Creating the CIRT: Defining Service Levels

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

When you start working on a Computer Incident Response Team (CIRT), you must manage expectations carefully to avoid disappointment, frustration and hostility from users who may want more than you can reasonably provide. Managing expectations is a general principle applicable in a wide range of projects, not just CIRT management; for example, in planning a large-scale transaction processing system where the contract stipulated a maximum response time per transaction of three seconds, I remember that the programming team built a timer into the system so that responses would take exactly three seconds even during the initial test phases. We knew that only a few data entry clerks would be working on the system to try it out for the first few weeks, and the last thing we wanted was to get them used to sub-second response times that would climb as the databases became increasingly loaded and when several hundred users finally began using the system. At first, the client thought that this strategy was odd, but after thinking about it, they realized that it made sense.

As you establish your CIRT, you may want to start small, as I mentioned before. Perhaps you can limit the scope of the CIRT to a few of the smaller production systems to avoid plunging into a new area of expertise with enormous stakes riding on your success. You should decide whether to start with working-hours only, extended hours (e.g., early morning to late night) or 24-hour, seven-day operations. If software development is part of your environment and (as most people will recommend) is physically distinct from production systems, perhaps that could be a good start for the nascent CIRT. Although many development staff may work long hours and on weekends, the effects of system emergencies may be less severe than attacks or breakdowns involving other systems such as, say, inventory, factory controls, customer service, sales and so on. When you are ready to tackle an even more significant production system, perhaps a system whose users tend to leave more-or-less at the end of the day might be a good candidate; e.g., the accounting system or support systems for any operation that does not run more than one shift per day.

In any case, be sure that you communicate your intentions for when your CIRT services will be available to your customers (and yes, that’s a deliberate use of the word).

The other aspect of service levels is how fast you can respond to emergencies. That’s a much more complex issue and will be the subject of articles on triage and setting the rules for triage later in this series.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information
Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.