

A quarter century of vision

The Lipman Report reflects on a successful history

This edition of The Lipman Report commemorates 25 years of security reporting on a wide range of cutting-edge topics. From the inaugural issue published in November 1977 until the present, The Lipman Report has offered management with up-to-the-minute intelligence on the latest security challenges and trends. This issue explores the evolving coverage provided by this publication on four critical topics during the past quarter century: terrorism, workplace violence, computer security and drugs in the workplace.

The terrorist threat

Since September 1979, the editors of *The Lipman Report* have chronicled the threat of terrorism in almost 70 newsletters. The August 1980 issue noted an increase in terrorism-related deaths, despite a decline in incidents. More importantly, 40 percent of international terrorist acts were directed against U.S. citizens and property, with more than 36 percent targeting either American businesspeople or their facilities.

The following year, in April 1981 the report pointed out the danger of complacency, as many executives failed **“to acknowledge the particular threat to themselves, their businesses and their families”** despite widespread reports of increased terrorist activity. Terrorism at that time was considered too remote a threat to constitute a serious hazard. Consequently, most organizations failed to address terror acts until after an incident such as a bomb threat or extortion attempt occurred, leaving them woefully unprepared when disaster struck. More than two decades later, this “it-won’t-happen-to-me” mindset continues to pervade corporate America in spite of the devastating attacks against the World Trade Center and the Pentagon in September 2001 and the Oklahoma City bombing in April 1995.

The January 1983 issue of *The Lipman Report* addressed the continuing terrorist threat to U.S. businesses, attributing the growing danger to the fact that American corporations and their executives represent the capitalist ideology. **“By targeting the symbols of Western power and**

wealth, terrorists are attacking what they consider ‘Yankee imperialism,’ an ideology totally hostile to many terrorist groups’ own political and economic goals.” The editors warned that U.S. society has no reason to expect these anti-American sentiments to decrease in the future.

Indeed, in November 1983, a terrorist’s bomb blast shook the U.S. Capitol building, bringing the foreign menace to domestic soil. The December 1983 newsletter examined the factors that led to the attack, then described the reactive security measures implemented in the wake of the blast. Next, the report recommended several additional precautions as further protection against a future assault, including limited vehicle access, electronic identification cards for employees, enhanced package control and redundant security systems. Many of these recommendations were considered for future implementation but were ultimately shelved as time passed and complacency returned.

The February 1984 issue described the Beirut Marine tragedy of October 1983 as “an omen of things to come.” U.S. forces in Beirut failed to heed numerous warnings of a car-bomb attack, leaving them vulnerable to the assault that killed 241 U.S. military personnel on a peacekeeping mission. **“We cannot afford complacency, nor can we depend entirely on Federal, State and local sources for protection against terrorist assault,” warned the editors in the report’s conclusion. “It is our responsibility as security advisers to alert America’s decision-makers of the immediate needs to create as secure an institution, organization or government as possible.”**

In upholding this responsibility, *The Lipman Report* addressed the dangers of chemical and biological weapons in May 1984, more than 10 years before the sarin nerve gas attack in the Tokyo subway system and almost two decades before a still-unknown enemy distributed weapons-grade anthrax through the U.S. postal
(continued on next page)

A quarter century of vision

The Lipman Report reflects on a successful history

(continued from preceding page)

system. The newsletter discussed the chemical and biological weapons capabilities of the then-Soviet Union, pointing out that the existence of these weapons, combined with terrorist fanaticism, could herald an unprecedented threat to the United States.

The November 1984 issue of this publication also addressed the growing menace of terrorism, examining its past, present and future. The editors pointed out that the United States has **“two methods to neutralize terrorist attacks upon our facilities. Defenses to prevent the attack, or deterrents sufficient to prevent an attack for fear of the consequences.”** The months following the terrorist attacks of September 11, 2001, demonstrated an evolved determination on the part of terrorist organizations such as al Qaeda, making it less likely than ever that the United States can hope to avoid future assaults. At the same time, organizations can still reduce their likelihood of attack by hardening their defenses and encouraging would-be attackers to seek a softer target.

The January 1986 edition focused on shortcomings in the U.S. transportation sector that represented serious vulnerabilities to the terrorist threat. The issue offered chilling observations given that 19 hijackers exploited these very weaknesses on September 11 in carrying out their suicide mission. The editors warned, **“It is probable that, if some Middle Eastern fanatic gives a command, the people who are to carry out the acts already have homes and jobs in this country, that they have their targets assigned and their instruments of destruction prepared, and expect to achieve their goals even at the cost of their lives if that is what it takes.”** Just over one year ago, these words rang true in the most tragic way.

Security initiatives recommended in this report that were not implemented until after the September 11 attacks included discontinuing curbside baggage check-in and permitting passengers only beyond the screening point. Curbside

check-in, however, has since resumed as the nation returns to its “business-as-usual” state.

Several issues of *The Lipman Report* in the mid-to late-1980s discussed the terrorist threat posed by Libya, Syria and Iran. These articles pointed out the political objectives of state-sponsored terrorist groups and demonstrated that these organizations increasingly targeted U.S. businesses and executives because they represented easier, although equally attractive, marks. Recommended precautions focused on travel security since most of the attacks occurred on foreign soil: increased perimeter security, a professional security force, executive protection teams. The reports also offered suggestions specifically geared toward traveling executives to decrease their likelihood of victimization: flying “neutral” airlines, selecting direct flights whenever possible, planning itineraries carefully, avoiding destinations with mounting political tensions, dressing inconspicuously and varying one’s daily routine, to name a few.

The April 1993 report, “War Without Frontiers,” described the factors contributing to the continued rise of terrorism, using as illustration the bombing of the World Trade Center in New York, which took place only two months before in February. The article cited the political motivation of terrorist groups in Puerto Rico and in the Middle East, emphasizing that the threat stemmed not from a single enemy, but from diffuse organizations. The spread of radical fundamentalism—with a trend toward more violent demonstrations—further heightened the danger of terrorist attack. The main contributing factor, however, ultimately lay in the founding principles that make the United States of America the greatest form of democracy yet devised: **“Because we do not monitor the activities of residents or visitors unless we have reason to do so, we cannot escape the fact that those bent on harming our people or institutions often find it easy to escape detection while they hatch nefarious plans. . . . There is only one method of recourse, only one avenue to increased safety: because we will not give up**

our liberties, it is imperative that we become more vigilant.”

These last words have appeared on the pages of this publication numerous times during the last quarter century; unfortunately, as time passes and threats recede into memory, many security departments cannot obtain the budgets and the maintain the executive focus necessary for such vigilance.

In the mid-1990s, *The Lipman Report* editors published several articles on the growing domestic threat, as demonstrated by the Unabomber attacks and the Oklahoma City bombing. Both of these instances demonstrated yet another evolution in the terrorist threat: the lone wolf. Law enforcement cannot infiltrate a cell and prevent future attacks if only one person is privileged to the information.

The September 1995 report described two salient features as characterizing the new terrorist threat. The first was the growing tendency for terrorist groups to become clandestine. In the past, these organizations often publicized their attacks to gain publicity and leverage for their political demands. This combination of overt denials and covert activities has made it increasingly difficult to detect terrorist operations in the United States. Second, until just recently, domestic groups that have demonstrated a dangerous paranoia dominated the terrorist threat in this nation. Of 12 terrorist acts committed in the United States in 1993, nine were perpetrated by animal rights groups, two were committed by skinheads, and the twelfth was the World Trade Center attack.

In spite of these changes in the attackers' profiles, traditional response methods remained valid: Hardening building protection, upgrading technology and expanding the uniformed security presence continued to reduce the threat of attack. Other recommendations involved a more active approach on the part of security directors: developing an intelligence network, communicating with employees and community contacts, and identifying and implementing best security practices.

The December 1996 issue again focused on airport security, examining recommendations developed by the White House Commission on Aviation Safety and Security. The commission proposed a \$1.1 billion anti-terrorism plan, which included \$350 million for improvements to airport security. Recommended security measures—which were ultimately discarded because of budget issues—included broader installation of explosives-detection machines, a full bag-to-passenger match for domestic flights, and development of an automated passenger profiling system that would combine information already available in a variety of databases to identify passengers believed to pose a security risk. The plan also called for more thorough background checks of all airport and airline employees, as well as for more uniform standards at the country's roughly 450 commercial airports. Implementation of these measures could well have tightened aviation security sufficiently to thwart the terror attacks of September 11, 2001, but again, budgetary concerns prevailed, sending security initiatives to the back burner until the next crisis.

In March 2001, *The Lipman Report* outlined recommendations from *Roadmap for National Security: Imperative for Change*, the report of the U.S. Commission on National Security. Led by former senators Gary Hart (D-Colo.) and Warren Rudman (R-N.H.), the commission tendered the following warning: **“The combination of unconventional weapons proliferation with the persistence of international terrorism will end the relative invulnerability of the U.S. . . . to catastrophic attack. A direct attack against American citizens on American soil is likely over the next quarter century.”** The publication described the report as “a call to arms”: **“The U.S. could face another Pearl Harbor, but the surprise attack this time would target cities and civilians. . . . Mass-casualty attacks on U.S. soil could undermine U.S. power and prestige, which is what terrorists want.”**

(continued on next page)

A quarter century of vision

The Lipman Report reflects on a successful history

(continued from preceding page)

This newsletter cited Central Intelligence Agency Director George Tenet, who had testified before the Senate one month earlier that Saudi exile Osama bin Laden's global network represented **"the most immediate and serious threat"** to U.S. security. At the time of the issue's publication, four members of bin Laden's al Qaeda network were on trial in New York for the 1998 bombing of two U.S. embassies in Africa, and bin Laden had recently praised the attack on the *U.S.S. Cole* in Yemen, also suspected to be the work of al Qaeda. The editors warned that the next attack could take place on U.S. soil, and less than six months later, it did.

The Lipman Report editors turned their attention to biological warfare in July, August and September 2001, a few months before refined anthrax spores appeared in the U.S. postal system, courtesy of an anonymous perpetrator who has eluded law enforcement to this day. The newsletters described inadequacies in the U.S. public health system and in the nation's overall ability to respond to a bioterrorist attack. As one example, the August edition pointed out that, even though anthrax was widely regarded as the greatest threat as a biological weapon, the nation had depleted its supplies of vaccine. Pharmaceutical companies were reluctant to devote resources to producing and, in some cases, developing vaccines and antibiotics to counteract remote, hypothetical threats—threats that materialized in October 2001.

During the last year, the country has dramatically improved its biological defense program, stockpiling smallpox vaccine and emergency "push packs" of vaccines and medications for immediate deployment in the event of a biological attack. This progress demonstrates how quickly the nation can act on this front, although much work remains before the United States can effectively respond to a successful, coordinated assault.

The report has focused exclusively on the continuing terrorist threat in the year following the

September 11 attacks, recommending security initiatives for both the public and the private sectors. While the government has a significant role in protecting the American people from terrorists, private industry must also accept greater responsibility to protect their human assets. The 2001 attacks brought the threat to a new level, targeting civilian men and women en masse. As a result, businesses must exercise greater vigilance to safeguard their employees against this now-omnipresent danger.

Violence in the workplace

Decades before office shootings became recurring features in the national news, *The Lipman Report* warned organizations of the mounting risk of violence in the work environment, from schools to hospitals to office buildings. As reiterated by the recent classroom shooting by a university student, violence in schools continues to be a threat for teachers and students alike—often creating a stressful work environment for adults and a traumatic learning environment for our nation's youth. The August 1979 issue of *The Lipman Report* noted that: **"The increasing problem of school violence, which results in about 100 deaths every year nationwide, has prompted one state to consider requiring special anti-violence training for principals and supervisors."**

Despite the continuous recommendations put forth in the newsletter, however, many facilities still lack adequate security measures to deter would-be assailants. In December 1985, the report urged security directors to take action against the "epidemic of violence" in the United States. **"As a result of this epidemic and its impact on the working environment, the standard approaches to reducing violence are being challenged. . . . It is increasingly vital that security management personnel explore sources of information and link up with individuals in their own organizations and communities to facilitate their participation in the new health care strategies aimed at dealing with this epidemic of violence."** Citing grim statistics, the report urged the implementation

of such measures as education programs to raise management's awareness of the threat and employees' ability to resolve conflicts and recognize potential problems; written policies for violence prevention; and a hotline to provide intervention or victim assistance.

The need for such steps grew increasingly evident throughout the 1990s, when workplace violence became firmly entrenched in the corporate lexicon. The May 1992 issue specifically addressed the threat of violence within hospitals. **"More and more, hospitals are sites where crimes occur rather than safe haven for victims of crimes that occur elsewhere."** Many of the recommendations for increasing physical security, however, applied equally well to health-care facilities or office buildings alike, including the use of employee photo-identification badges and a limitation on the number of entrances and exits, all of which should be monitored.

During the next 10 years, *The Lipman Report* repeatedly called for a heightened awareness of workplace violence and preventive tactics to help ensure the safety and security of an organization's employees and visitors. Detailing the high costs of workplace violence incidents, from loss of life to decreased productivity and morale, the September 1992 report identified an employer's responsibility. **"The time has come for business to protect the security of its personnel as conscientiously as it protects the security of its products, its property, and its proprietary information."**

In an effort to assist organizations in fulfilling this duty, the newsletter offered suggestions for implementing a strategy to help prevent violence in the workplace. The guidelines offered in the March 1994 issue prove just as effective today: conducting comprehensive background screenings on applicants to reduce the risk of employing a violent individual; escorting visitors to the facility at all times; enacting safe termination guidelines such as scheduling them late in the day and having those who terminate employees

learn counseling techniques; collecting identity badges and keys from terminated employees; and creating a threat management policy to help resolve conflicts before they erupt into violence.

The newsletter has also provided valuable information on recognizing characteristics often demonstrated by a perpetrator prior to a violent incident. In the July 1995 and August 1997 issues, for example, the report listed several warning signs, including a history of conflict; difficulty accepting criticism; depression or withdrawal from social contact; fascination with weapons; expressed approval for violent situations; domestic problems; too great a reliance on one's job for personal identity; and deterioration in work habits, health or hygiene.

In addition to disgruntled employees carrying out a grudge, violence in the workplace may also stem from domestic disturbances that follow an individual to the job. As noted in the March 1998 edition of the newsletter, **"Corporate America is concerned because domestic feuds do not vanish at the office door."** The report urged employers to look for clues that might indicate patterns of abuse or stalking involving an employee and to provide assistance by distributing educational materials, offering information on counseling and enacting security measures to reduce the risk of violence within the workplace setting.

Security directors must recognize the threat of workplace violence, utilizing careful employee selection procedures, implementing stringent physical security, and instructing managers and security officers how to detect and deter a potential threat. Violence in the workplace poses an ongoing concern for any organization. The July 2001 report pointed out that such risks place a burden on security professionals that they cannot afford to ignore: **"The strategies corporate security directors propose and the forces they deploy help determine whether employees, customers and property are safe and whether investors are confident."**

(continued on next page)

A quarter century of vision

The Lipman Report reflects on a successful history

(continued from preceding page)

Computer crime

The Lipman Report has targeted the evolving problem of computer crime since November 1978, when corporate America employed only an estimated 150,000 commercial-scale computers. At that time, the newsletter focused primarily on the need for strong internal security as dishonest employees presented the single greatest threat to a computer system. Primary vulnerabilities included the following: entry of false information, unauthorized use of computer facilities, alteration or destruction of files, and theft. The editors warned, **“The ‘computer age’ has brought rapid advancement to business, and to society in general. Accompanying the advancement, however, is the potential for enormous losses carried out by illicit use of the computer.”** Over the next 24 years, *The Lipman Report* emphasized the need to exercise caution when embracing the enhanced productivity afforded by technology, incorporating appropriate security measures with each step.

The November 1983 issue cited two incidents that illustrated the potential magnitude of computer crime. In one, a computer consultant noticed a funds transfer code taped to a wall in a bank’s wire transfer room; he left the building, arranged the transfer of more than \$10 million to a Swiss account, and converted the money into diamonds before the bank detected the fraud. In the second, a bank officer used his computer terminal to juggle more than 80 separate accounts, resulting in a loss of more than \$21 million to his employer. The stakes have grown in the last two decades, as computers have become ubiquitous and the knowledge required to manipulate technology is no longer a specialized commodity. Consequently, *The Lipman Report’s* advice of implementing a three-pronged approach to computer security—personnel security, physical security and technical security—holds true in an even more critical way today.

“Statistics about computer crime are hard to come by, because few corporate victims want

the public embarrassment occasioned by reporting computer crimes to the appropriate authorities.” These words appeared 17 years ago in the September 1985 report. This newsletter raised the vulnerability—still prevalent today—that arises when security managers have no jurisdiction over computer-related operations beyond the physical security of the computer facility itself. The editors noted, **“It is essential that the security functions in a computer facility be assigned to a security officer who is at least as knowledgeable in the systems, programs and functions of the data processing facility as the operations staff.”**

In November 1988, 10 years after the publication began coverage of computer crime, the estimated annual loss from computer crime had grown to \$200 billion. Naturally, the new computer-literate society proportionately increased the risk faced by businesses that had become dependent on the technology. The average known computer crime netted \$500,000, compared to only \$23,500 for the average white-collar crime and \$250 for the average armed robbery. Despite the many changes in technology and the myriad ways in which clever individuals learned to abuse computers for personal gain, basic premises of computer security remained solid: careful personnel screening, appropriate technological defenses and organizational awareness of the risks faced.

Computer security recommendations in *The Lipman Report* focused on individual actions during the 1990s and up to the present day, reflecting the fact that the widespread usage of computers at every level gives the power to abuse—and to protect—to virtually every employee. As a result, every person has a responsibility to contribute to the company’s overall computer security program by adhering to certain guidelines. Examples of these security procedures include password protection, backup and file deletion protocols, appropriate disposal of hard copies, and secure labeling and storage of sensitive files.

In recent years, these guidelines have expanded to address the special challenges presented by the prevalence of Internet connectivity and laptop computers.

The July 1996 issue, for example, addressed the dangers of exposing an organization's internal network to the Internet, acknowledging the potential productivity gains while recommending practices to reduce vulnerability to both outside attack and internal abuse. The newsletter offered specific instructions on developing and implementing an enforceable computer security policy, as well as on protecting the network through a combination of technical solutions and sound security procedures.

The Lipman Report first discussed the growing problem of laptop computer theft in October 1997, an issue that has steadily increased in prominence as the machines become smaller and more valuable—due to both the hardware itself and the information contained within. This report and subsequent issues offered behavioral guidelines and technological solutions to combat this issue, which costs U.S. businesses more than \$1 billion a year in hardware loss alone.

Employee Drug and Alcohol Abuse

The second issue of *The Lipman Report*—December 1977—proclaimed on-the-job drug abuse to be **“certainly one of the fastest growing, most publicized, but least understood crimes confronting American business managers. Like alcoholism, it too often is ignored or goes undetected until it becomes a serious problem. Sound business practices dictate that managers be alert to drug and alcohol abuse and stop it whenever it occurs.”** Citing injuries, liability issues and economic concerns for businesses, the report urged employers to engage in rigorous pre-employment screening to reduce exposure to drug-related losses.

In April 1978, the newsletter reported a case in which employees and a security guard collaborated in a plan to steal company property and to

sell drugs to their peers at the plant. After an outside investigator provided the company with details of the situation, employees engaged in the practice were fired and stronger controls were implemented. **“Management also hired a new guard service, which more carefully investigated and screened its guards.”** *The Lipman Report* recommended careful screening on countless occasions over the years, not only in response to drugs in the workplace, but also to alleviate other security concerns.

During the next four years, the monthly report addressed this persistent topic six more issues, providing business executives with insightful information on the problem. Readers benefited from coverage on symptoms of drug and alcohol abuse, the costs incurred by an organization in which abuse ran rampant, and shifting trends in drug use. The September 1982 issue reiterated the prevalence of drug use in the workplace and its detrimental effect on business productivity. **“In a typical large or medium-size company, drug abusers average 3% to 5% of the workforce. At first glance, this small percentage may seem relatively innocuous, but the impaired performance ability of even a few workers can create enormous potential for losses to the company.”** More than 20 years later, that potential can still threaten the success of an organization.

With the release of the President's Commission on Organized Crime recommending drug testing for employees, the April 1986 edition of *The Lipman Report* advocated the practice—a stand the editors maintain to this day. **“The inability to depend on government at all levels to control the drug problem has forced companies to manage the problem themselves.”** The newsletter emphasized, however, that using such measures as part of a pre-employment screening process presented a more advantageous solution than attempting to expunge drug use among the employee population. **“Catching the problem at the door is much simpler than trying to eradicate it later.”**

(continued on next page)

A quarter century of vision

The Lipman Report reflects on a successful history

(continued from preceding page)

Ongoing random testing, while debated on the grounds of privacy issues, provides the added benefit of discouraging future drug use among employees while removing existing users from the work force. **“The usefulness of drug testing is much greater than the recognized value of indicating employees who are currently using or have recently used illegal drugs. The belief of employees that they may be tested at any time has great deterrent value.”**

Revisiting these incessant problems several times during the next six years, the report continuously underscored the need for drug-testing programs. Such programs grew in prominence during this time, as noted in the November 1992 issue. **“In 1981, three percent of companies polled by a human resources management journal tested their employees for drug use. By 1990, 59.8 percent of the nation’s largest employers had instituted drug-testing procedures. The numbers have grown because testing works.”**

Support for drug testing continued to mount along with emphatic recommendations by the editors of *The Lipman Report*. In March 1993, the newsletter offered detailed guidelines for establishing and implementing an effective workplace drug-testing program. **“An optimum drug-testing program should be mandatory, universal and random.”** To ensure fairness and effectiveness, the test should be “mandatory” (all employees are obligated to consent and cannot refuse the test without risk of termination), “universal” (administered to everyone from entry-level positions to executives) and “random” (ongoing subsequent tests conducted on employees chosen by chance). The report also stressed the need for small and mid-size businesses to consider the recommendations seriously. **“As more and more of the nation’s larger companies require drug screens for job applicants, drug-abusing applicants target smaller organizations that may not yet have initiated comprehensive drug testing programs.”**

In the late 1990s, drug use was beginning at an increasingly young age, creating a surge in the number of abusers entering the workforce. The variety and potency of drugs intensified as well. The September 1999 issue suggested steps beyond a comprehensive drug-testing program. **“Drug users in the workplace annually cost employers up to \$100 billion in lost productivity, increased medical costs, theft and resultant extra security measures, destruction of property and job turnover.”** To combat this problem, employers were encouraged to create a written, publicized policy citing zero tolerance for violations; to instruct security personnel and employees on the warning signs of substance abuse; and to write a security plan outlining how suspected drug users should be handled. The February 2000 report also recommended that companies seek professional assistance from organizations such as the U.S. Drug Enforcement Administration in developing an effective drug-free workplace program.

During the last 25 years, we saw the end of the Cold War. During the next 25 years, the challenge will be even greater than the threat of nuclear destruction. We live now in a period that bears similarities to the feudal society of the Middle Ages. The war between the haves and the have-nots will not follow Geneva conventions. The risks to individual institutions, organizations, companies and countries are greater than ever—all the more reason to focus on national security with all the means that we can bring to bear. For those who are complacent or who follow the pattern of not learning the lessons presented earlier in this issue, the consequences will be great. The world is not a nice place, and those who will live long into the 21st century must be vigilant.



The Lipman Report Editors