

April 3, 2000

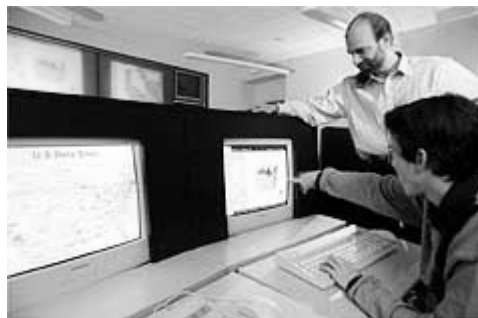
Beyond Computers in Computer Security

By JOHN MARKOFF

SAN FRANCISCO -- For all the power and complexity of modern computer networks, practical computer security against cybervandals may ultimately be found in the commonplace concept of a burglar alarm.

That is the notion of Bruce Schneier, one of the nation's best-known cryptographers -- people who specialize in writing and cracking secret codes. Schneier, who is a computer scientist and the author of a best-selling technical book, "Applied Cryptography," has recently transformed his small consulting practice into an Internet alarm company backed by venture capitalists.

Schneier's credentials include creating the Twofish encryption algorithm, which is a candidate to become the advanced encryption standard being set by the National Institute of Standards and Technology. So it may seem odd that a scientist who designs unbreakable mathematical locks for protecting information is calling on e-commerce companies to put mere people back in the computer-security equation.



Peter DaSilva for The New York Times

Bruce Schneier, left, and an analyst, John Crowley, at the offices of Counterpane Internet Security.

But Schneier argues that to trust the safety of information stored in a computer system to even the most powerful computer security software alone is foolhardy. That is why his new company, Counterpane Internet Security, has adopted a business model remarkably like that of ADT Security Services, the burglar alarm company.

"My basic philosophy is that technical protection mechanisms such as fire walls, encryption and authentication only go so far," Schneier said, referring to some of the more popular computer security technologies. "Every protection mechanism ever built has a flaw. They can be hidden for years, but they're there."

Counterpane, based in San Jose, Calif., and which last year raised \$7 million in financing from Accel Partners and Bessemer Venture Partners, has just finished building its first secure operations center in nearby Mountain View, Calif. (A backup center is being built in Chantilly, Va.)

The operations center, which has high-speed links to the Internet, is reinforced to resist physical attacks and further protected by video surveillance and special "biometric" access controls that require positive physical identification of staff members before they are allowed to enter.

Inside, operators work in shifts around the clock, watching their clients' computers, which are connected via the Internet from locations around the world. Although various companies have been taking part in tests, the one paying customer Counterpane would identify last week was VoteHere.com. The center's operators monitor information generated by a program that Counterpane developed, known as Socrates, which assigns categories and priorities to the network activities it detects, seeking signs of hostile computer attacks. Certain events that might be normal at one time -- backup files being made over a network at 3 a.m., for example -- might suggest a hostile intruder or an attack at another time.

The Socrates software also maintains a separate audit log. That is a potentially invaluable tool for forensic analysis after a computer break-in, since one of the first things that most sophisticated

computer intruders do after illicitly entering a computer is to erase the local log files to cover their tracks.

Counterpane may be a company in the right place at the right time, according to computer security market analysts. International Data Corp., a research house, estimates that the national market for computer security management services was \$703 million last year and will reach \$2.2 billion a year by 2003.

Until now, according to analysts, the market for such network-monitoring services has remained largely in the military and large corporate data processing markets and has been dominated by companies like IBM, Electronic Data Systems and Computer Sciences Corp.

But the rise of the Internet has created the need for such monitoring and alarm serves for e-commerce companies of all sizes. Besides Counterpane, Internet Security Systems and Pilot Network Services are among the new entrants to the monitoring field.

"The opportunity to build businesses here is huge," said David Tapper, a research analyst at International Data.

Schneier, the Counterpane founder, likes to draw an analogy between Internet security and a conventional metal safe.

He notes that modern safes are given specific Underwriters Laboratories safety ratings, which tell the safe owner how long it will take a skilled safe cracker to get at the information or money stored inside. The rating TL-30, for instance, means that it will take a skilled safecracker with tools a half-hour to break in. TL-TR-60 indicates that the safe will buy an hour's safety against the same safecracker, even if he has an acetylene torch at his disposal.

"What it means is that you bought an hour of security when you purchased the safe," said Schneier, who contends that clients deserve similar assurance with computer security software.

"The present state of computer security just isn't working," he said. "There are just too many attacks."

Related Sites

These sites are not part of The New York Times on the Web, and The Times has no control over their content or availability.

- [Counterpane Internet Security](#)
- [Twofish](#)
- [Internet Security Systems](#)
- [Pilot Network Services](#)

[Home](#) | [Site Index](#) | [Site Search](#) | [Forums](#) | [Archives](#) | [Marketplace](#)

[Quick News](#) | [Page One Plus](#) | [International](#) | [National/N.Y.](#) | [Business](#) | [Technology](#) |
[Science](#) | [Sports](#) | [Weather](#) | [Editorial](#) | [Op-Ed](#) | [Arts](#) | [Automobiles](#) | [Books](#) | [Diversions](#) |
[Job Market](#) | [Real Estate](#) | [Travel](#)

[Help/Feedback](#) | [Classifieds](#) | [Services](#) | [New York Today](#)

Copyright 2000 The New York Times Company.