logs, past incident reports, medical records, insurance records, workers’ compensation records, police reports, accident investigations, training records, grievances, minutes of meetings, etc. The Team will communicate with similar local businesses and trade associates concerning their experiences with workplace violence.

Additionally, they will inspect the workplace and evaluate the work tasks of all employees to determine the presence of hazards, conditions, operations and other situations which might place our workers at risk of occupational assault incidents. Employees will be surveyed to identify the potential for violent incidents and to identify or confirm the need for improved security measures. These surveys shall be reviewed, updated and distributed as needed or at least once within a two year period.

Periodic inspections to identify and evaluate workplace security hazards and threats of workplace violence will be performed by the following representatives of the Workplace Violence Prevention Team, in the following areas of our workplace:

- **Representative: John Smith**  **Area: General Office**
- **Representative: Frank Jones**  **Area: Shop and Lab**
- **Representative: Jane Doe**  **Area: Reception & Sales**

Periodic inspections will be performed according to the following schedule: *First Monday of every month.*
VI. APPENDICES

Risk/Hazard Assessment

On January 1, 2008 the Team completed the risk/hazard assessment. This consisted of a records review, inspection of the worksite, and employee survey.

1. Records Review. The Team reviewed the following records:

   - OSHA 200 logs for the last three years
   - Incident reports
   - Records of or information compiled for recording of assault incidents or near assault incidents
   - Insurance records
   - Police reports
   - Accident investigations
   - Training records
   - Grievances
   - Other relevant records or information: Workers’ compensation records

From these records, we have identified the following issues that need to be addressed:

- Employees have been assaulted by irate clients.
- Employees have been assaulted while traveling alone.
- There have been several incidents of assault and harassment among employees.

2. Review of Tasks. The Team also reviewed the work tasks of our employees to determine the presence of hazards, conditions, operations and situations that might place workers at risk of occupational assault incidents. The following factors were considered:

   - Exchange of money with the public.
   - Working alone or in small numbers.
   - Working late at night or early in the morning hours.
   - Working in a high crime area.
   - Guarding valuable property or possessions.
   - Working in community settings.
   - Staffing levels.

From this analysis, the following issues have been identified:

- Employees in client service area exchange money with clients.
• There are several employees who work very late hours or come in very early in the morning in the shop and lab areas.

Security Analysis

The Team inspected the workplace on January 15, 2008.

From this inspection the following issues have been identified:

• Access to the building is not controlled, and it is not limited to any of the offices on the four floors that we occupy. There have been problems with non-employees entering private work areas.

• Doors to the restrooms are not kept locked.

• Lighting in the parking lot is inadequate.

• In client service area, desks are situated in a way that makes it necessary for employees to walk past the client in order to leave area. There are many objects on top of desks that could be used as weapons (e.g., scissors, stapler, file rack, etc.).

Workplace Survey

Under the direction of the Workplace Violence Prevention Team, we distributed a survey among all of our employees to identify any additional issues that were not noted in the initial stages of the hazard assessment.

From that survey, the following issues have been identified:

• Employees who work in the field have experienced threats of violence on several occasions, and there have been several near-miss incidents. Employees noted that they were unsure of how to handle the situation and that they are often afraid to travel by themselves to areas they perceive are dangerous.

• Employees who work directly with clients in the office have also experienced threats, both verbal and physical, from some of the clients.

Workplace Hazard Control and Prevention

In order to reduce the risk of workplace violence, the following measures have been recommended:

Engineering Controls and Building and Work Area Design

• Employees who have client contact in the facility will have their work areas designed to ensure that they are protected from possible threats from their clients

Changes to be completed by June 1, 2008 include:

• Arranging desks and chairs to prevent entrapment of the employees.

• Removing items from the top of desks, such as scissors, staplers, etc., that can be used
as a weapon. Installing panic buttons to assist employees when they are threatened by clients. The buttons can be activated by one’s foot. The signal will be transmitted to a supervisor’s desk, as well as the security desk, which is always staffed.

Management has instituted the following as a result of the workplace security inspection and recommendations made by the Workplace Violence Prevention Team:

- Installation of Plexiglas payment window for employees who handle money and need to take payments from clients (number of employees who take money will be strictly limited).
- Adequate lighting systems installed for indoor building areas as well as areas around the outside of the facility and in the parking areas. The lighting systems will be maintained on a regular basis to ensure safety to all employees.
- Locks installed on restroom doors; keys will be given to each department. Restroom doors are to be kept locked at all times. Supervisors will ensure that the keys are returned to ensure continued security for employees in their areas.
- Installation of panic buttons in employees’ work areas.
- Memorandum to all employees requesting that they remove any items from their desks that can be used as a weapon, such as scissors, staplers, etc.

These changes were completed by January 1, 2008.

Policies and Procedures developed as a result of the Workplace Violence Prevention Team recommendations:

- Employees who are required to work in the field and who feel that the situation is unsafe should travel in “buddy” systems or with an escort from their supervisor.
- Employees who work in the field will report to their supervisor periodically throughout the day. They will be provided with a personal beeper or cellular phone, which will allow them to contact assistance should an incident occur.
- Access to the building will be controlled. All employees have been given a name badge that is to be worn at all times. If employees come in early, or are working past 7:30 p.m., they must enter and exit through the main entrance.
- Visitors will be required to sign in at the front desk. All clients must enter through the main entrance to gain access.

Training and Education

Training for all employees, including managers and supervisors, was given on May 1, 2008. This training will be repeated every two years.

1. Training included:

- A review and definition of workplace violence.
- A full explanation and full description of our program (all employees were given a
copy of this program at orientation).

- Instructions on how to report all incidents, including threats and verbal abuse; methods of recognizing and responding to workplace security hazards.

- Training on how to identify potential workplace security hazards (such as no lights in parking lot while leaving late at night, unknown person loitering outside the building, etc.).

- Review of measures that have been instituted in this organization to prevent workplace violence, including: use of security equipment and procedures; how to attempt to diffuse hostile or threatening situations; how to summon assistance in case of an emergency or hostage situation; post-incident procedures, including medical follow-up and the availability of counseling and referral.

1. Additional specialized training was given to:

- Employees who work in the field.

- Employees who handle money with clients.

- Employees who work after hours or come in early.

Specialized training included: Personal safety; importance of the buddy system; recognizing unsafe situations and how to handle them during off-hours.

This training was conducted by in-house staff, with assistance from the local police department on Oct. 1, 1995 and will be repeated every two years.

Trainers were qualified and knowledgeable. Our trainers are professionals certified by ASIS International.

At the end of each training session, employees are asked to evaluate the session and make suggestions on how to improve the training.

All training records are filed with the Human Resource Department/Personnel Department.

Workplace Violence Prevention training will be given to new employees as part of their orientation.

A general review of this program will be conducted every two years. Our training program will be updated to reflect changes in our Workplace Prevention Program.

**Incident Reporting and Investigation**

All incidents must be reported within Four (4) hours. An “Incident Report Form” will be completed for all incidents. One copy will be forwarded to the Workplace Violence Prevention Team for their review and a copy will be filed with the Human Resource/Personnel Department.

Each incident will be evaluated by the Workplace Violence Prevention Team. The Team will discuss the causes of the incident and will make recommendations on how to revise the program to prevent similar incidents from occurring. All revisions of the Program will be put
into writing and made available to all employees.

**Recordkeeping**

We will maintain an accurate record of all workplace violence incidents. All incident report forms will be kept for a minimum of seven (7) years, or for the time specified in the Statute of Limitations for our local jurisdiction.

Any injury which requires more than first aid, is a lost-time injury, requires modified duty, or causes loss of consciousness will be recorded on the OSHA 200 log. Doctors’ reports and supervisors’ reports will be kept of each recorded incident, if applicable.

Incidents of abuse, verbal attack, or aggressive behavior, which may be threatening to the employee but do not result in injury, will be recorded. These records will be evaluated on a regular basis by the Workplace Violence Prevention Team.

Minutes of the Workplace Violence Prevention Team meetings shall be kept for three (3) years.

Records of training program contents, and the sign-in sheets of all attendees, shall be kept for five (5) years. Qualifications of the trainers shall be maintained along with the training records.

(Source: OSHA/Long Island Coalition for Workplace Violence Awareness and Prevention/other sources)
E. Sample Employee Workplace Violence Survey

NAME: ____________________________________________________________

WORK LOCATION: __________________________________________________

(IN BUILDING OR ALTERNATE WORKSITE)

1. Do either of these two conditions exist in your building or at your alternate work site?
   ___ Work alone during working hours.
   ___ No notification given to anyone when you finish work.

2. Are these conditions a problem? If so, please describe (for example, Mondays, evening, daylight savings time):
   ______________________________________________________________________

3. Does your workplace have a written policy to follow for addressing general problems?
   ______________________________________________________________________

4. Does your workplace have a written policy on (check all that apply):
   ___ How to handle a violent client?
   ___ When and how to request the assistance of a coworker?
   ___ When and how to request the assistance of police?
   ___ What to do about a verbal threat?
   ___ What to do about a threat of violence?
   ___ What to do about harassment?
   ___ Working alone?

5. Does your workplace have: (check all that apply)
   ___ Alarm system(s)?
   ___ Security in and out of building?
   ___ Security in parking lot?

6. Have you been assaulted by a coworker? _________

7. To your knowledge have incidents of violence ever occurred among your coworkers? _________

8. Are violence-related incidents worse during shift work, on the road, or in other situations? Please specify:
   ______________________________________________________________________
VI. APPENDICES

9. Where in the building or worksite would a violence-related incident most likely occur?
   ___ lounge
   ___ exits
   ___ deliveries
   ___ private offices
   ___ parking lot
   ___ bathroom
   ___ entrance
   ___ other (specify)

10. Have you ever noticed a situation that could lead to a violent incident? __________

11. Have you missed work because of a potential violent act(s) committed during your course of employment?
    __________

12. Do you receive workplace violence-related training or assistance of any kind?
    __________

13. Has anything happened recently at your worksite that could have led to violence?
    __________

   If so, can you comment about the situation? ________________________________

14. Has the number of violent clients increased?
    ______________________________________________________________________

(Source: OSHA/Long Island Coalition for Workplace Violence Awareness and Prevention)
F. Workplace Violence Inspection Checklist

Staffing

Is there someone responsible for building security?

- Yes  - No  - Sometimes  Notes: _________________________________

Who is it? _______________________________

Are workers told who is responsible for security?

- Yes  - No  - Sometimes  Notes: _________________________________

Is adequate and trained staffing available to protect workers against assaults or other violence?

- Yes  - No  - Sometimes  Notes: _________________________________

Is there a “buddy system” to use when workers are in potentially dangerous situations?

- Yes  - No  - Sometimes  Notes: _________________________________

Are there trained security personnel accessible to workers in a timely manner?

- Yes  - No  - Sometimes  Notes: _________________________________

Do security personnel have sufficient authority to take all necessary action to ensure worker safety?

- Yes  - No  - Sometimes  Notes: _________________________________

Are security personnel provided outside the building?

- Yes  - No  - Sometimes  Notes: _________________________________

Is the parking lot attended or otherwise secure?

- Yes  - No  - Sometimes  Notes: _________________________________

Are security escorts available to walk workers to and from the parking lot?

- Yes  - No  - Sometimes  Notes: _________________________________

Training

Are workers trained in the emergency response plan (for example, escape routes, notifying the proper authorities)?

- Yes  - No  - Sometimes  Notes: _________________________________

Are workers trained to report violent incidents or threats?

- Yes  - No  - Sometimes  Notes: _________________________________
VI. APPENDICES

Are workers trained in how to handle difficult customers?
☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Are workers trained in ways to prevent or defuse potentially violent situations?
☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Are workers trained in personal safety and self-defense?
☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Facility Design

Are there enough exits and adequate routes of escape?
☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Can exit doors be opened only from the inside to prevent unauthorized entry?
☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Is the lighting adequate to see clearly in indoor areas?
☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Are there worker-only work areas that are separate from public areas?
☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Is a secure place available for workers to store their personal belongings?
☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Are private, locked restrooms available for staff?
☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Security Measures

Does the workplace have:

Physical barriers (Plexiglas partitions, elevated counters to prevent people from jumping over them, bulletproof customer windows, etc.)?
☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Security cameras or closed-circuit TV in high risk areas?
☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Panic buttons (portable or fixed)?
☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________
Alarm systems?
- Yes
- No
- Sometimes

Internal phone system to activate emergency assistance?
- Yes
- No
- Sometimes

Phones with an outside line programmed to call 911?
- Yes
- No
- Sometimes

Two-way radios, pagers or cellular phones?
- Yes
- No
- Sometimes

Security mirrors (convex mirrors)?
- Yes
- No
- Sometimes

Secured entry (buzzers)?
- Yes
- No
- Sometimes

Personal alarm devices?
- Yes
- No
- Sometimes

Outside the Facility

Do workers feel safe walking to and from the workplace?
- Yes
- No
- Sometimes

Are the entrances to the building clearly visible from the street?
- Yes
- No
- Sometimes

Is the area surrounding the building free of bushes or other hiding places?
- Yes
- No
- Sometimes

Is video surveillance provided outside the building?
- Yes
- No
- Sometimes

Is there enough lighting to see clearly outside the building?
- Yes
- No
- Sometimes

Are all exterior walkways visible to security personnel?
- Yes
- No
- Sometimes

Is there a nearby parking lot reserved for workers only?
- Yes
- No
- Sometimes
VI. APPENDICES

Is the parking lot free of bushes or other hiding places?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________

Is there enough lighting to see clearly in the parking lot and when walking to the building?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________

Have neighboring facilities and businesses experienced violence or crime?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________

Workplace Procedures

Is public access to the building controlled?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________

Are floor plans posted showing building entrances, exits?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________

Are these floor plans visible only to staff and not to outsiders?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________

Is other emergency information posted, such as telephone numbers?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________

Are special security measures taken to protect people who work late at night (escorts, locked entrances, etc.)?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________

Are authorized visitors to the building required to wear ID badges?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________

Are identification tags required for staff (omitting personal information such as the person’s last name and Social Security number)?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________

Are workers notified of past violent activity?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________

Is there an established liaison with local police?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________

Are broken windows and locks repaired promptly?
- Yes  ❏ No  ❏ Sometimes  ❏ Notes: _________________________________
Are security devices (locks, cameras, alarms, etc.) tested on a regular basis and repaired promptly when necessary?

☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Field Work

Staffing:

Is there adequate staffing in the establishment?

☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Are escorts or “buddies” provided for people who work in potentially dangerous situations?

☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Training:

Are workers briefed about the area in which they will be working (gang colors, neighborhood culture, language, drug activity, etc.)?

☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Are workers who work late at night or early mornings advised about special precautions to take?

☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Work Environment:

Is there enough lighting to see clearly in all areas where workers must go?

☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Are there safe places for workers to eat, use the restroom, store valuables, etc.?

☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Are there places where workers can go for protection in an emergency?

☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Is safe parking readily available for workers?

☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________

Security Measures:

Are workers provided two-way radios, pagers, or cellular phones?

☐ Yes  ☐ No  ☐ Sometimes  Notes: _________________________________
VI. APPENDICES

Are workers provided with personal alarm devices or portable panic buttons?
☑ Yes ☐ No ☐ Sometimes Notes: _________________________________

Are vehicle door and window locks controlled by the driver?
☑ Yes ☐ No ☐ Sometimes Notes: _________________________________

Are vehicles equipped with physical barriers (Plexiglas partitions, etc.)?
☑ Yes ☐ No ☐ Sometimes Notes: _________________________________

Work Procedures:

Are workers given maps and good directions covering the areas where they will be working?
☑ Yes ☐ No ☐ Sometimes Notes: _________________________________

Are workers given alternative routes to use in neighborhoods with a high crime rate?
☑ Yes ☐ No ☐ Sometimes Notes: _________________________________

Does a policy exist to allow workers to refuse service to unruly customers?
☑ Yes ☐ No ☐ Sometimes Notes: _________________________________

Has a liaison with the police been established?
☑ Yes ☐ No ☐ Sometimes Notes: _________________________________

Do workers avoid carrying unnecessary items, which someone could use as a weapon against them?
☑ Yes ☐ No ☐ Sometimes Notes: _________________________________

Is a safe vehicle or other transportation provided by the employer for use when conducting company business?
☑ Yes ☐ No ☐ Sometimes Notes: _________________________________

Are vehicles used in the field routinely inspected and kept in good working order?
☑ Yes ☐ No ☐ Sometimes Notes: _________________________________

Is there always someone who knows where each worker is while traveling during business hours?
☑ Yes ☐ No ☐ Sometimes Notes: _________________________________

Are workers notified of past violent acts committed by customers or other personnel?
☑ Yes ☐ No ☐ Sometimes Notes: _________________________________
Are special precautions taken when workers:

Perform “enforcement” functions (parking control officers, inspectors, etc.)?
- Yes  - No  - Sometimes  Notes: _________________________________

Have to take something away from customers (illegal credit cards)?
- Yes  - No  - Sometimes  Notes: _________________________________

Have contact with people who behave violently?
- Yes  - No  - Sometimes  Notes: _________________________________

Have contact with dangerous animals (dogs, rodents, etc.)?
- Yes  - No  - Sometimes  Notes: _________________________________

(Source: OSHA)
### G. Facility Assessment Questionnaire: Working Alone Risks

<table>
<thead>
<tr>
<th>Location:</th>
<th>Building/Unit:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
<td>Time:</td>
</tr>
<tr>
<td>Name of Person(s) Conducting Assessment:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>In unit/building...</th>
<th>Yes</th>
<th>No</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do workers sometimes work alone? If so, do they know emergency alert procedures?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has an emergency contact number been established for all hours of operation?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are emergency telephones located in key areas, accessible to all staff? If no, where is access needed?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a designated “safe room” where employees can go during an emergency?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does this room have a telephone and a door that can be locked from the inside?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In these isolated areas, is there a telephone or a sign directing individuals to emergency assistance?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In these isolated areas, how far is the nearest person who might hear calls for help?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At the time of the inspection, did any areas seem isolated? If yes, which areas?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do employees have alarms or panic buttons (personal or stationary)?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are the alarms or panic buttons easily accessible?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are the functioning of panic buttons or alarms periodically checked?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is it easy to predict when people will be around?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Source: Ontario Safety Association for Community and Healthcare Environmental Assessment Tool, Preventing and Managing Violence in the Workplace Best Practice Guidelines, Registered Nurses’ Association of Ontario, Canada, June 2009)
H. Checklist: Hiring Process

In the wake of a negligent hiring lawsuit, a plaintiff’s attorney is sure to grill an organization with the questions below. By answering the questions relative to a recent hire, an organization can identify strengths and weaknesses in the hiring protocol and vulnerability to legal action. The questions:

- What did you do to verify the information on the employment application?
- Did you interview the employee? What did you ask? What did he or she say? What notes did you take?
- Did you contact his or her previous employers? Who did you speak to? What did each say? What did you ask? Was the inquiry in writing? What notes did you take?
- Did you give him or her any pen and paper questionnaires to identify his history of violence or criminal conduct?
- Did you check his or her personal references? Who did you speak to? What did each say? Was the inquiry in writing? What notes did you take?
- Did you conduct a criminal history search prior to hiring the employee? What counties and states did you search?
- Did you conduct a Social Security number search of the employee prior to employment?
- Did you check the person’s credit history prior to hire?
- Did you have someone from security interview the employee prior to employment?
- What positive information did you ascertain about the employee prior to employment?
- What negative information did you ascertain about the employee prior to employment?
- What did you do once an employee was hired to periodically determine if he or she was potentially violent or unfit for continued employment?
- Did you give any written test to the employee? Did you ask any questions to determine his or her history of violence?
- Did you ever speak with the police or local law enforcement about the employee?
- What memos or notes have you written, in general, about concerns regarding hiring practices?
- What meetings did you have with other supervisors about hiring practices?
- Did the employee sign consent allowing you to contact past employers for a reference and conduct an investigation before hiring him or her?
- Do you have any current employees who have criminal records?
- Do you have any former employees who had criminal records?
- Do you know what other companies do differently in screening employee applicants?

(Source: Steven C. Millwee, CPP, SecurTest Inc., Tampa, Fla.)
I. Checklist: Domestic Violence

Whether or not an organization is currently facing unknown risks of domestic violence spilling into the workplace depends on its corporate culture. Workplace violence prevention teams can assess the company’s culture with respect to this issue by answering the questions below. The more “yes” answers a company records, the better its chance that workers are bringing such problems to the company’s attention. The more “no” answers an organization tallies, the more effort it should put into creating an atmosphere in which employees will report issues of domestic violence.

1. We have very high overall employee morale.
   - [ ] YES  [ ] NO

2. We have open communication styles across all departmental and organizational levels.
   - [ ] YES  [ ] NO

3. We provide training for supervisors that includes general awareness of domestic violence, how to ask employees about their situation, and how to appropriately respond.
   - [ ] YES  [ ] NO

4. We provide awareness training for employees about family violence, including resources in the workplace and/or local community services for victims and perpetrators.
   - [ ] YES  [ ] NO

5. We teach managers to identify early warning signs of family violence (such as employees sleeping in their car and not at home).
   - [ ] YES  [ ] NO

6. We provide resources in the workplace for victims or potential victims, such as pamphlets and cards with local domestic violence program telephone numbers, and community resources for potential perpetrators.
   - [ ] YES  [ ] NO

7. Corporate management has spoken out specifically on the issue of domestic violence and the help available for employee victims.
   - [ ] YES  [ ] NO

8. Domestic violence issues are occasionally included as a topic in corporate publications and newsletters.
   - [ ] YES  [ ] NO

9. Employees perceive a safe, respectful, and confidential environment in which they feel comfortable coming forward and sharing personal information.
   - [ ] YES  [ ] NO

10. We have a company policy statement regarding domestic violence that includes security measures, leave of absence, job security, confidentiality, and a safe work environment.
    - [ ] YES  [ ] NO

(Source: Adapted from “Interrupting the Cycle of Violence: Addressing Domestic Violence Through the Workplace,” Ramsey County Initiative for Violence-Free Families and Communities, Minnesota Center Against Violence and Abuse, and other sources)
J. Checklist: Robbery Prevention

IOMA has developed this security management tool from current best practices in violence prevention at retail establishments, including those recommended by the Occupational Safety & Health Administration (www.osha.gov), the Crime Prevention Service of Rutgers University (http://crimeprevention.rutgers.edu), published crime prevention research sponsored by the National Association of Convenience Stores (Alexandria, Va.; 703-836-4564; www.cstorecentral.com), case studies, and IOMA interviews with crime prevention experts.

- Through written security policies, we have clearly outlined the responsibilities that managers, supervisors, and employees have in preventing violent crime and robberies in our store(s).
- We measure whether or not managers, supervisors, and employees understand these responsibilities.
- We have a system in place through which employees can express their safety concerns and present ideas for preventing robberies and other crime.
- We have a system in place to ensure the prompt and accurate reporting—to both local law enforcement and corporate security—of any violent incident or suspicious person or activity at our store(s).
- We have emergency telephone numbers for law enforcement, fire, and medical services posted in areas where store employees have access to a telephone with an outside line.
- In our written program and during employee training, we make it clear to employees that they will not face reprisals for reporting a robbery or other violent crime.
- We actively encourage employees to promptly report security incidents and to suggest ways to reduce or eliminate risks.
- We train, and provide regular refresher training, to store associates and managers in procedures to follow during and after a robbery.
- We train managers to follow basic procedures to reduce the risk of robbery. For example, to take greater security precautions during opening and closing (when businesses are more vulnerable); not to make cash handling or bank deposits part of a routine; to avoid opening the business before or after regular business hours; to only handle cash when the store is closed and the doors are locked; and to maintain as little cash on site as possible by making frequent bank deposits.
- We train store associates to follow basic procedures to prevent/respond to robberies. For example, based on a risk analysis, we may train them to greet all customers as they enter (to let potential robbers know they are being watched), to watch for suspicious customers (individuals who seem to linger waiting for other shoppers to leave), to avoid wearing jewelry at work, and so on.
VI. APPENDICES

- We assess whether policies, procedures, and training are presented in language and comprehension levels appropriate for the individuals being trained.

- We evaluate the competency and background of individuals who deliver robbery prevention training to store employees and managers; and we are confident they are equipped to provide this training.

- We solicit managers’ help in our fight to reduce robberies by training them to recognize area developments that may impact (for good or bad) the security of the store(s), such as the opening of a nearby bar, the boarding up of a nearby building, the opening of a nearby police outpost, and so on.

- We require store managers to provide the corporate security department with routine reports on all such area changes that may impact security and the risk of robbery.

- We repeat training for all employees and managers as necessary, but at least annually.

- We conduct regular monitoring of employees and stores to measure adherence to security procedures for preventing the risk of robberies; and then adjust training content and frequency based on the results of monitoring.

- The security department has educated senior management on the resources necessary to protect employees from robberies given the risk, including resources for physical security, training, and staffing.

- We periodically give employees a questionnaire or survey to get their feedback on the potential for violent incidents/robberies and to identify or confirm the need for improved security measures.

- Each store has established a liaison with local law enforcement for help in identifying ways to prevent and mitigate robberies.

- Each location(s) has established contact with similar local businesses to learn about their experiences and to alert each other of patterns of suspicious activity and to identify crime trends.

- We recognize that working alone at night is an additional risk factor and that having two clerks on duty is a primary deterrent to robbers; and we consider this in our staff scheduling.

- We keep computerized records of security incidents at our store(s) that include brief accounts of what happened before and during the incident, relevant details of the situation, and its outcome.

- In the computerized record of each robbery we note characteristic details, such as the time of day, if a weapon was used, what specific tasks employee(s) were performing prior to the robbery, and so on.

- We tabulate the overall data to establish a baseline against which to measure improvement, to identify trends that suggest changes in risk, and to glean specific security measures that will make employees safer from robberies.
We analyze trends in robberies relative to individual store locations to identify changes in risk and possible security improvements.

Through data analysis we have identified jobs and locations that face the greatest risk of violence.

Through data analysis, we have identified processes and procedures that put employees at greater risk of assault.

When possible, we obtain police reports and recommendations after each violent incident or robbery.

We conduct security surveys of all stores at least annually to assess their attractiveness to robbers (location, cash-on-hand, etc.) and make necessary security adjustments based on this analysis.

We conduct a new store security survey after each robbery to identify new or previously unnoticed risk factors and deficiencies or failures in work practices, procedures, or controls.

We occasionally use independent reviewers, such as law enforcement or private security specialists, to offer fresh perspectives and advice on strengthening our robbery prevention program.

Based on our establishment’s security risk analysis, we have made a determination as to whether the following security steps should or should not be taken:

- Improve store lighting, especially the entrances and cash register.
- Improve outside surveillance lighting of the parking area and areas of approach.
- Provide employees with bulletproof barriers or enclosures.
- Increase the number of employees on duty.
- Place cash register(s) on a raised platform to increase associates’ visibility.
- Install mirrors to eliminate blind spots.
- Remove advertisements and posters from the front windows to increase visibility and improve lighting.
- Limit physical access of customers to the cash register and employees. (This could be as simple as using a lockable swing gate to get behind a counter.)
- Lock all side and back entrances, and doors to back storage rooms or offices.
- Install time-controlled drop safes to deposit large bills and maintain low cash in the register.
- Hang signs saying that there is little cash in the register.
- Eliminate easy escape routes (for example, by placing speed bumps in traffic lanes used to exit or by reducing the chance for a quick escape by putting a fence between the store property and adjacent parking lots where would-be robbers may park their car).
- Install visible security cameras/monitors.
- Affix height markers on exit doors.
- Strategically place fences to control access to the store.
- Reduce store hours of operation.
K. Checklist: Organizational Culture

“Healthy” organizations make workplace violence less likely. In order to address and prevent the horrifying phenomenon of workplace violence and to better protect the lives and well-being of everyone, a healthy organization works diligently to do the following ten things:

1. Place a high value on human dignity and emphasize, by example, respect for all people without regard to rank or position.
   - The management of organizations must set the tone by establishing an atmosphere of dignity and civility in all human interactions.
   - Some organizations have established rules, complete with sanctions, to make rules on civility enforceable.

2. Initiate an effective workplace violence policy for all acts or threats of violence.
   - The policy must have emphasis from the highest level within the organization.
   - The policy should be applicable to everyone within the organization.
   - An effective policy should identify the kinds of behaviors that are prohibited (e.g., assaults, threats, direct or veiled, hazing, and so on).
   - The policy should be accessible for review by any employee of the organization.

3. Promote prevention of violence through formal training acknowledging awareness and prevention as the most ethical, humane, and effective means of addressing internal violence.
   - Violence prevention training for managers and supervisors SHOULD BE MANDATORY. Managers and supervisors are the eyes and ears of your organization. A lack of awareness at this level could easily translate to a failure of your violence prevention efforts.
   - Periodically update training because training has a “shelf life” and must be renewed to keep employees on track as to what is expected of them.
   - Documentation of all training must be posted to all personnel files.

4. Establish procedures for the timely reporting of acts or threats of violence.
   - Direct reporting to specific individuals.
   - Reporting through the supervisory chain of command.
   - Reporting through specific hot lines established for this purpose.
   - Secure online reporting.
   - IMPORTANT: Organizations must honor anonymity when requested by the reporting person. Failure to allow for anonymity could result in the loss of valuable life-saving information.
5. Thoroughly investigate and document all violent acts and take immediate and appropriate action to deal with them.

- Every act or threat of violence must be taken seriously.
- Investigations should take place as soon as possible.
- Reports of investigations must be of a level of quality so as to render them usable in a court of law.


- A multidisciplinary approach to problem solving is the most desirable.
- At a minimum, the team should be comprised of representatives of the following organizational subdivisions: An assigned executive (so as to maintain executive emphasis), HR, legal counsel, safety manager, risk manager, security manager, key managers and supervisors. Additional team members might include representation from the employee level, union representation, and so on.

7. Employ proper hiring practices as the first line of defense against internal violence.

- In the application process, ensure that consent is obtained from the candidate allowing your organization to obtain information such as: driving record, criminal history, permission to contact prior employer(s) regarding behavioral or performance issues.
- Subject every candidate to some form of background investigation.
- Conduct a personal interview of every potential candidate.
- Subject every new hire to a probationary period (one year is recommended).
- Ensure that all newly hired employees are exposed to your organization’s policies on workplace violence and ensure that it is documented and posted to their personnel files.

8. Offer and provide professional assistance to employees in need of counseling or psychological support. Examples include employee assistance programs and peer support programs.

9. Attain the highest practical level of physical security but understand its limitations. While a high level of physical security will protect employees from outside threats, it will do little to protect them from threats arising out of internal violence. This is why there must emphasis on training employees, particularly first-line supervisors, on workplace violence awareness and prevention.

10. Constantly evaluate the violence prevention efforts of your organization. Retain aspects that are successful and eliminate those that are not. Allow for input from all levels within your organization and reward those employees who took time to offer improvements.

(Source: Larry J. Chavez, B.A., M.P.A., Critical Incident Associates, Rancho Murieta, Calif.; 800-977-0122; www.workplace-violence.com; and other sources)
L. Checklist: Supervisor Training Points—Dealing With Aggressive Employees

**Do:**

- Project calm: move and speak slowly, quietly and confidently. Accept 100% responsibility for the conversation.

- Lead with the behavior you want the aggressor to mimic. People naturally mimic others’ posture. For example, sit down if you want the employee to sit. Or, if an employee has their arms crossed, cross yours and then uncross them—they will do the same.

- Be an empathetic listener. Encourage the person to talk and listen patiently.

- Focus your attention on the other person to let them know you are interested in what they have to say. Put papers away, turn away from your computer screen.

- Maintain a relaxed yet attentive posture and position yourself at a right angle rather than directly in front of the other person.

- Acknowledge the other person’s feelings. Indicate that you can see that he or she is upset. Try to find some commonality between you and the aggressor or their viewpoint.

- Ask for small, specific favors, such as asking the person to move to a quieter area.

- Use numbers to switch an individual’s thinking from the emotional part of their brain to the analytical. Use phrases such as, “First, can you please repeat what you said, only more slowly.”

- Provide clear choices to the aggressor. (Make sure they are reasonable, you may be called on it.)

- Break big problems into smaller, more manageable problems that can be effectively addressed.

- Accept criticism in a positive way. When a complaint might be true, use statements like, “You’re probably right.” If the criticism seems unwarranted, ask clarifying questions.

- Ask for his/her recommendations. Repeat back what you feel is being requested of you.

- Orient your office so that your chair is the one closest to the exit door. Avoid typical office set-ups where others can easily block the door.

- Take into consideration any cultural differences, such as personal space needed, etc.

**Do not:**

- Use styles of communication that generate hostility, or order the aggressor with phrases such as “calm down.” Don’t be perceived as being cold or intent on going strictly by the rules.
● Reject all of the person’s claims from the start or make promises you can’t or do not intend to keep.

● Pose in challenging stances, such as standing directly opposite someone, hands on hips, or with your arms crossed. Don’t make sudden movements that may be seen as threatening. Be aware of your tone, volume, and rate of speech.

● Belittle the person in a way that can make them feel foolish or attempt to make the situation seem unimportant or less serious.

(Source: Compiled from OSHA handbooks, the State of Connecticut Department of Veterans Affairs, NSC Annual Congress presentation “Managing Aggression in Our Workplace,” and other sources)
### M. Highest-Rated Security Measures for Preventing Workplace Violence, by Industry*

<table>
<thead>
<tr>
<th>Industry</th>
<th>Staff on Staff Violence</th>
<th>Violence from External Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Best</td>
<td>2nd</td>
</tr>
<tr>
<td></td>
<td>2nd</td>
<td>3rd</td>
</tr>
<tr>
<td></td>
<td>3rd</td>
<td>2nd</td>
</tr>
<tr>
<td><strong>Academic &amp; Cultural Institutions</strong></td>
<td>Employee training</td>
<td>Policies &amp; procedures**</td>
</tr>
<tr>
<td><strong>Business Services</strong></td>
<td>Policies &amp; procedures</td>
<td>Employee training</td>
</tr>
<tr>
<td><strong>Entertainment &amp; Public venue[1]</strong></td>
<td>Employee training</td>
<td>Background screening</td>
</tr>
<tr>
<td><strong>Government &amp; Public</strong></td>
<td>Employee training</td>
<td>Policies &amp; procedures</td>
</tr>
<tr>
<td><strong>Hospital &amp; Health Care</strong></td>
<td>Employee training</td>
<td>Policies &amp; procedures</td>
</tr>
<tr>
<td><strong>Financial services &amp; Insurance</strong></td>
<td>Background screening</td>
<td>Employee training</td>
</tr>
<tr>
<td></td>
<td>Employee training</td>
<td>Background screening</td>
</tr>
<tr>
<td><strong>Property Management</strong></td>
<td>Employee training</td>
<td>Policies &amp; procedures</td>
</tr>
<tr>
<td><strong>Retail</strong></td>
<td>Policies &amp; procedures</td>
<td>Background screening</td>
</tr>
<tr>
<td><strong>Security Services</strong></td>
<td>Policies &amp; procedures</td>
<td>Employee training</td>
</tr>
<tr>
<td><strong>(tie) Background screening</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td>Background screening</td>
<td>Employee training</td>
</tr>
<tr>
<td><strong>Utility [2]</strong></td>
<td>Employee training</td>
<td>Background screening</td>
</tr>
</tbody>
</table>

*Survey of organizational security representatives

**including discipline

***including lighting

[1] including restaurant, lodging, sports stadium, casino, convention center, etc.

[2] including oil and gas

(Source: IOMA/SDR)
N. Illustrative Pair-wise Threat Analysis

### Threat Likelihood

<table>
<thead>
<tr>
<th>Threats</th>
<th>Workplace Violence</th>
<th>Physical Destruction</th>
<th>Hazmat Release</th>
<th>Theft</th>
<th>Cyber</th>
<th>Vandalism</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workplace Violence</td>
<td>5.00</td>
<td>5.00</td>
<td>4.00</td>
<td>5.00</td>
<td>3.00</td>
<td>22.00</td>
<td></td>
</tr>
<tr>
<td>Physical Destruction</td>
<td>1.00</td>
<td>4.00</td>
<td>1.00</td>
<td>3.00</td>
<td>1.00</td>
<td>10.00</td>
<td></td>
</tr>
<tr>
<td>Hazmat Release</td>
<td>1.00</td>
<td>2.00</td>
<td>1.00</td>
<td>2.00</td>
<td>1.00</td>
<td>7.00</td>
<td></td>
</tr>
<tr>
<td>Theft</td>
<td>2.00</td>
<td>5.00</td>
<td>5.00</td>
<td>4.00</td>
<td>2.00</td>
<td>18.00</td>
<td></td>
</tr>
<tr>
<td>Cyber</td>
<td>1.00</td>
<td>3.00</td>
<td>4.00</td>
<td>2.00</td>
<td>2.00</td>
<td>12.00</td>
<td></td>
</tr>
<tr>
<td>Vandalism</td>
<td>3.00</td>
<td>5.00</td>
<td>5.00</td>
<td>4.00</td>
<td>4.00</td>
<td>21.00</td>
<td></td>
</tr>
</tbody>
</table>

1 = Much Lower Than  
2 = Lower Than  
3 = Same As  
4 = Greater Than  
5 = Much Greater Than

### Threat Impact

<table>
<thead>
<tr>
<th>Threats</th>
<th>Workplace Violence</th>
<th>Physical Destruction</th>
<th>Hazmat Release</th>
<th>Theft</th>
<th>Cyber</th>
<th>Vandalism</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workplace Violence</td>
<td>4.00</td>
<td>4.00</td>
<td>5.00</td>
<td>4.00</td>
<td>5.00</td>
<td>22.00</td>
<td></td>
</tr>
<tr>
<td>Physical Destruction</td>
<td>2.00</td>
<td>3.00</td>
<td>4.00</td>
<td>3.00</td>
<td>5.00</td>
<td>17.00</td>
<td></td>
</tr>
<tr>
<td>Hazmat Release</td>
<td>2.00</td>
<td>3.00</td>
<td>4.00</td>
<td>3.00</td>
<td>5.00</td>
<td>17.00</td>
<td></td>
</tr>
<tr>
<td>Theft</td>
<td>1.00</td>
<td>2.00</td>
<td>2.00</td>
<td>3.00</td>
<td>4.00</td>
<td>12.00</td>
<td></td>
</tr>
<tr>
<td>Cyber</td>
<td>2.00</td>
<td>3.00</td>
<td>3.00</td>
<td>3.00</td>
<td>4.00</td>
<td>15.00</td>
<td></td>
</tr>
<tr>
<td>Vandalism</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>2.00</td>
<td>2.00</td>
<td>7.00</td>
<td></td>
</tr>
</tbody>
</table>

### Design Basis Threat

<table>
<thead>
<tr>
<th>Threats</th>
<th>Likelihood</th>
<th>Workplace Violence</th>
<th>Physical Destruction</th>
<th>Hazmat Release</th>
<th>Theft</th>
<th>Cyber</th>
<th>Vandalism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likelihood</td>
<td>22</td>
<td>10</td>
<td>7</td>
<td>18</td>
<td>12</td>
<td>12</td>
<td>21</td>
</tr>
<tr>
<td>Impact</td>
<td>22</td>
<td>17</td>
<td>17</td>
<td>12</td>
<td>15</td>
<td>15</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>484</td>
<td>170</td>
<td>119</td>
<td>216</td>
<td>180</td>
<td>147</td>
<td></td>
</tr>
</tbody>
</table>

(Source: Using CARVER to determine the relationship between your assets and the consequence of threats, Pearson & Patterson, 2009 ASIS International Annual Conference 2009)
### O. Matrix of Workplace Violence Training Requirements

<table>
<thead>
<tr>
<th></th>
<th>Senior/Middle Mgmt.</th>
<th>Staff (No Public Contact)</th>
<th>Staff (Public Contact)</th>
<th>Department Supervisors</th>
<th>Emergency Responders</th>
<th>Trainers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsibility of organization for worker safety</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Effective organizational approaches to management of violence</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y/N</td>
<td>Y</td>
</tr>
<tr>
<td>Basic personal safety training</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y/Y</td>
<td>Y</td>
</tr>
<tr>
<td>Dealing with verbally abusive clients</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Verbal de-escalation</td>
<td>N</td>
<td>N</td>
<td>Y/N</td>
<td>Y</td>
<td>Y/Y</td>
<td>Y</td>
</tr>
<tr>
<td>Escape techniques</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Apprehension/restraint</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Teaching and presentation skills</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Duration of training (hours)</td>
<td>7 to 15</td>
<td>3.5 to 7</td>
<td>14 to 21</td>
<td>21 to 30</td>
<td>31 to 40</td>
<td>40 to 70</td>
</tr>
</tbody>
</table>

(Source: UK National Health Service Trust and other sources)
P. Checklist: Program Deficiency Audit

Below are 12 markers that suggest a deficient violence prevention process. Companies need to review their programs if:

- They don’t track incidents. Companies need to track when, where, and how often threats or violence occurs.
- They don’t use a team approach. Except for the smallest of companies, organizations need to respond to issues of workplace violence through a team comprised of all necessary stakeholders.
- They don’t have all the team members it needs. Companies need to have on board representatives from HR, legal, a threat assessment specialist, security, safety, and so on.
- They have failed to write, update, and distribute a workplace violence policy to everyone.
- They haven’t provided training at all levels that includes the levels of violence, warning signs, and what to do about it.
- They do not have a clear system for reporting incidents. A system must include distributing to all employees the phone numbers and contact information for people to whom employees should make reports.
- They don’t make someone available 24/7 to accept calls from employees who need to report an incident. For example, an employee who faces a domestic violence issue over the weekend should be able to notify his or her employer of the incident before Monday morning.
- They don’t have access to an individual(s) who is competent to conduct a threat assessment should an incident arise (which could be a security team member but should also include a mental health specialist).
- They fail to write procedures for conducting a workplace violence investigation.
- They don’t have a written violence vulnerability assessment. Companies need to look at themselves and determine where they might be prone to violence.
- They have not partnered with external resources. Security directors need to be on a name basis with at least two members of local law enforcement who are higher than foot patrol level. They also need to have a relationship with a private security company in the event security requirements exceed what the organization can do itself. They should also have the names and contacts for at least one organization that deals with domestic violence.
- They don’t conduct background screening that would turn up evidence that an employee might be a risk.

(Source: IOMA interviews, including James Madero, Ph.D., president of Violence Prevention International, www.vpi-prevent.com). VPI performs workplace violence prevention training, develops workplace violence prevention plans with clients, and conducts threat assessments.)
Q. Conflict Accounting Tool—Conflict Cost Estimation Worksheet

Identify one conflict that is very familiar to you—something you supervised or of which you were a close observer. It may be a conflict that is still current or one that happened recently. Derive cost estimates for each “cost factor” by following the worksheet instructions. Not all cost factors are relevant to every conflict, but every conflict incurs cost by several means. Ask yourself with regard to each cost factor, “Did/does the conflict have the effect of…” If you answer yes, calculate its dollar cost in the ways suggested.

Conflict identifier: ____________

<table>
<thead>
<tr>
<th>Cost Factors/Estimated Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Wasted time: $ ____________   ● Salary and benefits per hour/day (150%).</td>
</tr>
<tr>
<td>2. Reduced decision quality: $ ____________   ● Any decision made by you and/or others, independently or jointly, affected by the conflict.</td>
</tr>
<tr>
<td>3. Loss of skilled employees: $ ____________   ● Cost of loss of human resource (150% of total annual compensation).</td>
</tr>
<tr>
<td>4. Restructuring: $ ____________   ● Inefficiency of work redesigned to accommodate conflict.</td>
</tr>
<tr>
<td>5. Sabotage, theft, damage: $ ____________   ● Equipment, work processes, reputations.</td>
</tr>
<tr>
<td>6. Lowered job motivation: $ ____________   ● Reduced performance/productivity percent reduction x salary.</td>
</tr>
<tr>
<td>7. Lost work time: $ ____________   ● Number of days lost at prorated daily salary.</td>
</tr>
<tr>
<td>8. Health costs: $ ____________   ● Stress-related.   ● Insurance premiums linked to rate of claims.</td>
</tr>
</tbody>
</table>

Total cost: $ ____________

Worksheet instructions

**Factor 1: Wasted time.** Conflict distracts employees from otherwise productive use of their time. Studies show that managers spend 30% to 42% of their time reaching agreements stemming from conflict. Estimate the amount of time wasted by each person who is/was affected by the conflict. Then calculate the financial cost as a fraction of monthly or annual salary or wage, including the value of insurance and other fringe benefits (typically at least 50% of gross salary). Example: Four employees waste 40 hours each during a six-month period because of conflict. They each have an annual salary of $40,000. A year’s salary is generally about two-thirds of total compensation. The dollar value of the four employees’ wasted time is $4,615.38.

**Factor 2: Reduced decision quality.** Decisions made during conflict are inferior. Why? (1) They are not based on an optimum quantity and quality of objective information. (2) The struggle tends to contaminate the decisionmaking process. A precise estimate is impossible, but ask yourself, “What opportunities were lost by poor decisions affected...”
by this conflict? What might have been gained if a better decision had been made?” Considering these influences on
decisions made by the people affected by your target conflict, conservatively estimate its potential financial impact.
Guideline: Use 50% of the dollar impact of decisions made during the conflict (e.g., $2,500 if a team was in conflict over
the purchase of a $5,000 piece of equipment).

**Factor 3: Loss of skilled employees.** Exit interviews reveal that chronic unresolved conflict is a decisive factor in at
least 50% of all departures. Conflict accounts for up to 90% of involuntary departures. Raytheon Corp. determined
that replacing an engineer costs 150% of his or her total annual compensation. This determination was reached by
accounting for lost productivity, recruiting fees, interviewing time, staffing department employee salaries, orientation and
retraining costs, etc. So, replacing an employee whose annual salary is $40,000 incurs a cost of $90,000. If one or more
employees were to depart at least partially because of the conflict, figure the cost to your organization.

**Factor 4: Restructuring.** Employers frequently redesign workflow to reduce the amount of interaction between
employees who are in conflict. Restructured work is usually less efficient than the original design. Use a subjective
assessment to give a reasonable estimate of the loss. Guideline: Use 10% of the combined salaries of the employees
involved in the restructuring for the duration of the restructuring. Example: Estimate $8,000 if four employees, each
of whom is paid $40,000 annually, were reassigned to different task groups for a six month period; i.e., ($40,000
x 4)/10/2). Rationale: The financial value of employees to an employer is, by definition, roughly equivalent to their
salaries. Restructured work, used to control interpersonal conflict, is probably not the most efficient allocation of human
resources.

**Factor 5: Sabotage/theft/damage.** Employee conflict increases damage and theft of inventory and equipment.
Employee anger at the organization increases covert sabotage of work processes and management’s efforts.
Management often does not recognize such losses or excuses them as “accidental.” Enter a conservative figure on the
worksheet. Guideline: Use 10% of the acquisition cost of equipment, tools, and supplies that employees involved in
the conflict use in performing their jobs. Example: $2,500, if an operator of a $20,000 machine in a manufacturing
environment is angry with his/her supervisor ($2,000 for careless operation and maintenance of the machine, plus $500
for unnecessary scrap and waste of raw materials).

**Factor 6: Lowered job motivation.** Motivation decreases due to the stress of trying to get along with a “difficult
person.” As a baseline figure, use the productivity that would have occurred had there been no conflict. Then, estimate
a percentage decline of that productivity. Multiply that percentage times the dollar value of the total compensation of
the person(s) affected to derive a figure. Example: Three employees’ productivity declines 20% for three months. Using
figures similar to those above, the three employees’ total compensation was 3 x $60,000, or $180,000. Since one-fourth
of this amount ($45,000) was earned during the three-month period, this factor cost the organization $9,000.

**Factor 7: Lost work time.** Absenteeism varies directly with job stress, especially the stress associated with anger
toward coworkers. Additionally, nearly every physical illness and injury is partially psychogenic (caused by psychological
conditions). Arrive at an estimate by prorating daily or monthly compensation. Guideline: Use 10% of the annual salaries
of the employees in conflict. Example: $18,000 if all six members of a department, each of whom is paid $25,000
annually, are in ongoing conflict with their supervisor, who is paid $30,000, throughout the year ($25,000 x 6) divided by
10 + $30,000 divided by 10.

**Factor 8: Health costs.** Conflict contributes to the rate of claims that affect the premium paid by an employer to its
insurer, making insurance an indirect cost of workplace conflict. Estimate the percentage of the psychogenic component
of medical problems that have occurred while your targeted conflict has gone on, and multiply this percentage by
the premium increase imposed by your organization’s insurer. Admittedly, this psychogenic component is difficult to
ascertain, and you may not be privy to the insurance costs of your employer. So, enter a conservative figure based on
your knowledge. A shortcut is to enter 10% of the number you have entered for Factor 6, since the stress that results in
reduced productivity is also related to physical health.

**Total cost:** Add the figures in each of the eight cost factors for an estimated total cost of the conflict. This is the cost
to your organization of this one conflict. Multiply the figure by the estimated number of conflicts companywide, for an
estimate of conflicts’ overall drain on your company resources.

(Source: Adapted from Managing Differences: How to Build Better Relationships at Work and Home, by Daniel Dana,
revised 2nd edition)
VI. APPENDICES

Healthcare example

Using the conflict accounting model detailed above, the following spreadsheet shows an example of costs from an actual case of conflict between a doctor and two nurses in a patient care facility in New England. By examining the table in conjunction with the worksheet and instructions, one can follow how this specific case of unresolved conflict cost the hospital more than $60,000.

<table>
<thead>
<tr>
<th>Factor/Description</th>
<th>loss</th>
<th>loss units</th>
<th>Nurse #1</th>
<th>loss</th>
<th>loss units</th>
<th>Nurse #2</th>
<th>loss</th>
<th>loss units</th>
<th>Doc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salary</td>
<td>$22,000</td>
<td></td>
<td>$33,500</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$100,000</td>
</tr>
<tr>
<td>Salary + benefits</td>
<td>$33,000</td>
<td></td>
<td>$50,250</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$150,000</td>
</tr>
<tr>
<td>Workweek hours</td>
<td>37.5</td>
<td></td>
<td>28.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>37.5</td>
</tr>
<tr>
<td>Length of unresolved conflict</td>
<td>52.0</td>
<td></td>
<td>12.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>52.0</td>
</tr>
<tr>
<td>1. Wasted time/energy</td>
<td>3.0 hrs/wk</td>
<td>$609.23</td>
<td>5.0 hrs/wk</td>
<td>$2,070.74</td>
<td>2 hrs/wk</td>
<td>$1,846.15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total $ wasted time</td>
<td></td>
<td>$4,526.13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Reduced decision quality</td>
<td></td>
<td>$1,500</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Loss of skilled employees</td>
<td>2.0 empl</td>
<td>$42,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employee #1 salary</td>
<td>$22,000</td>
<td></td>
<td>$33,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employee #2 salary</td>
<td>$20,000</td>
<td></td>
<td>$9,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Restructuring</td>
<td>2.0 empl</td>
<td>$1,858.33</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employee #1 salary</td>
<td>$33,750</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employee #2 salary</td>
<td>$22,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Sabotage; theft; damage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Lowered job motivation</td>
<td></td>
<td>$2,938</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employee #1 salary</td>
<td>$33,500</td>
<td></td>
<td>8.0 % decline</td>
<td>40%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employee #2 salary</td>
<td>$22,000</td>
<td></td>
<td>52.0 % decline</td>
<td>20%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employee #3 salary</td>
<td>$20,000</td>
<td></td>
<td>1.0 % decline</td>
<td>20%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employee #4 salary</td>
<td>$20,000</td>
<td></td>
<td>20.0 % decline</td>
<td>20%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Lost work time</td>
<td></td>
<td>$9,300</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employee #1 salary</td>
<td>$37,500</td>
<td></td>
<td>$3,750</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employee #2 salary</td>
<td>$22,000</td>
<td></td>
<td>$2,200</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employee #3 salary</td>
<td>$33,500</td>
<td></td>
<td>$3,350</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Health costs</td>
<td></td>
<td>$293.85</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL COST OF CONFlict</td>
<td></td>
<td>$60,916.77</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

About the Author

Garett Seivold

Garett Seivold has been covering corporate security for industry professionals for 14 years. He has been recognized by several organizations for outstanding writing, investigative reporting, and instructional journalism. He is also a former First Place Award Winner for Best Instructional Story by the Newsletter Publisher’s Association. Since 1998, he has served as the writer and editor of IOMA’s Security Director’s Report, a monthly newsletter highlighting trends and best practices in corporate security management. He is the author of IOMA’s monthly e-zine, Security Insider’s e-Alert, and has authored more than a dozen research reports and best practice manuals on crime prevention, disaster preparedness, workplace violence, and counterterrorism. He is a graduate of the University of North Carolina-Chapel Hill and currently resides in Indio, California.

IOMA/IOFM’s research, education and training resources for corporate security professionals include:

- Security Guard Firm Ratings & Benchmarks Report
- Security Director’s Report, a monthly newsletter covering all forms of workplace protection in today’s environment
- IOMA’s Global Corporate Security Leadership Network
- Security Policies, Practices and Management Standards 2010
- Security Budgets & Cost-Containment Strategies 2010
- Physical Security Performance 2009: Metrics, Benchmarks and ROI
- Benchmark Report on Security Department Salaries & Training Practices
- Disaster Preparedness: The Guide to Building Business Resilience
- Security Regulation, Compliance & Liability Prevention
- Hospital Security Best Practices, Benchmarks & Compliance
- Safety Management Best Practices
- Corporate Anti-Terrorism Benchmarks and Best Practices
- The Complete Guide to Managing Risks To—And From—The Mobile Workforce

IOMA’s Institute of Finance & Management
Corporate Security Products & Services

The Leading Source of Information for Corporate Security Professionals