

February 15, 1998

## Terrorism in Cyberspace

### Presidential commission uncovers vulnerability of national infrastructure

*The telephone system in Dallas malfunctions. Chicago and San Diego bankers find their largest corporate accounts missing from the database. An electrical grid glitch blacks out Los Angeles. The Internal Revenue Service loses taxpayer information from New York.*

*Without fatalities or a note claiming responsibility, if these computer scenarios were real they might be dismissed as coincidence and it could be months before they are identified as part of a cyberattack on the infrastructure of the United States.*

*The United States is unprepared for such a cyberattack, according to The President Commission on Critical Infrastructure Protection (PCCIP). The commission spent 15 months studying the physical and cybersecurity of the nation's transportation, gas and oil, water, emergency services, banking and finance systems, government services, electrical power, and telecommunications—eight areas of the nation's infrastructure primarily owned by private industry.*

*The commission concluded that computerized interaction within and between these eight areas is so widespread a cyberattack could wreak havoc with the nation.*

*The PCCIPs work outlines ways private industry and the government can protect essential services. Some of these recommendations are also contained in issues of The Lipman Report on network security (February 1996), internal computer threats (February 1997), and intrusion via the Internet (July 1996). However, the commission report in October 1997 is the government's first coordinated effort to deal with infrastructure security.*

### New Tools, New Risks

A French computer hacker is fined and given a suspended 18-month jail sentence for breaking into an FBI computer system and charging \$250,000 worth of calls in 1996.

Experts in computer security estimate companies worldwide—especially banks and hospitals—lost more than \$800 million in 1995 to computer trespasses.

Given such costly estimates of computer-based losses, it should come as no surprise that security in cyberspace was the number-one technology issue for business in 1997, according to a poll

conducted by the American Institute of Certified Public Accountants. Increasingly, business and government leaders realize that the cyberspace tools operating a safe, cost-effective, reliable infrastructure are the same tools that can be used to destroy it.

Today, the United States is the nation most dependent on cybertechnology for the day-to-day operation of its most vital services. Figures from PCCIP show nearly half the world's computer capacity and 60 percent of its Internet assets are housed in the United States.

In 1996 when 400 million personal computers and 32 million Internet access devices existed, the figures compiled by the PCCIP showed 17 million people in the world had the skills to launch a cyberattack against essential services. By 2001, when 500 million personal computers and 300 million Internet access devices will exist, 19 million people will have those skills.

### Impact of the Report

Cyberspace security experts predict the commission's report will have four positive impacts. It will:

- Raise the national awareness of cybersecurity problems;
- Begin the cyberspace security research and educational processes that are essential for long term and lasting solutions;
- Herald an era of cooperation between segments of government and private industry;
- Start the laborious process of changing outdated laws that hinder the investigation and prevention of cyberintrusion. For example, today it may be necessary to solve the cybercrime before it is possible to determine which agency of the government should investigate it.

Among the laws and regulations that need changing are those governing freedom of information

**(continued on next page)**

---

## Terrorism in Cyberspace

### Presidential commission uncovers vulnerability of national infrastructure

(continued from preceding page)

and a company's privacy. Tighter controls on what information is open to the public might help convince companies to be more forthcoming with information about intrusions.

Creating a more secure cyberspace means breaking down the code of silence that protects private industry and government from embarrassment. Victims used to keep a breach in cybersecurity secret. The public only learned of the cybersecurity problem if the intruders were caught or if the nature of the problem caused inconvenience to a large number of people. For example in the last few years the public learned: two hackers re-routed 911 emergency calls in northern Florida to the White House; an angry student flooded Monmouth University with 24,000 e-mail messages and crashed the system; a Russian stole millions from a New York-based bank without leaving his country.

However, most of the nation's cybercrimes still go unreported, so it is difficult to determine who the attackers really are and how they operate. A 1997 report from the Computer Security Institute (CSI) in San Francisco shows only 17 percent of private companies reported cybercrimes to law enforcement. Yet 75 percent of the 563 companies responding to the CSI survey admitted financial losses due to computer security breaches last year.

Most frequently, cybercrime is not reported to avoid bad publicity or to prevent exposure of company operations. The commission calls for raising the level of cooperation between law enforcement and private industry so that computer intrusions and related thefts are reported routinely.

Citing the need for accurate information on the nature and frequency of intrusion, the presidential commission recommended bringing laws related to investigative authority, liability, fair business practices, trade secrets, proprietary information and Freedom of Information classifications into the computer age. Laws should make it easier for

companies to report and cooperate with investigating authorities without exposing themselves to risk or ridicule.

Only when private industry and the government understand the nature and scope of the problem can trustworthy security measures be developed and adopted. The commission considers accurate information on the cyberattacks to be extremely important, particularly to the creation of an early warning system and to the problem of detecting security breaches.

So far the detected security breaches have been costly, but no more than inconveniences. For example, the U.S. Defense Department has suffered 250,000 intrusions into its systems with lasting damage. In 1994 the Internet Liberation Front hacked into the computers of NBC, IBM and General Electric to leave warnings about Internet restrictions. Until information is shared and a warning system implemented, the United States' infrastructure will be vulnerable to a coordinated attack.

#### New Thinking

Cooperation between government and private industry in the prevention, detection and apprehension of cyberintruders requires a paradigm shift. In the past, private industry and government wrestled over such issues as privacy, proprietary information, and control of computer encryption keys. To attain security in cyberspace, some measure of trust must be exacted from both sides and these issues resolved.

Only owners and operators of the eight areas of vital infrastructure have the knowledge, access and technology to defend their cybersystems. Only the federal government has the legal authority, law enforcement capability, intelligence resources and research dollars needed to ensure the safety of the nation's infrastructure. Our sources indicate that law enforcement, like private industry, lack the technological tools as well as the legal

---

tools needed to handle cybercrime. For example, thanks to the development of fiber optics and the lack of legal direction in defining how and what can be tapped, law enforcement cannot tap the telephones in any section of the country that uses fiber optics in telephone transmissions.

Industry officials are pleased by the tone of the PCCIP report and see it as a necessary first step toward cooperation. "What impressed us most was the report recognized the need for private industry leadership. It is significant the commission did not mandate government regulation or standards for networks or technology," said a technology industry official.

The report suggests cooperative ventures in setting standards for security software and hardware. The commission also calls for the nationwide licensing of private security specialists by professional organizations or the government. The growing necessity for outside computer security personnel makes the new business ripe for corruption. One of our sources said the most lucrative criminal activity he can imagine now is to form a cybersecurity company, install security software on company computers that has a gateway encoded in it, then milk company assets or proprietary information at one's leisure.

Cyberspace security software certification programs do exist in the private sector and more are being developed. For example, the National Computer Security Association offers certification for certain products such as a secure vendor program to reduce risks associated with the exchange of sensitive data between companies and vendors. However, no certification for software can assure the user that the program is 100-percent effective. The computer user must be responsible for monitoring and updating security programs.

### **Where to Start**

Incumbent upon each company, the PCCIP said, is adoption of its own set of risk assessment best practices. The commission suggested the following eight:

- Conduct an employee security training program integrating physical security needs with cybersecurity information.
- Authenticate the-identity of all users of the system and restrict access to only the authorized functions.
- Isolate critical operational control systems from all public and most internal networks or provide firewall software protection.
- Provide adequate procedural and technical controls to assure data integrity, to detect unauthorized change or deletion, and to recover data when necessary. One top cyberspace security expert recommends installing intelligent auditing software to notify management immediately of unusual activity within the system. He also suggests adopting a dynamic password system that constantly and randomly changes access passwords.
- Log and save the origin of all commands to change the operation conditions of the infrastructure.
- Create a Computer Emergency Response Team or similar group with the education and equipment to investigate intrusions, isolate and recover damaged systems, and restore services.
- Insure adequate back-up and recovery capability for programs and data needed for normal operations and customer service. To assure the availability of key control systems, information systems and data, consider redundancy, geographic separation of systems, firewalls, effective use of encryption, and other options.
- Conduct regular assessments of systems vulnerability and learn about new types of cyberthreats by consulting the expertise of the National Security Agency and other agencies. Learn about new techniques for attacking systems and assess if they can be contained by current protective measures.

**(continued on next page)**

## Terrorism in Cyberspace

### Presidential commission uncovers vulnerability of national infrastructure

(continued from preceding page)

The members of the commission concede no amount of training or vigilance on the part of private industry alone can prevent a cyber Pearl Harbor. However, government does have responsibility in the prevention, detection, investigation and prosecution of cyberattacks.

Therefore, in addition to its advisory, legislative and investigative role, the commission recommends the federal government allocate billions of dollars over the next five years to education and research and development. The education funding would attack the computer problem at the root with computer ethics programs for school children and at the prevention level with information assurance training for university students and advanced security training for specialists.

#### Prognosis

Unfortunately, indications from those in an inter-agency group working on the commission's report are that many PCCIP recommendations will never make it to legislation. One New York cybersecurity researcher holds that the commission report—particularly its education components—will be a key element in altering the way America survives in the Information Age. He believes the report will initiate nothing less than cultural change by beginning to change the mindset of the youngest members of society—a grassroots shift that is essential to a nation wishing to protect its critical infrastructures.

The leaping technological changes of the last few years require paradigm shifts in how government and private industry guard proprietary information. As a former FBI official said: "We used to think of the theft of things. Now the greater threat is the theft of ideas or information."

Businesses and governments must both realize information is an expensive commodity that needs protection. For example, in one 1997 incident alone, a hacker gained access to information

via a file server in a software developer's Texas office and stole codes to a computer game worth hundreds of thousands of dollars. The technology lost to a dishonest competitor cannot be retrieved by merely finding the culprit and putting the information back into a computer.

*Information and ideas are the lifeblood of business and government. Careless handling of valuable proprietary information can lead to more repercussions than stealing hard drives or computer chips or a safe full of money.*

*Businesses and the general public must learn about the dangers of computer theft, the ways intruders can enter a company's computer system, and must develop ways to protect what a company or government spent countless hours and many dollars to develop.*

*Education for the general public is vital to cyberspace security. But for company security directors, cybersecurity is of immediate concern and steps should be undertaken to develop a defense against intrusion. For example, companies might begin by adopting e-mail practices that make communication difficult to attack. Encryption and digital signatures required on e-mail are two techniques to investigate. A necessary first step should be the creation of a division within the security department which is responsible for cybercrimes within the corporation.*

*The presidential commission laid a strong foundation to build a more secure cyberspace for individual companies and the nation. The commission issued the warning; it is up to private industry to heed it. National security demands constant vigilance by business and government for the mutual protection of both.*



The Lipman Report Editors