In the preceding column, I discussed how to plan for the use of social engineering techniques in penetration testing. Today I will finish with a brief look at how to use the information collected during such studies.

In a _Network World_ column published in 2000 <http://www.networkworld.com/newsletters/sec/2000/00292157.html>, I wrote, “In an organization wide debriefing, the results of the tests can be discussed so that everyone learns from the experience without feeling humiliated. The essential point is that by turning penetration analysis into a collective exercise, the disadvantages of social engineering can be reduced.”

If one or more people succeeded in resisting social-engineering tricks, the atmosphere of the postmortem can be cheerful and low-stress: that’s the easy case. One can capitalize on the success by analyzing the successful cases; ask the people involved how they spotted the fraud, how they responded, and if there’s anything they would suggest to improve the response. Ask the social engineers what they could have done to reduce suspicions or respond better to the successful resisters. Role-playing is a powerful tool for such work – and then the group can brainstorm additional countermeasures. The whole exercise becomes an opportunity for security improvement through encouragement, praise and good will.

But how can one approach the postmortem analysis to minimize stress when someone or several people failed to counter the social engineers? Those people will be entering the discussion with a natural sense of discomfort at the least – dread and shame at the worst. It’s important to set the tone at once: “We’re here to learn from the exercise – that’s what it’s all about. I don’t want anyone to feel that they have failed the group or are a Bad Person: the exercise is _succeeding_ by bringing out areas we have to improve. Now let’s get down to business.” And by the way, that statement has to be _true_: group leaders should not pretend that they are positive about the exercise if they are internally contemptuous and hostile because of the successful trickery of the social engineers. Instead, the group leaders have to either resolve their feelings before the meeting or find someone else to lead the meeting.

During the postmortem, it can be helpful to use role-playing again. The people who were tricked can be encouraged to figure out what they missed, perhaps with the help of the social engineers or others. Group moderators can encourage those same victims of the trickery to act out successful resistance to the tricks, reinforcing the sense that the session is a learning experience. Keeping the tone light, friendly and positive will help counter what could otherwise become a session of bitter and dispiriting self-flagellation.

Most important in all cases is to keep a record of the suggested improvements and then to plan how to implement them in a phased sequence according to the criteria the group decides on. The criteria for scheduling the improvements can include resource limitations and dependencies among the recommendations (critical-path charts <
http://www.netmba.com/operations/project/cpm/ > can help sort out those problems).

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@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.