

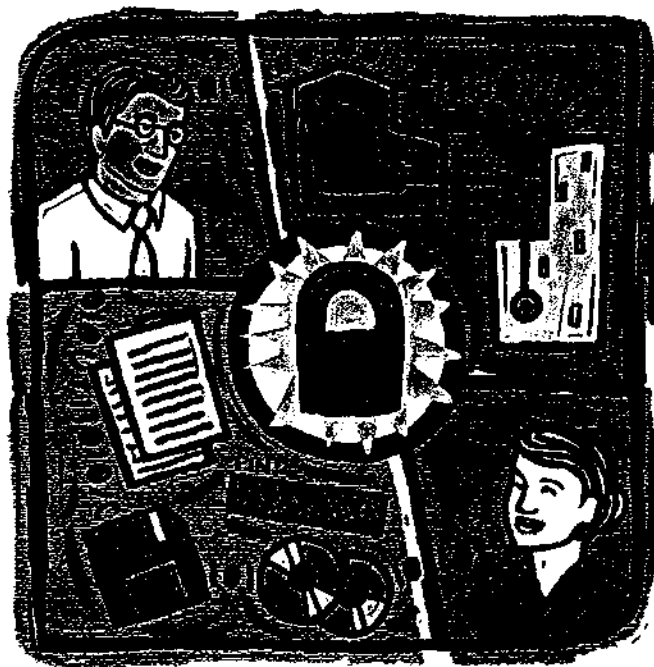
How to Tighten Computer Security

Before September 11, directors were quick to red-circle proposed technology budgets and urge top management to push back. Information-technology (IT) officers communicated in tongues that few directors understood, and it didn't help that technology departments were always asking for costly upgrades and cooler stuff.

Now directors and their IT people are on the same page. In fact, board members are pushing to spend more in attempting to make their companies' systems secure. "They used to ask, 'Do we really need this?'" says Peter G. Neumann, the principal scientist at SRI International's computer-science lab and a leading expert in technology security. "Now they're asking, 'Are we doing enough?'"

Boards aren't worried about physical violence alone. A skilled hacker can maim a company's computer systems, corrupting, jamming, or tanking Web pages, databases, financial networks, and internal communications. Here's what directors need to be asking their IT officers—and some of the answers they should be getting:

What's our information-security plan? The board should ask for a written document that describes, in plain English, how the company is protecting its technology (including hardware, software, and infrastructure), what it plans to do if employee access to hardware and networks is disrupted, and how it will continue to do business if its website is damaged or taken



down in a cyberattack. "The goal is for the company's intelligence data to be physically decentralized but logically centralized," says Kevin Mandia, co-author of the book *Incident Response: Investigating Computer Crime* and director of computer forensics at Foundstone Inc., a security firm. "The same data must exist in several different locations but be accessible from any one of them."

How are we "hardening," or protecting, our systems? In tech talk, to harden means to reduce unauthorized access to network servers, which handle the in-house commands of employees and the external clicks of website visitors. Hardening strengthens the "firewall," the security software that blocks unauthorized access. Another part of the hardening process involves having all

servers on the network use intrusion-detection sensors so that the IT department can monitor activity and security breaches can be spotted and reported quickly. Mandy Andress, president and founder of the security firm ArcSec Technologies and author of *Surviving Security*, urges companies to install the latest "hot patches," new codes that close security gaps in the system. Companies also need to plug holes that might compromise their websites. A Web application scanner, for example, will identify all breaks in security and give the alert.

What's our disaster-recovery plan? Companies whose systems are knocked out need to stay in business. One way to do this is to contract with a disaster-recovery firm. Such an outfit keeps a second set of computers in your offices

or plants, copies everything your system does, and regularly transmits the data to another site. If a hacker does knock you out, this backup system essentially picks up where your system left off. In addition, many larger companies now protect themselves against the collapse of landlines by installing wireless systems that can transmit data from one office building to another, or to a disaster-recovery site.

Do we have backup office space, with computers? You should. Your company needs to duplicate its essential computers and other hardware at an offsite location where employees can get back to work quickly, using the data your disaster-recovery contractor provides. This means you must invest in a lot of spare laptops or desktop computers, and also in dial-up modems in case your T-lines go down. Make sure the offsite premises have enough phone lines and jacks, and take other business-as-usual steps based on the size of your company and the nature of its work. Do this now, not when disaster strikes. And don't forget furniture, which at a minimum should include folding tables and chairs.

Now is also a good time to push employees to start backing up their computers each night and to stop programming their PCs to remember passwords. These last two security measures may seem like make-work, but they're not. They protect the company's intellectual property.

by Marc Myers