

September 15, 2000

## Future Information Technology Threats

*The Lipman Report* editors examine the future of computer crime and security

*In the 1940s and 1950s, when the first computers were born, computer security was relatively simple: lock the door to the room and ensure adequate refrigeration. Since then, computers have rapidly evolved into such powerful machines that a new personal computer (PC) now has more than 100 times the computing power of its predecessors of only 10 years ago. These technological marvels have reshaped the modern world, enhancing people's lives in ways dreamed only by science fiction writers, and the wonders show no signs of ceasing—or even slowing. The same human creativity that makes such advancements possible, however, also invents ingenious methods of corrupting them for selfish gain.*

*Two well-publicized events this past spring reminded the world just how vulnerable it is to computer assaults. In February 2000, a group of hackers executed several distributed denial-of-service (DDoS) attacks within a matter of days, crippling some of the most prominent sites on the World Wide Web. A few months later, in May, a former student in the Philippines allegedly unleashed the notorious “Love Bug” virus, disabling computers across the world and causing an estimated \$10 billion in damage within the first 24 hours. Neither of these events required amazing technological skill; in fact, several tools exist on the Internet that allow amateur hackers to perpetrate the same type of mischief. But the severity of the incidents provided a dramatic wake-up call to the dangers that lie ahead.*

*The concern is well justified: As long as society commits billions of dollars to developing technology, individuals will continue to work equally hard at turning the results to their personal gain.*

*This special edition of The Lipman Report examines the current state of computer security and identifies potential problems and developments that could well come to pass during the next decade. In many cases the groundwork has already been completed; the world simply is waiting to see who will push the button.*

### Encryption

As computers become even more essential to daily functioning, the next decade will witness several important developments in the field of encryption. Organizations will rely increasingly on encryption technology to protect the proprietary information now stored on hard drives instead of inside locked

filing cabinets. Rapid advancements in technology, combined with the growing technological skills of the general population, will demand this additional layer of protection to shield valuable information from prying eyes.

One factor that will drive the encryption industry is the recent lifting of export controls on 128-bit encryption. Although this level of encryption has been available for several years, the U.S. government previously banned its exportation, lest terrorists and other criminals use it to hide their plans from intelligence agencies. The elimination of this barrier will encourage hardware and software developers to build stronger encryption algorithms—an essential element in the future of e-commerce.

Right now, 128-bit encryption represents the strongest level used by most commercial organizations, such as financial institutions. As early as 1998, however, encryption products have been available that use 4,096-bit algorithms. For scale, decrypting a message encoded with a 40-bit key would require more than one trillion guesses, using a brute force approach; a 4,096-bit key would take a number of attempts that is impossible to describe. Although some might consider encryption of such strength overkill, the amazing speed of technological advancement demands continuous innovation in this arena as well.

In 1990, top secret documents were routinely encrypted with 48-bit encryption technology. Brute force would require approximately 256 trillion guesses to break this level of code. For 1990 computers, such a task would have been virtually impossible, taking almost 11 years for a single machine. Today's computers could crack the encryption in a few short years, and within the next three years, the computers of tomorrow will reduce that time to a matter of months. Unless organizations take advantage of new developments in encryption to protect older files, they could expose themselves to an extraordinary array of risks.

**(continued on next page)**

---

## Future Information Technology Threats

*The Lipman Report* editors examine the future of computer crime and security

(continued from preceding page)

Furthermore, the threat will only increase as hackers exploit the rampant growth of the Internet to harness the powers of next-generation PCs and create supercomputers capable of defeating the most sophisticated defenses. Nearly half of U.S. households currently use the Internet, and the ranks of online citizens are swelling at the rate of 700 new households every hour. The growing prevalence of digital subscriber lines (DSLs) and cable modems will make it easier for hackers to hijack home and business systems for nefarious purposes; the continuous connection to the Internet affords hackers greater opportunity to infiltrate a system. The University of California at Berkeley uses this technological concept in its SETI@home project, which is part of the Search for Extraterrestrial Intelligence program. The project allows individuals to participate in the extraterrestrial search by installing a special screensaver on their home computer; the screensaver transmits information to the university via the Internet.

The world witnessed a negative example of such power last spring when hackers unleashed thousands of “zombie,” or “slave,” computers upon a handful of Internet giants, overwhelming their servers and shutting down their sites for several hours. The lack of a sure-fire defense against this type of attack makes it a formidable threat.

### Authentication

Along with encryption, authentication—the process of verifying an individual’s electronic identity—will also become a paramount issue. The next decade will witness a tremendous surge in the number of transactions conducted electronically, and users will require assurance that the party at the other end is truly who that person or organization claims to be.

Some companies and individuals continue to limit their online activities due to lack of confidence in Internet security, but each day, more and more bricks-and-mortar organizations

expand their operations online to meet the rising demands of electronic consumers. Financial institutions, for example, represent an industry that has taken a very conservative approach to electronic commerce, but several prominent banks are increasing their online options for corporate customers. The investment in online banking is projected to balloon from \$90 million last year to \$300 million by the end of 2003.

Initiatives such as the Electronic Signatures in Global and National Commerce Act, recently signed into law by U.S. President William J. Clinton, are removing many of the barriers that have previously kept e-commerce in check. The act, which was ratified last June, gives digital signatures the same validity as their ink counterparts, removing obstacles to using electronic technology in legally binding contracts. Several challenges still limit the viability of using digital signatures on a widespread basis—lack of a universal standard and the fraud risk of storing such valuable information on an insecure PC—but the online world will overcome them, changing the face of electronic communication and commerce.

As the use of digital signatures becomes widespread, many consumers will refuse to accept e-mail that is not digitally signed. This practice would enable users to virtually eliminate spam, or electronic junk mail, which currently floods electronic mailboxes; it would also provide protection against e-mail fraud and virus attacks. Both the “Love Bug” virus of last May and the Melissa virus of 1999 replicated themselves in e-mail messages distributed through users’ electronic address books; lack of a digital signature would alert recipients to a potential problem.

An effective digital signature system could have prevented the electronic publication of a fake press release last month. Unknown authors convinced the late-night production staff of an online newswire to release erroneous information that drove a company’s shares down 50 percent, resulting in a market capitalization loss of

---

as much as \$2.5 billion. The authors of the release, which was transmitted via the Internet, correctly followed the newswire's policies and procedures for submission, giving it the appearance of legitimacy. As a result, the story was picked up by two leading wire services.

### **The new face of crime**

Of course, not all the results of technological advancement will be positive. Society's increasing reliance on the Internet and computers in general will usher in a new era of computer crime.

**Manipulation of media.** While the newswire hoax represented a pure case of fraud, and not a security breach, the day will come when hackers decide to circumvent the wire service and simply change the front page of a national newspaper by breaking into the publication network. Such a feat can be accomplished in much the same way as the web site defacings that have plagued organizations since the advent of the World Wide Web. The perpetrators of today's online vandalism are teenagers, primarily interested in the technological challenge; as they get older, however, they will take a keen interest in turning their skills into profit—and not always by legitimate means.

**Next-generation bank robberies.** The growth of online banking will convince many bank robbers to ply their trade in the relative anonymity and safety of the electronic world. In August, British police arrested three individuals suspected of attempting a cyberspace robbery of an Internet bank. Although the loss to the bank was small—estimated at a few thousand pounds—the incident offers a presage of the security challenges to come as more criminals lay aside their guns in favor of a keyboard and mouse.

**Employee theft.** While insider theft has always plagued businesses, the widespread use of computers makes disgruntled or dishonest employees an even greater threat, in terms of the potential damage they can wreak. Instead of pilfering office

supplies or employer products, today's employees have the frightening potential to transfer millions of dollars to overseas banks for laundering. The increasing technological savvy of the average employee also raises the likelihood of using information technology (IT) systems for traditional crimes, such as corporate espionage, sabotage and extortion. British authorities arrested two men in London last August for allegedly breaking into a computer system in an attempt to extort \$200,000; one of the suspects was a contact for the victimized company in spring 1999, when it was providing database services to his organization.

**Internet piracy.** The current controversy surrounding Napster, an Internet-based system that allows users to share digital files of copyrighted songs, illustrates the difficulties that organizations are experiencing with modern piracy, a problem that will only worsen as technology continues to improve. As the recording industry attempts to shut down the popular Napster site, several companies are developing online music services that will give subscribers unlimited access to digital music files for a nominal monthly fee. The music files would employ special encryption to prevent the buyers from transferring the files via e-mail or a file-sharing network like Napster. "Corporate America is trying to control the uncontrollable Internet by owning it, but the reality is that it cannot be owned in the same manner as corporations have staked their claims in the past," says one expert.

### **Meeting the challenge**

To combat the technology perils of the future, organizations need to lay a strong security foundation now. Many of tomorrow's challenges can be thwarted with strict adherence to the protection principles of today.

Employee screening, for instance, will continue to play an integral part in an effective security program. Although companies will face an increasing

(continued on next page)

## Future Information Technology Threats

*The Lipman Report* editors examine the future of computer crime and security

(continued from preceding page)

number of threats from external sources, the greatest threat to their IT systems will still come from within: insiders who possess intimate knowledge of the systems and security measures are in the best position to exploit any weaknesses. At a minimum, organizations need to incorporate the following in their pre-employment screening: verification of work history, educational institutions and degrees earned; drug testing; confirmation of professional and personal references; and investigation of criminal records and, where applicable, military discharge status. *These same standards should also be applied to contract employees, especially those with access to the computer network, to decrease the possibility of third-party infiltration.*

Investing in the newest technology will also be a critical component of developing a strong IT security program, and the very nature of technology will require companies to upgrade their investment on a continuous basis. Just as software and hardware designers develop new methods of preventing unauthorized access, the criminal element constantly finds ways to defeat these safeguards. Any IT purchasing decisions should also include a security budget to protect those systems and applications. At the same time, companies cannot rely upon technology alone for protection. Network administrators must audit the system logs on at least a weekly basis to look for any suspicious activity. If unauthorized activity is discovered, the system logs could prove critical in identifying and apprehending the perpetrators.

Identifying and arresting an electronic intruder, however, will do little good if no legislation exists that applies to the crime in question. Last month, the Philippine justice department dropped charges against the individual believed to have released the "Love Bug" virus because, at the time of the act, the Philippines had no laws that specifically addressed computer crimes. The president of the Philippines signed

a new law in June that corrected this oversight, but the legislation did not apply retroactively to the alleged "Love Bug" author.

Organizations need to push for new legislation that applies to the threats of the Information Age. Piracy laws, for instance, should be updated to address unauthorized file sharing of films and music. According to one newspaper, the most recent James Bond film was available free on the Internet even before its official release in the theaters. The new laws must include appropriate penalties for individuals who use the new technologies for malicious purposes. Even more importantly, these laws must be enforced. The openness of the Internet facilitates sharing, making it easy for people with the appropriate technological skills to circumvent copyright protections or to transmit sensitive information. Private industry and law enforcement need to work together to create an environment that balances the protection of business and individual freedom.

*As advancing technology hurtles the world into a new era of computer dependence, governments and private organizations must move with equal speed to protect themselves from ever-evolving threats. Such action will require a combination of protective technology and adherence to traditional security practices, as well as new legislation that specifically applies to the challenges of cyberspace. Above all, the threats of the next decade will demand greater commitment to information security as a whole. Society's growing reliance on IT systems raises the stakes of a security breach at an exponential rate. Organizations that fail to make such a commitment now jeopardize their future.*



The Lipman Report Editors