ICJE, P.O. Box 293, Montgomery, AL 36101 * 334-280-0020

ICJE Feature Article, March 26, 2001

Preventing Workplace Crime

Robert T. Thetford, J.D.

Many crime surveys, including the FBI's Uniform Crime Reports, show a drop in crime during the 1990s. The latest figures (December, 2000), however, show that the drop in the crime rate has at best leveled and at worst is climbing again. **(1)** Even if violent crime has leveled in the year 2000, it still averages 40 percent higher than in 1969, a sobering statistic.

Workplace violence is a major area of concern for Americans, with about 2 million people each year becoming victims of violent crime or threatened violent crime in the workplace, according to a study by the Justice Department's Bureau of Justice Statistics (BJS) which covered the years 1992 through 1996.**(2)**

In fact, murder is the number one cause of death for women at work, and the number two cause for men at work, with an average of twenty-one Americans murdered each week at work.**(3)** Domestic problems account for the majority of the workplace homicide motives with many of the victims being killed either by people they knew or with whom they had personal relationships.**(4)** What makes these statistics so amazing is that workplace homicide was virtually unknown a quarter of a century ago. Conditions have quickly deteriorated, however, and the homicide rate has virtually tripled in the last decade.**(5)**

A Gallup Poll published in September, 2000, found that American workers are increasingly feeling pressure from rapidly changing technology, mounting job stress and fear of random workplace assaults, and that they blame their bosses for giving them little or no guidance on how to deal with it.**(6)**

In one particular area alone (the health care industry), nurses are victims of assault at a rate of 24.9 per thousand, much higher than the average of 14.8 per thousand for all occupations.**(7)** Violence is associated with all kinds of health care settings, including surgical and pediatric units, and especially emergency rooms.**(8)**

It is little wonder that the rise in workplace crime is accompanied by an explosion of litigation against employers owning or controlling the workplace. The duty of care required of employers

generally consists of a combination of Federal Law, particularly the General Duty Clause of the Occupational Safety and Health Act, and state tort law, particularly negligent employment torts. The rates of litigation in this area parallel or exceed the rates in other areas of society, with the percentage rise of suits and judgments now reaching staggering proportions.

Even though workplace violence receives most of the attention, other workplace area crimes continue to increase, including theft, burglary, drug sales and possession, and recently computer related crime.

Again in the health care industry, the storage of drugs, frequent location of facilities in high crime areas, the apparent lack of visible security, and the presence of elderly people who are least likely to resist robbery or assault, provide a fertile field for the proliferation of crime.

Health care facilities have embraced technology in recent years with computers touching every aspect of the industry. Recently, however, this industry, like most businesses, has discovered just how vulnerable it has become to intrusion, viruses and electronic theft. Targets for computer intrusion include employee files and human resource data, business plans and strategies, research and development plans, facility floor plans and blueprints, technical data, financial conditions and perhaps most importantly, patient or client records.**(9)**

While funding for prosecutors remains static, computer crime has quadrupled over the past three years, according to a survey by the FBI and San Francisco's Computer Security Institute. Seventy-five percent of the hacking victims - most often corporations and government agencies - said it cost an average of $1 million per intrusion to investigate, repair and secure their systems. Corporations spent $7.1 billion in 1999 on corporate security to protect themselves against cyberattacks and the bill could reach $17 billion by 2003, according to Internet analysts at Aberdeen Group in Boston, Mass.**(10)**

In the summer of 2000, a sophisticated hacker took command of large portions of the University of Washington Medical Center's internal network and downloaded computerized admissions records for four thousand heart patients. The intrusions began in June, and continued until at least mid-July, before network administrators at the Seattle teaching hospital detected the hacker and cut him off. The medical center was reportedly unaware that patient records were downloaded, and elected not to notify law enforcement agencies of the intrusions.

The hacker, a 25-year-old Dutch resident who calls himself “Kane,” posted a notice that stated, "All the data taken from these computers was taken over the Internet. All the machines were exposed without any firewalls of any kind."**(11)**

If it is not enough dealing with homicidal spouses, thieves, burglars, and malicious hackers, we now must face a new threat - the terrorist, who may be intent on destroying the very infrastructure of a society through any means available. Recently, we have observed evidence of the future kind of war, a Cyberwar in which the targets are more likely to be businesses rather than government installations.**(12)**

The first steps in neutralizing the above cited dangers are to recognize potential threat origins, analyze the nature of the threats and identify the likely targets. This is accomplished through implementing a thorough assessment of the strengths and weaknesses of organizational security, specifically identifying those areas which need physical, technological and/or administrative attention.

Once the assessment of security needs is completed and the serious nature of any likely threat is understood, it is vital to clearly communicate the findings and recommendations to management at all levels of the organization in order to insure commitment in addressing the threat and implementing a Crime Prevention Plan as an augmentation to the organization's policy and procedure manual. This will necessarily include awareness and security training for supervisors and employees as well as a review of pre-employment screening for signs of instability or potential criminal behavior.

The Crime Prevention Plan must be continuously measured against known, published attacks, penetrations and other criminal acts occurring in similar organizations to insure the security measures in place afford the highest level of safety for the organization, its employees and the public it serves.

Finally, a thorough After-Action Plan must be formulated and implemented for those incidents which do occur within the organization. No Crime Prevention Plan is perfect, and only through careful and thorough examination of the organizational response to each incident will a security plan become effective at deterring, detecting and neutralizing criminal activity.

Endnotes

.1. **FBI UNIFORM CRIME REPORTS FOR RELEASE, JANUARY - JUNE 2000 DECEMBER 18, 2000.** The number of Crime Index offenses reported to law enforcement agencies throughout the United States declined 0.3 percent during the first 6 months of 2000 when compared to the figures reported during the same period of 1999. The violent crimes of murder, forcible rape, robbery, and aggravated assault and the property crimes of burglary, larceny-theft, and motor vehicle theft both decreased 0.3 percent. During the first quarter of 2000, a drop of 0.2 percent in serious crime was reported when compared with the numbers reported for the same quarter of 1999. Second quarter numbers increased 0.3 percent.
.2. PRNewswire, July 26, 1997.
.3. Lylnne Falkin McClure, Ph.D., Risky Business: Managing Employee Violence in the Workplace. (New York: The Haworth Press, 1996), P.1 (Citing a study by the National Institute for Occupational Safety and Health).
.4. Ibid, p. 2.
.5. S. Anthony Baron, Ph.D., Violence in the Workplace, (Ventura, Calif.: Pathfinder Publishing 1993), p. 15.
6. Alex Johnson, "Fear and Loathing on the Job," *MSNBC Online*, 9/4/00. .
.7. Greg Warchol, *Workplace Violence, 1992-1996*, (Washington, D.C. U.S. Department of Justice, Bureau of Justice Statistics, 1998).
.8. Richard Denenberg and Mark Braverman, The Violence Prone Workspace, (Ithaca, N.Y.: Cornell University Press, 1999), p. 9.
.9. William C. Boni and Dr. Gerald L. Kovachich, I-Way Robbery, (Boston: Butterworth Heinemann, 1999), pp. 104-107.
.10. By Martha Mendoza ,The Associated Press S T A N F O R D, Calif., April 6
.11. Kevin Poulsen, "Hospital records hacked hard," The Register, 7/12/00, online at http://www.theregister.co.uk/content/6/15285.html.

.12. "Middle East Cyberwar Could Spread to U.S.," *NewsMax.com,* Wednesday, Nov. 1, 2000, Online http://www.newsmax.com/articles/?a=2000/10/31/202920.
