CAREER OPPORTUNITIES

The Importance of Security

By Douglas E. Welch

Of all the issues facing the high-tech careerist in the coming year, security, in all its forms, should be the top priority on everyone's list. I am not just talking about Internet firewalls, VPNs (Virtual Private Networks), and encryption, though. While all these are important, security involves the entire company, not just a few pieces of computer equipment. As a high-tech careerist, it will be your responsibility to convey the importance of technology security to everyone. This is simple self-preservation. Regardless of who might be at fault, if security is breached at your company, you will quickly find that everyone will hold *you* responsible.

The Outside

Keeping unauthorized users out of your systems can be a tremendous amount of work. Free-roaming "script kiddies" will be using their downloaded hacker toolkits to try every technology doorknob in your site, looking for an easy entry. Viruses and worms will try to trick unwary users into opening backdoors in their systems and spewing infected e-mails both inside and outside of the company. The good news is that there are a variety of tools to help you protect and monitor your systems, including firewall software and hardware and antivirus programs. The bad news is, there are more insidious holes in your security, often of your own making.

The Inside

If you fail to develop security procedures to accompany all the hardware and software mentioned above, you might as well turn it all off and let people freely wander through your systems. All the technology in the world cannot combat lax internal policies.

Do you have a procedure for assigning and removing user IDs for network servers and other resources? Do you have old IDs floating around for users who left months, or even years, ago? If so, you are in good company. Many other businesses have similar holes lurking in their systems. While a past employee might not actively engage in the sabotage or unauthorized use of your systems, others, with less noble intentions could easily make use of IDs and passwords they come across. Don't take any chances. Lock down your systems and treat passwords the way you treat the keys to your own house. If you lost your keys, you wouldn't hesitate to replace your locks. Do the same for your systems.

Recovery

More than ever, the security of your systems depends on your ability to recover from crises, both large and small. Along with the usual issues of flood, fire and earthquakes, you must also think about new situations that could damage or remove access to your building. There may never be another terrorist attack or HazMat situation, but the mere threat of these attacks is enough to evacuate buildings and cordon off entire blocks. You need to be able to cope with the worst, even if you can't access your equipment directly.

Backups, in all their forms, are your best protection against any and all crises. They come in many forms and levels. First, even in smaller companies, all data and specialized programs should be duplicated and stored at a remote site on a regular (no less than weekly) basis. This information would allow you to set up shop at a new site, on new equipment, if necessary. Backups such as this are your first line of defense. Nothing can protect your company, and your career, better than the ability to rebuild your entire operation.

Second, you should have some way to access systems from off-site locations, in a secure fashion. This type of setup would allow you to move personnel off-site while still maintaining access to your systems. Even though you would lose access to hard copy information, the data in your systems would allow the company to continue working.

Along with physical backups, you will need procedures in place that allow you to maintain and make use of these backups, should the need arise. Tapes and other storage media need to be checked regularly to ensure that they actually hold data and are not blank due to some technology or human failure. Backups must be kept current and rotated out to off-site locations. Finally, you will need to develop and test procedures that will allow you to deal with some of the issues mentioned above. Even if you have all your data, you will need to know how you will rebuild your operations from the ground up, if needed.

Protect your systems and your high-tech career this year by focusing on security in your company. You may never need these backups or procedures, but if you do, you will need them desperately. ❑

Douglas E. Welch is a freelance writer from Van Nuys, California, and can be reached by e-mail at douglas@welchwrite.com *or on the Web at* www.welchwrite.com.