In Week 9 of the 11-week course on Computer Security Incident Response Team Management that I taught in summer 2008, one of the weekly discussion 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.”

This is part 2 of a lightly-edited report on my students’ conversation.

* * *

Eric Jernigan contributed a valuable checklist from his US Army experience: “Of all the jobs I had in my life, I think the most ingenious postmortems are the ones taught in the Army. Every time we

- Built a bridge
- Blew up a bridge
- Jumped out of a perfectly good airplane
- The aircrew flew their perfectly good airplane
- Did a mission plan or fixed a tank…

…we did an After Action Review (AAR). They were effective because we did them immediately after the task and because they were simple. The main format of the AAR is:
1. What was the mission (task/activity) and your part?
2. What needs improvement?
3. What should we sustain (continue doing)?

The chain of events should be part of the first section. It doesn’t look like much, but when you assemble the whole team tell them their opinion matters (equally), key details rise to the top every time. If there is any blame to go around, it is usually becomes self evident.”

Steven Doan remembered his experiences in software development: “The experiences I have had with non-CSIRT postmortems were related to project releases. This occurred whether there was success on a project release as well as when there was a failure (e.g., where the planned implementation or upgrade did not proceed as anticipated and a rollback was necessary to return
the environment to its original state). The postmortem pulled all involved and management parties together to

- discuss the project plan and
- determine what went well,
- what went wrong and
- what action could be taken to improve the efficiency/effectiveness of the project implementation or
- was necessary to correct the failure issue and
- why it was not identified in the first place.

Unfortunately it seemed that after a time, these postmortem events did not return as much value as they should have because there was too much politics and red tape regarding how the postmortem meeting was conducted: not everyone was able to express their opinions and so valuable data and information was lost. Thus, it is important to have an environment where all parties are exempt from criticism and have the opportunity to express their opinions on what went wrong or right and opportunities for improvement or ideas they think could be of benefit for the next release cycle. Without this format, people do not feel valued and may not share their ideas and experiences in ways that can help the team find success.”

[MK: these students all got high grades for that week’s discussion!]

* * *

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!

* * *

Steven Doan is a systems engineer for a software development group in a large oil & gas services organization.

Eric Jernigan is the Information Security Manager at a large community college system in Oregon. His job responsibilities include information security program development and governance, incident response, security awareness training and education.

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 Steven Doan, Eric Jernigan, & 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.