COMPUTER SECURITY FACT SHEET

Companies' growing concern for security is not unfounded:

"I would move around the Internet asking myself: 'Who should die today?' And by 'die,' I mean cut off from the Internet."

Ehud Tenenbaum, the 18-year-old known as Analyzer told Jerusalem's *Yediot Ahronot.*

 " ... This was the latest "wake-up call" on the vulnerability of government and corporate computers to sophisticated search software owned by professionals and amateurs."

Deputy Defense Secretary John Hamre on the subject of recent hacker break-in on the US military computer system

Computer Crimes Growing

The FBI says that annual losses to US industries totals $63 billion from the theft of intellectual property stored on computers. The Computer Security Institute recently polled over 500 companies who reported losses totaling $236 million to saboteurs, viruses, laptop theft, financial fraud, telecommunications fraud and stolen proprietary information.

- Computer security breaches have risen 16% in the past year, according to a recent Computer Security Institute survey. The same survey found that 64% of organizations polled reported that they suffered a break in during the past 12 months.
- A recent survey of 1,000 large corporations by KPMG Peat Marwick in New York found that 41% of respondents said security concerns were the most significant barriers to their ability to do Web-based electronic commerce.
- Password files are stolen regularly thanks to hacker "kits" that are widely available and easy enough to deploy by novices who want to illegally collect account numbers and passwords.
- Firewalls may not help either: experts say 80% of the culprits are employees or ex-employees.

Increasing Number of Targets = Growing Security Market

Consumers are spending a bundle online, making them easy targets for credit card theft. The Yankee Group estimates that on-line spending for the 1997 holiday season was $800 million. Consumers spent a total of $2.74 billion last year.

While they freely use their credit cards online, not many consumers are willing to use the Internet to manage their bank accounts: 25% of US households have the ability to bank on-line -- only 7% have even tried it. Despite the convenience, users are concerned with security and reliability issues. So far, consumers are depending on businesses to provide the security to conduct online transactions.

- The market for computer network security products is $6 billion worldwide and is expected to double in size every year.
- Growth of corporate spending on security measures -- everything from firewalls, to digital certificates, to consulting services, is expected to compound 100% annually over the next four years.
- Investment bank Soundview Financial Group for example, predicts the marketplace will reach $1.1 billion in 2001.
- There are over 450 books in print and 650 web pages devoted to the topic of computer security

Corporations are installing Internets and extranets to connect an increasingly mobile workforce in need of remote access to corporate information systems. They're putting up direct sales sites to serve their business customers. This makes and companies more vulnerable to illegal access and computer crime. To safeguard their assets companies are turning to a number of security technology and service companies, as a result, the computer security industry market is growing just as rapidly as the crime rate.

- One area of security is emerging as an essential buy for any business: digital certificates and public key infrastructures (a.k.a. PKI). Digital certificates ensure that the parties in a transaction are who they say they are; a PKI manages those certificates, providing ways, for example to revoke them or recover lost passwords.
- Public-key encryption can save $5 million annually for a large corporation by lowering networking and help desk costs, according to Forrester Research.
- According to the 1998 CSI/ZONA Information Security Market survey, deployment of encryption products is on the rise -- 58% of respondents already use encryption in a variety of ways: 43% plan to buy encryption products in 1998

What's a PKI?
The comprehensive system required to provide public-key encryption and digital signature services is known as a public-key infrastructure (PKI). A PKI manages keys and certificates. By managing keys and certificates through a PKI, an organization establishes and maintains a trustworthy networking environment. A PKI enables the use of encryption and digital signatures services across a wide variety of applications.