On Hacker Conventions, SecurityPortal and List Sponsorship

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

Recently President Richard Schneider of Norwich University wrote to me about a message he had received from one of our alumni concerning a message that appeared on one of the well-known and respected SecurityFocus discussion lists, Security Basics <http://www.securityfocus.com/archive/105/445936>. The alumnus was concerned that the call for participation in the PAKCON conference might tarnish the reputation of our University because we pay for advertising in the SecurityFocus lists.

I wrote back “In my opinion, as sponsors of this list, we have no responsibility whatever for its content. It is difficult for me to imagine anyone assuming that there is any association between Norwich and what random individuals post on a public discussion list hosted by someone we pay money to for ads.”

In addition, I wrote, “the PAKCON conference seems to be no worse than DEFCON, to which we regularly pay for Norwich students to attend as part of their learning experience. The location in Pakistan is irrelevant, as is the name or ethnicity of the organizer.” In sum, then, “I see no problem here. I am copying my colleague Prof Stephenson for his opinion on this matter.”

Peter R. Stephenson, PhD, CISM, CISSP, FICAF is Associate Program Director of the graduate program in information assurance at Norwich. He wrote to President Schneider as follows:

[The following is Peter’s text, used with permission.]

I concur with Prof. Kabay. There are several hacking conferences around the world (DEF CON <http://www.defcon.org>, HOPE <http://www.hopenumbersix.net/>, etc.). There was a time when we, as security professionals, were divided about the value and ethics of participating in these. That position has changed markedly.

While there still are a few who oppose any connection with hackers or hacking conventions (sometimes called "cons"), most enlightened security professionals see great value in participating as observers. This is especially true of those in our profession who lean towards the technical side as I do. These events are attended regularly by law enforcement as well and for the same reason.

There are a few credible information security portals of which SecurityFocus <http://www.securityfocus.com> is arguably the oldest and most credible. It is a commercial portal now, owned by the large security firm Symantec. It contains valuable information and as a university program interested in attracting top candidates as future students. It is wholly appropriate for the MSIA to be a sponsor and have advertising there. This portal gets hundreds of thousands of readers and most are serious information security professionals.

Because it is a global portal it is reasonable to expect that there would be participation from
around the world. This portal has evolved into a very professional operation and we no longer see the kind of behavior that was typical of the hacker boards of the 1990s.

Additionally, this is a source of what we refer to as full disclosure vulnerability reporting. This has been controversial over the years but most security professionals with experience agree that it is a good thing and, for some organizations, has truly saved their skins on many occasions by having the identification of and defense against what we call zero-day exploits. These are attacks that get into the wild before the software developers have time to create patches to protect their software. Rules for full disclosure have evolved over the years and SecurityFocus has been a leader in promoting responsible full disclosure.

The bottom line, in my view, is that SecurityFocus is a positive contributor to our profession, a good source of leads for new admissions and completely appropriate for us to sponsor.

[end of Peter’s text]

My own position with respect to speaking at meetings remains consistent with the (ISC)^2 Code of Ethics which requires CISSPs and other holders of the organization’s professional certifications “To discourage such behavior as:

- Professional association with non-professionals
- Professional recognition of or association with amateurs
- Associating or appearing to associate with criminals or criminal behavior.”

When asked to speak on panels at conferences, I always ask who else will be on the panel; I have refused to speak on panels where known criminal hackers or apologists for criminal hacking are to speak. However, I have spoken at conferences where such people were in attendance or where they spoke in their own sessions. But having our university sponsor SecurityFocus lists seems perfectly acceptable to me as a security professional.

If readers are interested in contributing to this topic for a follow-up column, I will collate correspondents’ responses into an article. Please let me know whether and how to identify you when I quote your comments (e.g., with or without employer affiliation, title and so on). I will send the draft of their edited comments back to each contributor selected before publishing the compilation.

My thanks to President Schneider for authorizing public discussion of this interesting issue.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance at Norwich University in Northfield, VT. Mich can be reached by e-mail at mekabay@gmail.com; Web site at
Copyright © 2006 M. E. Kabay & P. R. Stephenson. 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.