Managing the CIRT: Avoiding Burnout

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
Norwich University, Northfield VT

This is another in an occasional series of articles looking at computer incident response team (CIRT) management. A primary source for this series is the US Defense Information Systems Agency (DISA) training course listed at the end of the article.

Much of the discussion below applies equally to CIRTs and to help desks; in a sense, one can view the CIRT as a specialized help desk. Many CIRTs are specialized subsets of the help desk team.

Any organization, even one with a relatively small CIRT or a small help desk, can suffer spikes in demand. Ordinary business cycles can influence network usage; for example, universities often see perfectly normal but large increases in call volumes at registration times as new students forget their passwords, try to connect unverified laptops to the university network, or get blocked for violating appropriate-use policies. At any site, a denial-of-service attack, a plague of computer virus infections, or an infestation of computer worms can cause a flood of calls “way above normal levels.

Another trend is the ironic observation that the better a CIRT (or help-desk team, but I’ll continue by focusing on CIRTs) becomes at handling problems, the more readily members of its community will turn to it to report problems or ask for help. Thus the better the CIRT does its job, the heavier its workload can become, at least for a while. According to the DISA course, “As a new CIRT grows and the workload increases, and especially on those teams that provide 24-hour emergency response, burnout becomes quite common. By studying the issue, one national CIRT determined that a full-time team member could comfortably handle one new incident per day, with 20 incidents still open and actively being investigated.”

Staff members who face increasing workloads may become stressed. Working long periods of overtime, missing time with family and friends, perhaps even missing regular exercise and food – these factors may lead to increased errors and turnover if people are forced to accept increasingly demanding conditions for long periods.

One of the most valuable organizational approaches to preventing burnout is to rotate staff through the CIRT function from your IT group on a predictable schedule. For example, you can assign people to the CIRT for three- or six-month rotations. Such rotations require especially good training programs and particularly good documentation to maintain efficiency as new people come on duty; in addition, the assignments must be staggered so that the CIRT doesn’t have to cope with large numbers of newcomers all at once. Ideally, there wouldn’t be more than one switch of personnel a week.

How should existing assignments be transferred within the CIRT? I recommend that...
existing cases be transferred to staff members who have been on duty for a few weeks, not to the incoming staff member (even if she has experience on the CIRT). The incoming CIRT member should be given a chance to get into (or get back into) the rhythm of the job before being hit with the most intractable problem or the orneriest client.

Every incident must have a case coordinator – the person who monitors the problem, aggregates information from varied resources and serves as the voice of the CIRT for that incident. When transferring responsibility for a case from one case coordinator to another, be sure to have the previous coordinator prepare the clients for the transition and introduce the new coordinator to the key client contacts to ensure a smooth transition of control. Clients often come to depend on the person they have been working with to resolve an incident; an unexpected change can be unsettling and even disturbing.

The DISA course writers suggest, “Allow team members to allocate time away from high stress incident response assignments and pursue broader interests in areas such as tool development, public education and presentations, research, and other professional opportunities.” CIRT members, by the nature of their work, will have a great deal to contribute to the awareness, training and education of their colleagues.

Making the CIRT a stimulating and enjoyable duty that people _want_ to be on is one of the best approaches to avoiding burnout and ensuring reliable response to computer-related problems.

** **


** **


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msis.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 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.