Learning from Emergencies: Root-Cause Analysis

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

This is another in an occasional series of articles looking at computer security incident response team (CSIRT) management. In my last column, I discussed the incident postmortem analysis. Today I want to look at root-cause analysis.

One aspect that sometimes gets lost in the incident postmortems I’ve been describing is exploring the reasons for the problems. If we don't pay attention to underlying causes, we may fix specific problems and we may improve particular procedures but we will likely encounter different consequences of the same fundamental errors that caused those particular problems. We must pursue the analysis and deeply in off to identify structural flaws in our processes so that we can correct those problems and thus reduce the likelihood of entire classes of problems. Readers interested in learning more about management style and small-group leadership tools may find some material of value in the Management Skills lectures and in the Leadership lectures on the MSIA section of my Web site <http://www.mekabay.com/msia/public/index.htm>.

The US National Institute of Standards and Technology Computer Security Incident Handling Guide by Tim Grance, Karen Kent and Brian Kim <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf> specifically recommends a post-incident analysis in section 3.4. The authors’ list of suggested questions is as follows (quoting exactly):

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

The authors also recommend the following (paraphrasing and summarizing):

- Invite people to the postmortem with an eye to increasing cooperation throughout the organization;
- Plan the agenda by polling participants before the meeting;
- Use experienced moderators;
- Be sure the meeting rules are clear to everyone to avoid confusion and conflict;
- Keep a written record of the discussions, conclusions, and action items.
On this last point, I must add that all action items should indicate clearly who intends to deliver precisely what operational result to whom in which form by when.

In my next column on this subject, I'll be looking at continuous process improvement through knowledge sharing within the organization.

* * *


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

Copyright © 2007 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.