

January 15, 1999

## Securing Vast Gains; Avoiding Vast Dangers

### Business Concerns for the New Millennium

*In the history of mankind, profound societal transformations have been rare. In the Ice Age, human existence was nomadic and isolated. Hunting was the primary work. Then, in the Age of Trade, communities began to be established. Our ancestors farmed, raised animals, and began to interact along fixed routes. In the Age of Discovery, explorers spread the influence of their empires around the globe. In the Age of Industry, the invention of machines and processes increased production. Each new frontier was intimately connected with the concept and practice of work, and in each instance, the elapsed time from one great transformation to the next became shorter and shorter.*

*Now society has entered another new age—the Age of information. Once again, powerful forces are transforming economies, politics, and societies. And they are transforming business from a production-based economy, founded on land, manufacturing plants, and labor, to a knowledge-based economy, founded on ideas and communication. In 1975, an intellectual property expert stated, more than one-half the value of all Fortune 500 companies “was attributable to tangible assets. By 1995, that figure had dropped to about 25 percent.” Of the intangible assets now in the majority, more than on-half are some form of intellectual property.*

*As corporate America prepares to embark upon the journey into the new millennium, an awareness of the forces propelling it forward will make the journey safer and more successful. Some of the trends cited in this issue of The Lipman Report already are affecting business health and security; others are predictions for the future. Speed is the hallmark of them all. And readiness begins with a careful consideration of their implications.*

### Information age gains

Across virtually the entire spectrum of American business, the technologies of the information age have spurred innovation, productivity, and growth, and boosted revenues at the fastest rate since World War II.

Law enforcement uses new DNA technologies and giant computer databases to identify criminals. Medical practitioners use new technologies to diagnose, treat, and monitor patients. Researchers in basic sciences use new technologies to manipu-

late genes for the development of new drugs, to grow human tissue, and even to clone living organisms. Industry uses new technologies to improve design, manufacture, and transportation of products, to streamline inventory and retailing operations, and to fine-tune personnel scheduling. Agricultural engineers use new technologies to boost yield, nutritional value, and disease resistance of crops. Banking, finance, government, education, the environment and a host of other fields depend heavily on computer technology. In the not-so-distant future, scientists predict that microelectronic systems will predict earthquakes, warn of disease, and even mimic nature by creating matter, atom by atom.

The potential for profits that rival any in history is another benefit of the new age. Four of the nation's five wealthiest people are technological entrepreneurs. They and others like them have helped to create the technological explosion that is fueling the U.S. economy and altering society.

### Information age dangers

The unprecedented opportunities often hold within themselves the seeds of vexing problems.

One problem relates to **globalization**. Although usually considered an advantage, globalization has resulted in greatly intensified competition. Everyone, everywhere has access to the same markets, accelerating the demand for raw materials, labor, and ever new technologies to move products and services. Because the potential rewards are so great, the nature of the quest has changed. Economic rivalries have acquired military overtones. Companies engage in commercial warfare and “capture” market share. Industrial espionage has become an expected strategy. The Lipman Report for September 1998 addresses protection of intellectual property.

Globalization, too, makes distant problems our own. The performance of U.S. firms frequently is affected by political or financial upheavals abroad.

(continued on next page)

---

## Securing Vast Gains; Avoiding Vast Dangers

### Business Concerns for the New Millennium

(continued from preceding page)

Another peril relates to the **declining role of governments and the protections offered by them**. In particular, the regulatory role of government is diminishing. "Transnational enterprises," says a noted authority, "have increasingly usurped the traditional role of the state, and now exercise unparalleled control over global resources, labor pools, and markets." The Internet, which has revolutionized communication and is in the process of revolutionizing trade, is virtually ungovernable.

The power of central governments as a guarantor of justice is likewise diminishing. More and more, corporations must look after their own security and well-being. U.S. laws protecting intellectual property already are ignored or circumvented by other nations. American manufacturers, unable to halt the unauthorized replication of their products, lose billions each year to pirates.

An increased awareness of security risks conferred by such recent high-profile terrorist incidents as the bombings at the U.S. embassies in East Africa and the declining ability of governments and law enforcement officials to meet demands for protection, have fueled growth in the private security industry. By the year 2000, projections indicate that private security officers will outnumber public law enforcement officers by a ratio of three to one. This trend creates yet another problem. Because private security services are purchased primarily by those with resources, their growth underscores the emergence of a dangerous new gulf between haves and have-nots.

**Cybercrime** is another serious concern. Just as business uses sophisticated technologies to increase production and profitability, so criminals use sophisticated technologies to perpetrate costly and dangerous frauds. In a recent case, two men in St. Petersburg, Russia, broke into a major U.S. bank system and electronically transferred to their own accounts more than \$10 million in funds held by corporate clients of the bank.

Because many organizations do not know they have been victimized, crimes often go unreported for months. Those that are detected are believed to be the tip of the iceberg. To combat this growing danger, in September the International Chamber of Commerce (ICC) and Interpol set up a cybercrimes unit to help companies worldwide. *The Lipman Reports* for May, June, July, November and December 1998, address wire transfer fraud and computer crime.

**Terrorism** has become an increasingly insidious and pervasive threat to individuals and companies. As new technologies place unprecedented power in the hands of small bands of criminals, the worst may be yet to come. Highly mobile, contemptuous of international laws, terrorists use computers to plot attacks efficiently, invisibly, and globally. Blurring distinctions between crime and war, a single "martyr" for any of myriad extremist causes can disable fragile network upon which business and the world depend for information and energy. "In cyberattacks .....", says an authority on catastrophic terrorism, "the deployment of weapons can be entirely electronic." *The Lipman Reports* for January, February, April, and August 1998, address terrorism.

**The millennium bug, aka the Y2K problem** is another concern. Unless they are updated, computers in which the date is programmed with the last two digits of each year instead of the entire four-digit number, may interpret the digits "00" as the year 1900 instead of the year 2000. The very real dangers of this condition range from the inconvenience of a stalled elevator or temporarily inaccessible bank account to the catastrophe of malfunctioning life support equipment, failed air traffic control systems, or accidental nuclear war.

Corporate information technology systems are particularly vulnerable. Because few businesses operate today without some computerized functions, failure to ready the systems for the year 2000 threatens to seriously affect corporate per-

formance. But readying the systems poses additional security problems as institutions allow unprecedented access to computers containing vital information. A programmer working with computer source code can easily insert a "trap door" through which he or she can later return to steal information, alter records, or transfer money. Additional concerns about sabotage and espionage stem from the fact that a significant number of system upgrades are being performed by programmers in India, Pakistan, Ireland, and the Philippines, countries which harbor active anti-American groups. Indeed, the Philippines was an operations base for associates of Osama bin Ladin, thought to be the mastermind of last summer's U.S. embassy bombings in East Africa.

Other high tech-systems are vulnerable as well. Pre-programmed computer chips, difficult to access and re-code, are embedded in a wide variety of equipment vital to the operation of an enterprise. Virtually everything electronic is controlled by microchips. Security systems, closed circuit TV monitors, time clocks, elevators, climate control apparatus, power supplies, telephones, fax machines, postage meters, inventory control systems, and machinery that is serviced at regular intervals, among many others, could be hobbled. A U.K.-based supplier of millennium software says that as many as ten percent of small- and medium-sized firms "will go into liquidation as a result of system failure."

Another danger inherent in the Y2K dilemma lies in the fact that both sides of the communication process must function properly. If the business supplier has a problem, the client has a problem, and vice versa. U.S. officials are seriously concerned that financially stressed Southeast Asian and other developing nations, governed by lower standards of disclosure than U.S. firms and lagging behind in addressing the problem, could impact U.S. businesses. One U.S. law firm is advising its clients to insist that their suppliers certify that they are Y2K compli-

ant and that they will be able to fill customers' orders. The firm is cautioning its clients to verify that the certification is provided by *bona fide* experts in Y2K technology. One large U.S. automaker is so worried about compliance by its supplier network that it has begun to stockpile key parts and line up alternate sources.

Although we now enjoy a full-employment economy, **unemployment** is a growing peril. According to an internationally known author on economic trends, the new markets and new jobs created by the emerging knowledge sector "will be far too few to absorb the vast numbers of workers displaced by the new technologies."

Business is affected in two ways. The first is that higher unemployment means shrinking markets. Near worker-less factories and virtual companies yield populations unable to buy products and services. The second is that the growing ranks of unemployed create a more dangerous, unstable society. An expert on economic trends cited above warns that "reduced wages, steadily rising unemployment, and the increasing polarization of rich and poor [are] turning parts of America into an outlaw culture." As wealth and power are concentrated in the hands of a smaller and smaller elite, the nation faces all the problems of a war between haves and have-nots. Businesses and communities must focus intently not only on finding productive work for the unemployed, but also on matching them with appropriate positions.

### **Meeting the challenge**

As noted, previous issues of *The Lipman Report* detail specific strategies for coping with some of the problems described above. Security professionals should call attention as well to the following areas.

For the near term, business must adopt a sense of urgency. Historic periods of change are compressed. All but the most nimble and best

**(continued on next page)**

## Securing Vast Gains; Avoiding Vast Dangers

### Business Concerns for the New Millennium

(continued from preceding page)

informed will become also-rans in the dizzying race to exploit technology. Security must become more proactive. Security professionals must help management to anticipate change, to discern problems, to seize opportunities. Management in turn must offer to security professionals the support and attention they need. Together, they must begin now to prepare for the rapidly approaching tomorrow.

Management also must check and re-check. It must evaluate the effectiveness of corporate protection on a regular basis, and update or revise coverage in a timely manner. Older equipment requires special attention. Is the manufacturer still in business? Are knowledgeable technicians still available? Can the items be updated? If "no" is the answer, consider replacement. Recognize, too, that suppliers and vendors are integral components of each business network and try to ensure that their operations function smoothly. Offer help where appropriate and make backup plans just in case.

For the longer term, business must take its place in the vanguard of those who know that a healthier society yields healthier profits. It must support initiatives that make a difference to communities. Education, ethics, and volunteerism are three.

Education is the capital of a strong and prosperous enterprise. Beginning with primary grades, business must advocate for school reforms that not only impart quality learning, but that emphasize the connection between educational attainment and personal success. Relevant education is particularly important. Business must continue to emphasize the diminishing availability of blue-collar work and the need to prepare students for high-tech jobs. At least 29 nations in the world, says an education leader, "require four years of technical reading and writing . . . to graduate from high school." These nations are our competitors. Some U.S. states do not even require one day of such training.

As respect for law declines and as individual power grows, the need for minimum ethical standards becomes ever more urgent. Business must work to ensure that responsible citizenship becomes an integral part of every curriculum. Students must be taught the need for ethical behavior, for stewardship of our institutions and resources, for tolerance of diversity, and for the kind of honesty that begets trust. Business, likewise, must model such principles in all its transactions. Ethical behavior is not a burden; it is a magnet for commerce and profits.

The development of a third sector, known also as a volunteer or independent sector, is a time-tested approach to looming social problems. Volunteers often served as the glue that held American communities together in trying times. They again can help to shape and cushion the American experience as we confront the perils of the millennium. As employment shrinks and governments reduce spending for social programs, business must encourage the establishment of a third sector to alleviate social ills and to harness the talent and energies of millions of displaced workers.

*Corporate security is not simply the defense mounted by an organization, not simply what it does to keep out of harm's way or how it reacts to adverse circumstances, although these are standard components of a protection plan. Corporate security is a combination of many factors that create an effective and harmonious whole, and that in turn can yield a stable, secure, enduring, and profitable enterprise. It is corporate leadership of the most effective sort. It is an ability to read societal trends and translate them into action to secure the future.*



The Lipman Report Editors