;login:

THE MAGAZINE OF USENIX & SAGE

June 2002 volume 27 • number 3

inside:

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

apropos

Don't Shoot the Messenger

by Tina Darmohray

Tina Darmohray, co-editor of ;login:, is a computer security and networking consultant. She was a founding member of SAGE.

<tmd@usenix.org>

If you've considered security at your site for very long, you've probably thought about what to do in an emergency. That is, if there is a computer security incident, what procedures are to be followed during the crisis, who will be in charge, who will make decisions to cut off services, who will talk to the media, etc. In fact, discussing and planning ahead for these crisis procedures is considered to be "industry best practices" and, as such, is becoming a pretty mundane topic, as it should be. I would have thought so, too, until just a few months ago, when I heard of a slight twist to this type of planning that should be considered by all organizations.

Has your organization considered what the procedure would be if the security threat is within your own walls? That is, do you know who to tell, who makes decisions to cut off services, etc.? Do any of the procedures differ from those designed for an attack from the outside? What happens if what has to be said or done is "unpopular" with the designated decision person? Has this potential conflict of interest been taken into consideration?

Recently, I participated in a security review of a site that had already considered this potential conflict of interest. In order to address it they have a security incident reporting structure that is different from that of the line-management of the security group. It's actually quite a clever design, which simultaneously incorporates varied user groups' computational needs and organization-wide security concerns. At this site, the responsibility for computer security comes through the CIO and then through the typical management chain-of-command to the computer security officer. What is unique in this organization is, in a parallel fashion, computer security issues are considered through a committee hierarchy: the senior manager's Committee on Computing, the Computer Coordinating Committee, and finally the Computer Security Committee, which is made up of computer and network security specialists and representatives of the organization's computer users groups. The computer security officer is a member of the Computer Security Committee. In the event of a security incident, the computer security officer is the one calling the shots. In the event of a computer security issue, the computer security officer has a committee, already in place, to report it to. In this way, security of the organization will be placed above the agenda or best interests of a single individual, or at least it will be openly discussed. Additionally, the computer security officer is protected from being "the messenger" if the security concern is about, or within, his or her chain of command.

So, if you haven't taken the time to create crisis-mode procedures for your site, do so now. If you haven't considered how such procedures might differ, depending on the source of the crisis, do that too.