Telecommunications Security Against Criminals

by Lynda Voyles

Computer Crime on the Rise

Computer crime is well on its way to becoming the # 1 business crime in America. While exact figures are unavailable, experts place the cost of computer crime anywhere between $5 billion and $50 billion a year. And they predict increases in both the number of crimes and the dollar amount lost per case.

As new communication technologies expand into almost every aspect of commercial life, employers and employees alike need to take precautions to protect their vital information. For many companies, the cost of failing to keep up-to-date with the latest methods of protecting information has become too high.

Information security technology has long been available to prevent interlopers — from inside and outside the company — from committing computer crime. But it was often too cumbersome or time consuming to be used effectively.

New Technologies

Fortunately, the industry is developing new technologies that are not only easier to use but will also alert systems managers to security infringements. In addition, the industry is working on processes and standards to protect information when companies conduct business domestically, internationally, and via Internet.

The federal government continues to support information security. Businesses can expect government/business coalitions to develop security measures that meet the needs of both. The government is also advancing legislation against computer criminals and producing educational programs to define technology ethics for consumers and students.

"The criminals will always be in a position of one ups-manship," says Donn B. Parker, Senior Management Consultant, SRI International. "As we develop new safeguards, the crooks develop new methods of crime. There will always be initial losses as we use new technology. But we are more rapidly bringing the criminals under control."

The biggest advances in information security will be seen in cryptology. It is the one protective technology that is trusted throughout the industry. And experts believe it is the only one that can secure data sent over the information superhighway.

In addition to more sophisticated encryption methods, the industry looks to public key cryptography (a technology developed by RSA Data Security) or key escrow agents (developed by the U.S. government) to secure information sent via information networks and the global marketplace.

For businesses to take full advantage of cryptography, however, the technology must become more user-friendly and the government must revise its export restrictions. Currently, domestic companies are not allowed to develop encryption for export to the world market, a situation that has artificially suppressed the development of the technology, according to Mike Godwin of the On-line Council, Electronic Frontier Foundation.

Another key development involves establishing community, domestic,

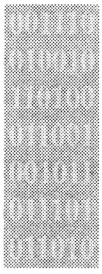
and international security standards for interoperability. Such standards allow like businesses to secure their own information and take advantage of national and international markets, says William J. Buer, Vice President of Marketing, Los Altos Technologies Inc. Historically, the best example of implementing such interoperable global security standards is the banking community's use of encryption and message authentication via automated teller machines and wire transfer networks.

Low-Cost Controls

In addition to new developments in cryptology and security standards, businesses will see an increasing number of low-cost controls that protect information and money through the use of the computer. Examples include audit controls that give detailed accounts of transactions, smart cards to protect data files from unauthorized access, and one-time passwords.

"With the advances in technology, a growing number of products and solutions for information security will be available, but they will be increasingly provided by non-U.S. companies," says Buer. "And with the adoption of international standards, companies will achieve cost-effective security for telecommunications and the information highway."

"As we develop new safeguards, the crooks develop new methods of crime."



The Human Element

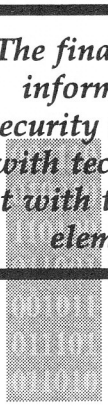
The final key to information security rests not with technology but with the human element. Ensuring that employees use security measures correctly and consistently is essential, as is increasing the awareness of computer ethics—and the consequences of violating those ethical standards.

But no matter how sophisticated the security technology a company uses, information managers must follow basic, common sense measures to ensure that their system is secure, says Rebecca Duncan, Associate Analyst for DataPro. She suggests managers use the following security checklist:

- Check defaults in the PBX (private branch exchange) system.
- Make sure passwords for routers are encrypted and few people know about them.
- Maintain up-to-date records on personnel so unnecessary access to systems is immediately removed.
- Ensure that maintenance ports are not open, protecting your system from service reps as well as computer technicians who might leave the company.
- Keep track of calling card and credit card records, and review audit trails.
- Join a telecommunications or security association and leverage your contacts.

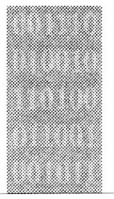
The last step to protecting information is employee education. For example, the average employee might not realize that scanners can eavesdrop on cellular phone conversations, or that sensitive information should not be left on voice mail. Employees must also be taught to respect network boundaries.

The final key to information security rests not with technology but with the human element.



Conclusion

Systems administrators can reduce security risks by implementing new technologies and fostering employee training. To do so they must enlist the support of top level management -- to commit the resources and underscore the



importance of security policy to the company.

Lynda Voyles is the principal of Phoenix Communications and writes frequently on telecommunication issues.