The computer incident response team may be a permanent, full-time assignment for a fixed group of experts or it may be a part time role assigned to dynamically as conditions require. In either case, or for any of the intermediate arrangements, certain fundamentals will dictate your choice of staff members for the CIRT. Cowens and Miora [1] write,

“Maturity and the ability to work long hours under stress and intense pressure are crucial characteristics. Integrity in the response team members must be absolute, since these people will have access and authority exceeding that given them in normal operations.

“Exceptional communications skills are required because, in an emergency, quick and accurate communications are needed. Inaccurate communications can cause the emergency to appear more serious than it is and therefore escalate a minor event into a crisis.”

The DISA course on CIRT Management [2] addresses the question of the technical level required by CIRT staff. The authors suggest,

“Using a scale from 1 to 10 with 1 representing the novice or support staff, and 10 representing the technical wizard,. . .

“To handle the initial Triage process, which involves separating service request into categories and directing them to the appropriate team member, individuals in the 1 to 3 technical range should be sufficient.

“Information requests can be handled by team members in the 1 to 5 range. For example, a support staff person can send out publications, while someone with greater expertise would be required to address the question about identifying spoofed e-mail.

“To handle incidents . . . team members in the 5 to 8 technical range are necessary. This response can involve technical analysis and communicating with compromise sites, law enforcement technical staff, and other CIRTs. In handling incidents that represent new attack types, you may need to call the wizards to help understand our analyze the activity.

“Vulnerability handling requires your most proficient personnel, falling into the eight to 10 range. These individuals must be able to work with software vendors, CIRTs, and other experts to identify and resolve vulnerabilities. Many CIRTs don't have access to this level of technical expertise.”

I want to add to these excellent comments that in my experience, CIRT staff with the psychological flexibility to allow them to adapt quickly to changing requirements will do better than people who resist change or resent ambiguity. Ideally, the team will include problem-
solvers with an intuitive grasp of the differences between observation and assumption, hypothesis and deduction. As always, team-players committed to getting the problem solved will contribute more than people interested in acquiring personal credit for achievements. I also think that having at least one person on the team with a penchant for meticulous note-taking is a real benefit; more about recordkeeping in another segment in this series.

* * *

References:


* * *

M. E. Kabay, PhD, CISSP is Associate Professor of Information Assurance in the Division of Business & Management 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>.

A Master’s degree in the management of information assurance in 18 months of study online from a real university – see <http://www3.norwich.edu/msia>.

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.