Creating the CIRT:
Establishing Policies and Procedures

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

As the DISA training course on CD-ROM about computer incident response teams succinctly puts it, “policies and procedures are not merely bureaucratic red tape.” They are the scaffolding on which you can establish clear understanding and expectations for everyone involved in incident response. These living, evolving documents are tools that provide guidance on (quoting the CD-ROM)

* Roles and responsibilities
* Priorities
* Escalation criteria
* Response provided
* Orientation.

Policies are the statements of the desired goals; procedures are the methods for attaining those goals. Policies tend to be global and relatively stable; procedures can and should be relatively specific and can be adapted quickly to meet changing conditions and to integrate knowledge from experience. Policies cannot be promulgated without the approval and support of appropriate authorities in the organization, so one of the first steps is to identify those authorities. Another step is to gain their support for the policy project.

All policies and especially CIRT policies should be framed in clear, simple language so that everyone can understand them and should be made available in electronic form. In previous articles published by Network World Fusion, I have pointed out that hypertext can make policies more understandable by providing pop-up comments or explanations of difficult sections or technical terms.

Similarly, procedures show how to implement the policies in real terms. For example, a policy might stipulate, “All relevant information about the time and details of a computer incident shall be recorded with regard for the requirements of later analysis and for possible use in a legal proceeding.” That policy might spawn a dozen procedures describing exactly how the information is to be recorded, named, stored, and maintained through a proper chain of custody. For example, one procedure might start, “Using the Incident_Report form in the CIRT Database accessible to all CIRT members, fill in every required field. Use the pull-down menus wherever possible in answering the questions.” Again, as the DISA CD-ROM points out, these procedures should minimize ambiguity and help members of the team to provide a consistent level of service to the organization. A glossary of local acronyms and technical terms can be helpful as part of these procedures.

Whenever policies and procedures are changed in a way that may affect users, it’s important to let people know about the changes so that their expectations can be adjusted. The DISA course recommends using several channels of communications to ensure that everyone gets the message; e.g., send e-mail, use phone and phone messages, send broadcast voicemail, announce
the changes at staff meetings, and use posters and Web sites.

***

Reference:


***


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.