A Thousand Points of Entry

Establishing enterprise-wide security is no easy matter. Here are some key issues to address in planning a comprehensive solution.

BY DON MONKERUD

Security used to be almost as easy as locking the door to the computer room at the end of the day. In today's multivendor, client/server environments, often networked in enterprise-wide systems, security is infinitely more complex. Networking computers, establishing global networks and streamlining systems to gain business efficiencies create new vulnerabilities to unauthorized access from within the company and from outside.

Enterprise-wide networks, coupled with a major thrust in electronic commerce on the Internet, potentially open a company's internal information to the whole world. While the Internet promises a new way of doing business, the risks incurred in using it are many. Effective security becomes the critical enabler in extending a company's network to improve service and accommodate the road warriors using remote access, while protecting the organization's valuable information assets.

No national clearinghouse keeps statistics on computer break-ins and computer crimes, and victims are understandably reluctant to publicize their experiences. Therefore, reports of the extent of the problem are largely anecdotal, although news reports chronicle some crimes of hackers. The British Banking Association estimates that computer fraud costs banks $8 billion a year. A survey of 320 information security professionals at large organizations conducted by the San Francisco-based Computer Security Institute found that only 51 percent of companies connected to the Internet had *firewalls*—electronic barriers to limit access from the outside—in place and that 30 percent of the breaches in security occurred even with a firewall.

A new study of 200 computer security directors by a team at Michigan State University in East Lansing found a startling increase in the number of computer crimes reported by the *Fortune* 500. Much of the crime resulted from lax security measures associated with a lack of value placed on intellectual property such as new designs, new concepts and marketing information.

Additionally, networking creates security issues that go beyond the company itself and beyond the security problems it thinks are important. "Technology has grown exponentially and created new and different types of vulnerabilities," says Andra Katz, a research associate at Michigan State. "There's a geometric growth in the amount of abuse [reported], from 60 percent [of all respondents] a few years ago to 98 percent today. That's a huge leap."

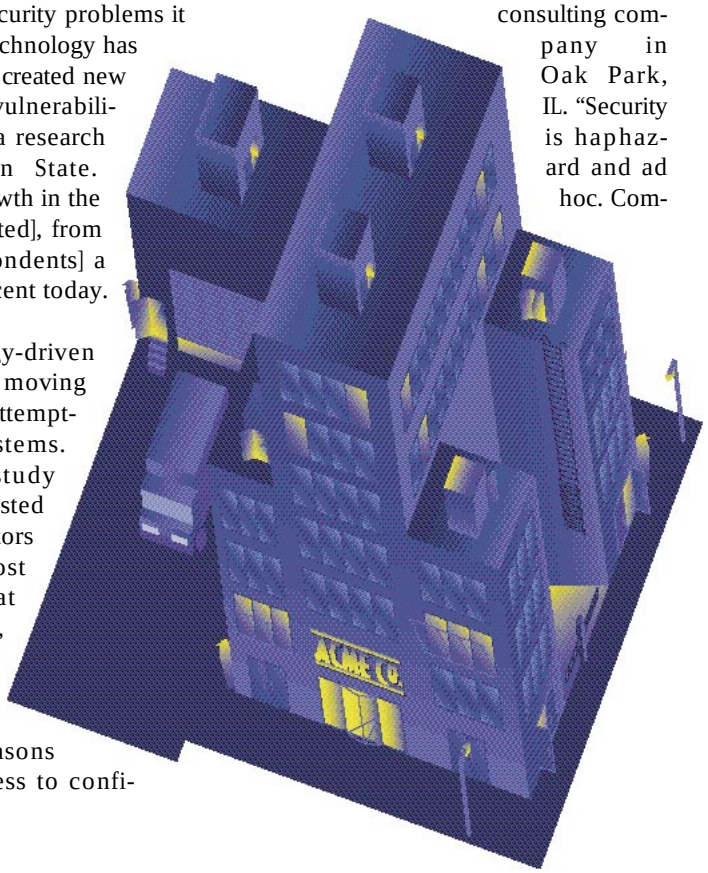
The new technology-driven vulnerabilities create a moving target for IS managers attempting to secure their systems. The Michigan State study found that full-time, trusted employees and contractors are responsible for most computer crimes that include credit card fraud, telecommunications fraud, copying of software, the use of computers for personal reasons and unauthorized access to confidential files. Many employees access confidential data to gain advantages over fellow employees.

At the same time as the Michigan study shows a rise in internal security breaches, IS managers record an increasing number of "door knocks from the outside." Hackers are getting increasingly sophisticated and, instead of exploiting a single machine, attack the infrastructure of the networks. The rise of "information brokers" and the "information underground" means hackers no longer have to know the value of the information they steal; brokers will locate a buyer for confidential company information and pay the hacker accordingly.

Developing a Plan

What can an organization do to neutralize threats such as these? Most computer systems grew willy-nilly, sometimes with limited oversight that paid little attention to overall security. Policies and procedures have been initiated in response to problems as they arose. Today's situation requires proactive planning, but developing a framework for a security infrastructure is complicated.

"Security is hard because solutions that are good and easy to use aren't here yet," says Bruce Schneier, author of *Applied Cryptography* (second edition, John Wiley and Sons, 1996) and president of Counterpane Systems, a security consulting company in Oak Park, IL. "Security is haphazard and ad hoc. Com-



panies hope for the best, but most company security is in pretty sad shape."

Rich Pethia is manager of Trustworth Systems at the Software Engineering Institute of Carnegie Mellon University in Pittsburgh and led one of the first Computer Emergency Response Teams (CERT). Trustworth Systems is an outgrowth of CERT; its goal is "to help the software-producing and -using communities build and maintain trust in software-intensive systems by decreasing the risks of computer security incidents." According to Pethia, security incidents reported to CERT increased from 770 in 1992 to 2,400 in 1994. By analyzing factors that contribute to the increase in security breaches, companies can begin to find solutions, he says.

First, intruders are becoming more technically sophisticated, and there are more of them. They have better understanding of networks and are more deeply analyzing network software to exploit vulnerabilities. For example, an awareness of topology lets them know where to plant eavesdropping software, such as sniffers that steal passwords.

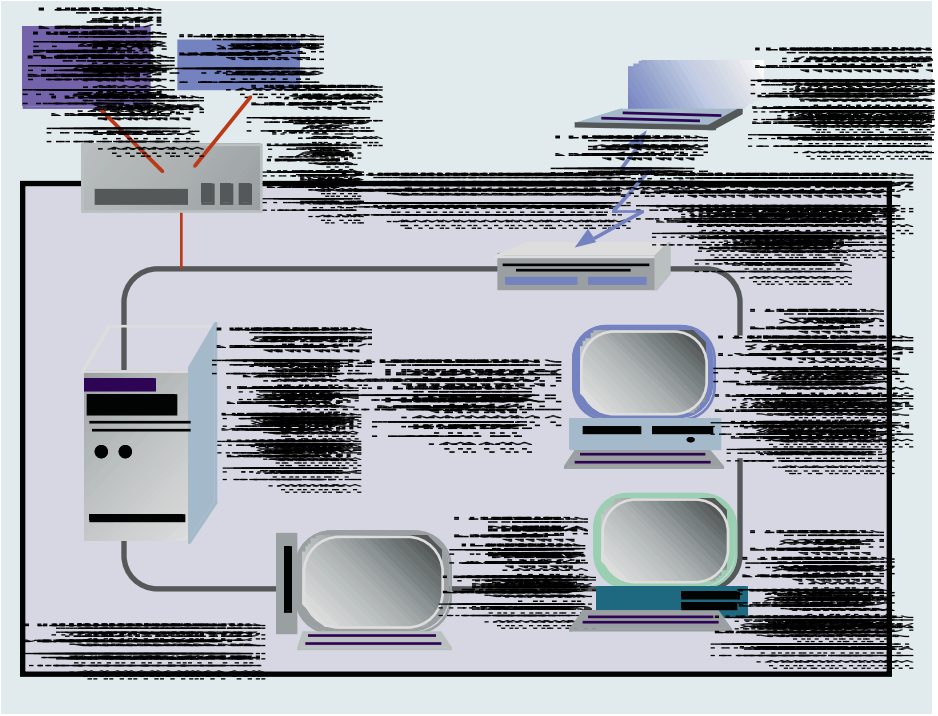
Second, moving from centralized mainframes to decentralized client/server configurations causes rapid management changes and reorganization. In-house security expertise may be fragmented and diffused throughout the organization, making technical solutions more difficult to determine and accomplish.

Third, the rapid growth in networks and changes in technology push many people into system administration without proper training. Such technicians often are unable to configure secure systems.

Coupled together, these trends are disturbing, and companies need to establish policies before they can counter the problems. Vendors are becoming more security-conscious, which will help in the long run, but in the short run users must try to anticipate and counter as many problems as they can. For example, companies are placing heavy emphasis on firewalls but may be overlooking the hundreds of modems installed to establish Internet connections. "A company needs to look at the entire organization from top to bottom and side to side to make sure they aren't missing any significant problems," says Pethia.

Analyzing Risks

As the first step in a comprehensive security plan, experts recommend identifying assets, placing values on them and evaluating the threats to those assets. Michele Crabb, a computer security analyst for the NAS facility at NASA Ames Research Center at Moffett Field, CA, suggests conducting a risk analysis that includes determining what information must be protected and at what level, as well as the real threats to them.



This typical network security configuration employs several methods to protect data from unauthorized access. *Source: Trusted Information Systems*

NASA Ames does formal analysis. Assets include hardware, software, contract personnel, storage media and facility building costs. Intellectual property assets include program code, input data, system and program documentation, World Wide Web servers and home pages, and databases. Safeguards analysis features three categories: physical, such as building access controls and remote camera surveillance; administrative, which includes all the policies and procedures; and technical, such as computer access control, system monitoring, password controls and audit trails.

According to Crabb, many sites suffer the same weaknesses. (For a list of common weak spots in site security, see "Holes in the Wall" on page 42.) Once the safeguards are evaluated, Crabb attempts to "break the rules" by having a friend pose as an intruder to enter the building or restricted areas without authorization or break into the computer system from the outside. After determining areas of vulnerability, she balances the risks against the cost of protecting the assets. At this point, the company must determine how much it is willing to pay to make the assets secure.

"One of the major problems comes down to the company's security stance," says Crabb. "What does a company want to protect, and what can it afford? Not everyone needs the same level of security."

Failing to dedicate management resources to security can pose a major problem. Few sites have a dedicated security officer, although a rule of thumb is that any site with more than 100 machines needs someone whose primary responsibility is to provide security for them. That person in turn needs ongoing security training to keep up with new techniques for intrusion.

Acquiring Tools

Crabb says that, after determining the security philosophy for a site, the next essential item is a collection of security tools. Intruders themselves run many of these tools as they attempt to find a weak link to exploit, and countering them will make the system more secure. (Tools listed below are freely available as shareware over the Internet.) Crabb classifies tools into four categories:

1. *Tools to scan and test for system vulnerabilities.* Some tools locate early versions of the *sendmail* Unix utility (which allowed unauthorized access to a system) and alert the system administrator. Oth-

ers allow administrators to check all hosts on the local network from a single host. (Examples: Internet Security Scanner, Securescann and SATAN.)

2. *Tools to scan the local hosts for configuration errors*, such as world-writable files and directories, poor passwords, unnecessary entries in the /etc/inedt.conf file and others that can lead to security vulnerabilities. (Examples: COPS, Tripwire, Crack and TAMU.)

3. *Tools to enable users to perform functions in a more secure manner*, such as by enforcing stricter password construction or encrypting e-mail. (Examples: npasswd, S/Key, Kerberos and tcp_wrapper.)

4. *Tools to analyze what an intruder did* after or during a security incident. They can scan log files for inconsistencies or determine open files. (Examples: LSoF, naiad, SLIC and prob_ports.)

While these free tools can answer many security needs, they are not for everyone. Some companies do not want to rely upon shareware for security, because public domain packages receive little software engineering and require knowledgeable professionals to install and keep them up to date. Universities, where shareware is often created, seldom have networks that carry mission-critical data.

"Corporations have standards for software, and it's unlikely that public domain tools will be developed in a way that meets corporate standards," says Gene Schultz, program manager at SRI International, a research institute in Menlo Park, CA. "If a university's machines crash, there's little cost. But if a corporation's machines crash for an hour, it could cost millions of dollars."

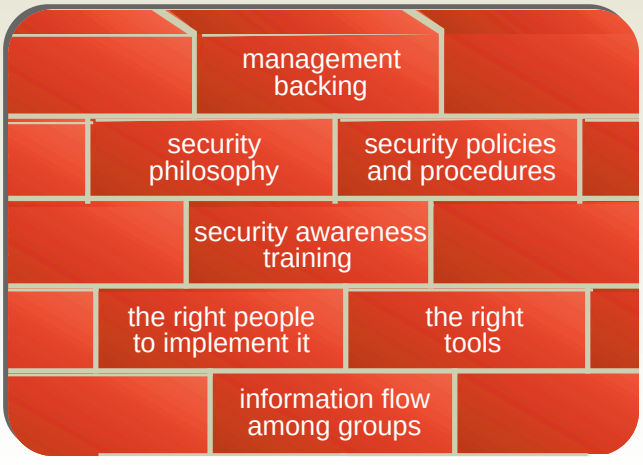
Private Policy

Viewing policies and procedures as a one-time exercise that establishes a fixed plan is futile, because the rapidly changing computing environment will render policies and procedures obsolete. Schultz favors having an evolving security infrastructure in which teams from different corporate functions, such as security, IS and various business units, brainstorm on what the network will look like over time. By developing "snapshots" of the network at given points in time, it is possible to anticipate threats and attempt to develop and design mechanisms into the network to counter them.

"Threats have to be addressed on a priority basis," Schultz says. "If it's an Internet connection to a corporate network, think about some kind of gateway-level control, like secure routers or firewalls. If it's to secure servers in internal networks, think about running a network-wide tool, like a network intrusion detection tool. But by all means develop intrinsic capabilities, which are fundamentally more important than add-on capabilities. Intrinsic capabilities will be more difficult to defeat and less costly to implement and maintain."

Another trend—the baseline control approach—is gaining popularity, according to Schultz. While risk analysis can be useful if an industry has a unique configuration, companies often get bogged down in resource-consuming guesswork. The *baseline control* approach simply implements the kinds of security controls that peer companies are using. This process works because security controls are evolving along with the threats and tend to focus on the most serious threats, rather than any possible threat that might occur. In essence, if your peers on the Internet are using firewalls, use firewalls; if LAN administrators are installing audit packages, do the same.

"The main kinds of controls people are using today are gate-level controls, like firewalls and secure routers, service-based security controls that make TCP/IP more secure and enhanced authentication tools, like tokens and smart cards," Schultz says. "At the same time, I never want to leave an impression that network security can be completely managed. Heterogeneous environments and protocols are impossible to control completely."



Building effective enterprise-wide security requires a variety of strategies and tools, all working together.

Source: Michele Crabb, NASA Ames

Wising Up Users

While security tools are good for technical people, it's the users who often allow intruders into a network. Most people view their computer as an appliance, like a telephone, and don't want to bother about security. Yet they should understand security issues and the vulnerabilities they create when they log onto the Internet.

"I agree with the statement, 'Security is not something you buy, it's something you do,'" says Sandra Sparks, computer scientist and manager of the United States Department of Energy's Computer Incident Advisory Capability team at Lawrence Livermore National Laboratory in Livermore, CA. "We're paying for years of neglect because security didn't get built into our information processing systems. It was usually an afterthought. Unix is an example of an operating system that was built to get solutions quickly, without needing to consider security. It was never intended for use in the business arena of today, and we are paying a price for its popularity."

Outthinking intruders is tough. Sparks reports one case where a desktop computer's security was compromised, and the company placed a guard on the office. The guilty employee simply saw the guard at the door, slipped into a nearby office and logged into the guarded computer from the PC in there. Another case involved a company that placed firewalls on its servers and then discovered a sniffer installed just inside the firewall.

Nevertheless, making users aware of security risks can increase the level of security. For example, Boeing Information and Support Services in Everett, WA, sees its employees as the first line of defense. A training program attempts to make all employees responsible for sensitive data on the network. Security professionals develop technical safeguards

(CONTINUED ON PAGE 42)

This page
intentionally left
blank

(CONTINUED FROM PAGE 40)
such as firewalls and encryption.

"There are many pressures pushing electronic commerce forward at a feverish pitch," says Bob Jorgensen, a spokesperson for Boeing. "We have to make sure that security moves as rapidly on the social and economic side."

Built-in Security

On the IT side, another trend is to build security features and functions into hardware and software. Many companies rely on third parties for security features, often on an OEM basis; others, such as DEC, Hewlett-Packard and IBM, are building security capabilities into their products, which can be used as needed. For additional security, third parties provide special features.

"In today's seven [days]-by-24 [hours] global organization, you go into the information systems and turn on the security features that you want," says Jim Schindler, information security programs manager for HP in Cupertino, CA. "For a minimum, you want a set of tools for authentication, access control authorization, integrity, and audit mechanism and audit reduction tools that provide analysis of the data to detect system and information attacks."

According to Schindler, no one tool is enough. This core set of tools can analyze vast amounts of data automatically. The tools are necessary to control the physical boundaries of the system and control access.

Currently, three methods of controlling access are the most effective and popular: firewalls, security tokens and encryption.

Firewall Functions

Firewalls allow access from the outside only to specifically registered individuals, who encounter challenge/response schemes that operate on layer three, four or seven of the OSI communications protocol stack, with the most security found at the highest level. Companies are using firewalls not only to protect the network from the outside; often several firewalls are used to partition off an internal network and protect departments within the company (for example, separating accounting from engineering).

A recent trend is the creation of virtual private networks that encrypt messages between firewalls. In this way secure data can be sent over the Internet but be freely accessible once it reaches the internal network destination.

"One of the reasons we've seen such growth is that firewalls impose no compatibility, functional or performance penalties," claims Steve Lipner, vice president of Trusted Information Systems, a vendor of firewall systems in Glenwood, MD. "A properly designed firewall gives transparency, function, high performance and a high degree of security."

However, there are evident limits to firewalls. One is their lack of flexibility; like any wall, they keep out everyone, even some people to whom you would like to give access. Also, many sites install firewalls and ignore internal security or forget that some machines are remotely accessible via another route.

Playing the Secure Card

Originally, hackers gained access into computer systems by exploiting easily crackable passwords. Although passwords remain prevalent in many networks, they are becoming a thing of the past, especially because of concerns over network eavesdropping and sniffer attacks. As firms use more contractors, employees working out of their homes, and salespeople and managers on the road, a secure method of reaching the internal network to access e-mail and databases is essential.

There are several schemes for tokens or secure cards to access a network. Patty Rosewater, IT risk manager at Hewlett-Packard in Palo Alto, CA, chose a random-number generator card to guard remote access to the corporate network. The card generates a random set of numbers that at some given time will match the number set on the CPU of the computer. When they match, the user then has 30 seconds to enter a password. Such a system typically runs about $100 per user, including hardware for the modem and software, plus $10 to $15 per month in support.

Rosewater sees systems evolving in the future to include "bio-verification" by

(CONTINUED ON PAGE 44)

Holes in the Wall

The following security problems often plague sites connected to the Internet. They are listed from most frequent to least frequent.

- Sites do not dedicate enough resources to improve and maintain security.
- Network and system support personnel do not have the management support or the authority to deploy appropriate security measures.
- Vendors still shipping systems with poor default security configurations and customers are still buying these systems even though they know they have security problems.
- Vendors do not disseminate information regarding patches to their customer sites and sites do not install vendor patches for security problems they do know about.
- Sites still use a login authentication system which uses reusable passwords or passwords which are transmitted over the net in clear text.
- Sites with strong Internet security but poor dial-up security.
- Sites do not monitor or restrict network access to their internal hosts.
- Sites do not install user accounts in a consistent manner.
- Sites do not monitor account activity and do not always remove accounts for terminated users.
- Sites do not place good controls on root and other special system accounts.
- Sites do not implement/enforce procedures and standards for installing new hosts on their network.

Source: Network Security Institute

This page
intentionally left
blank

(CONTINUED FROM PAGE 42)

which voice, finger or retina prints will verify a user. Alternatively, a user may carry a card that, when inserted into a PC, will not only allow access to the network but set up the individual's entire desktop and file system on the accessed machine.

However, token card systems are expensive and, in the secure ID model, the master server can become a single point of failure. If the server is accessible, all the information is compromised. The master server also becomes susceptible to denial-of-service attacks.

"Although cards will be with us for a while, the future is encryption," says Rosewater. "We have road warriors who work from their car or home and need to dial into our networks. We're increasingly sending confidential information over public networks. With hackers getting more sophisticated equipment, we'll have to go to encryption."

Encryption the Answer?

Public-key encryption essentially provides a secure "secret code" consisting of two "keys," a public one that is available for everyone to use (and generated by multiplying two large numbers) and a private one of two large numbers known only to the user. Because the *factoring* of the public key—the number of digits that multiplied together will give the public key—is so large, breaking the code is quite difficult. For example, mathematicians are currently working on factoring a 150-digit number, while secure public keys typically have more than 230 digits.

Because this technology is complex, encryption software companies typically OEM their products. Operating an encryption program also must be transparent to the user. "The adoption of encryption is increasing dramatically," says Jim Bidzos, president of RSA Security Systems in Redwood City, CA, a leading vendor of this technology. "By the end of 1996, every new product will feature built-in security, and by 1997 no products will be sold that don't have built-in encryption." But encryption has problems related to standards and U.S. government controls over exporting encryption technology.

It remains certain that no security mechanism will eliminate all worries. Security, almost by definition, requires human diligence. Peter G. Neumann of SRI International, author of *Computer-Related Risks* (Addison-Wesley, 1995), addresses the limits of purely technological solutions. "Although this year's simplistic answer to security is firewalls, there is no magic bullet," he says. "Even the best technology can be made useless by sloppy management practices. A third- or fourth-level exposure threat can become number one very quickly. You can't count on tools to give you the answers; you need good attitudes." Those responsible for security have no choice but to stay abreast of current developments. IT

Don Monkerud *writes about business and computer issues from Aptos, CA. He can be reached at 70713.2215@compuserve.com.*

Analyst's Couch

What's So Great About Electronic Commerce?

(CONTINUED FROM PAGE 72)

These are benefits for business purposes, but are they good for people? Critics of Internet fever perceive the trend toward an online nation as furthering dehumanization and isolation, the reduction of active citizens to passive consumers. The PC "revolution," whose proponents promised increased access to democratic processes, is 15 years old, and we seem to have a less egalitarian society than when it began.

If it doesn't change fundamental issues, why the big noise over electronic commerce? Well, capitalism is by definition restless, ever searching for new markets and new means of making money. Not many observers doubt that there's gold in those virtual hills. This opportunity alone is enough to make business on the Net a rich lode of strategies and tactics for profit (and of topics for the press and analysts). But let's not mistake it for something else. IT

Jeffrey Bartlett *is the executive editor of UniForum.*

Did something in this column press one of your hot buttons? Then let us hear what you think by sending a response to pubs@uniforum.org. We'll consider it for publication in "Letters to the Editor."