CSIRT Management:
Lessons from Other Group Postmortems (1)

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


In 2008, I was blessed with five excellent students who not only wrote their weekly essays well but also participate enthusiastically in the weekly discussions (we have three or occasionally four topics for them to use in sharing insights and experiences) and in Week 9 of the 11-week course, one of the questions was as follows:

“Postmortems are conducted in many other fields – well, for example, as autopsies! But perhaps some of you have actually participated in non-CSIRT teams where a postmortem was standard operating procedure. Examples might include, say, a sports team, any kind of problem-solving team, a marketing group looking at an advertising campaign, a group of professors evaluating a new course, and a group of detectives or attorneys looking at how an investigation or a courtroom proceeding turned out. Please share interesting experiences of this kind with your classmates and see if any of your insights can be constructively applied to CSIRT management.”

In collaboration with my students, I am publishing a lightly-edited summary of their discussion in this column and the next in the hope that readers of the series will enjoy their comments as much as I did.

* * *

Tikuo Chen wrote, “When I was back in California, I belonged to a very well run Cub Scout organization which routinely used post-mortem like analysis to figure out how to make pack activities more enjoyable for the scouts and their families. Just over two years ago, after a couple of the den leaders shared concerns during one of the pack planning meeting about how some dads were becoming a bit too hands-on in managing their scout’s pinewood derby cars, we undertook a concerted effort to figure out how we could put the focus back on the scouts. …[W]e decided to create more hands-on opportunities for the scouts. Instead of just one main event where the scouts essentially place their cars on a gravity track and watch the cars run, we added two more equally prestigious events (e.g. top performers earned the same trophies, but there was a one-trophy per person limit). These two events allowed scouts to roll their cars to first attempt to get the closest to a line and then to attempt to get the closest to a set quarter-sized mark. Not
only did the format change take the pressure off both scouts and their parents to build the fastest car, but it also encouraged the scouts to learn how their cars handled and it created more opportunities for parent involvement. The added events meant that we needed more parent helpers to supervise and act as ‘race coordinators’. What this experience showed me was how important it is to understand the real objective in any situation (for scouting, it is creating fun opportunities for scouts and their families) and that there are often better ways to motivate behavior change besides attempting to impose sanctions.”

Michael Sanclimenti posted an interesting comment: “I participated in postmortems for disaster recovery tests and resolving problems that caused a large data network or voice network outage. The disaster recovery postmortem was conducted by quality assurance (QA) and it was mostly a review of what went wrong or took too much time. Blaming a department or individuals was not part of the meeting. The meeting was constructive criticism and a review of processes. QA was responsible to make the necessary changes before the next test. When there was a data or voice network outage and it had an impact on the business, then a postmortem meeting with the network team and the vendor was held. I worked for a foreign bank at the time, so communications between the U.S. and the main country were very important. The majority of the time, it was an equipment failure that affected circuits. The VP of the network group would call his team and the supplier of the circuits to the meeting. The vendor’s sales team was there to give mostly excuses as to what happened while we gave all the facts about the incident. These meetings did not accomplish much since the outage was out of our hands and the vendor never changed their processes. All the vendor did was to give us a credit on the monthly bill. However, as long as the postmortem meeting is organized and has a purpose, it should be held for most incidents.”

Enrique Parker had an excellent list of ground rules for postmortems: “My case study organization is very active in project management and we are required to complete a project retrospective within one week of completing a project. In fact most of the rules and structure of conducting a postmortem are founded on the established procedures from the project management processes. Even though the goals and objective may be different between the project management retro and the CSIRT postmortem, the ground rules can certainly be equally used. The general ground rules include:

- Focus on the processes and roles and not on people
- Build on other’s ideas
- Listen actively: don’t kill an idea before it’s been fully expressed
- Participate – Everyone
- Refrain from justifying your previous actions
- Once conversation at a time

To keep the team focus the project team provides a list of functions that are generally part of a project

- Project Planning
- Team participation
- Decisions
- Communication
- Processes and procedures
- Training
- Results.”
Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are “Introduction to IA for Non-Technical Managers,” (July 18-23)<http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php> “Management of IA,” (Aug 1-6)<http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php> and “Cyberlaw for IA Professionals.”(Aug 8-13)<http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php> Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

Tikuo “T.C.” Chen works with a nanomanufacturing company in the Information Security & Risk Management department and is currently posted in Shanghai, China, where he is responsible for ensuring that his employer’s China operations comply with technology control program requirements.

Enrique Parker works for a fair-sized credit union in California as a Senior Security Architect and has been busy establishing the security infrastructure of the company.

Michael Sanclimenti works in the Managed VPN group of AT&T Labs and is responsible for developing their managed IPSec, Firewall/IPS, multicast, and GETVPN offers.

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/> 

Copyright © 2009 Tikuo Chen, M. E. Kabay, Enrique Parker, & Michael Sanclimenti. 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.