Regular readers may recall that in early January 2007, we distributed a column I wrote about Norwich University’s support of a discussion group that posted news about a questionable conference.<http://www.networkworld.com/newsletters/sec/2007/0101sec1.html> My colleague Dr Peter Stephenson, PhD, CISM, CISSP, FICAF and I expressed a yawning lack of concern about the association.

One correction I want to post in public is that I was mistaken in writing, “Code of Ethics <https://www.isc2.org/cgi/content.cgi?category=12> which requires CISSPs and other holders of the organization’s professional certifications “To discourage such behavior as….” As several alert readers pointed out, what I quoted is not a requirement but only “Objectives for Guidance” and the Web page clearly states, “These objectives are provided for information only; the professional is not required or expected to agree with them.”

Readers interested in the full-disclosure debate may want to read some articles published in this newsletter some years ago:


On that note, MSIA 2007 graduate student Timothy MalcomVetter, CISSP sent me some heartfelt comments which I am publishing here with his full collaboration. The remaining text is Mr MalcomVetter’s own work with some minor editing.

* * *

To the audience of Professor Kabay’s column this self-reflection may not seem important, but I do not want to skip over this point: I consider myself to be a free-thinking person in general; moreover, I am almost never the person who takes the most traditional position on any subject.

As a security professional, I understand the nature of those like me. Quite possibly the most overlooked characteristic of people who “get security”, as Bruce Schneier puts it in his text _Beyond Fear_ (2006, Springer, ISBN 0-387-02620-7) <http://tinyurl.com/29xto8> is the rule-breaker mentality, the ability to walk through a retail store and immediately recognize its security weaknesses. By nature, traditionalists rarely challenge social norms; hence traditionalists do not make great security professionals. Since the world needs security people
and since security people tend to break rules, it therefore seems perfectly acceptable to many people to extend these rule-breaking tendencies to the realm of the full-disclosure debate. However, releasing attack details and exploit code is just plain irresponsible.

Professor Stephenson selected the adjectives “enlightened” and “technical” to describe security professionals who value the observance of hacker-fests. I disagree that any reputable security researchers or practitioners should associate with hacker conventions. But more important, I disagree with the notion that full disclosure is good.

Dr Stephenson brought an argument commonly made when justifying the attendance of these events: that full and complete disclosure (i.e., with specific details of how to exploit a vulnerability, often accompanied by exploit code) prevents zero-day attacks, and since many of these details are released in hacker forums, attendance by legitimate security professionals seems appropriate. What research has been fielded that validates the claim that zero-day attacks decline because of exploit code publication? Besides anecdotal evidence, is there any hard evidence that shows that organizations and individuals are safer because a security researcher has posted his exploit of the latest bug on BugTraq <http://www.securityfocus.com/archive>? Doesn’t it seem more reasonable that some of these people are using the postings to market themselves as better security researchers, or that the proliferation of malware is higher because supposedly reputable security researchers handed-out exploit code that the malware authors can append to their latest bot code?

It seems to me (yes, this is just an impression) that those in favor of full disclosure share a common ideology: a belief that information should be free, a belief that the ends justify the means, and a belief that a grass-roots underground effort is the only way to modify the behavior of the big guy—the corporate software vendor.

As for Norwich University’s MSIA program sponsoring an open forum where invitations to fallacious and irresponsible events could abound, there’s clearly a fine line to be drawn. In general, there are valuable and varied opinions flourishing in these types of forums. Obviously no sponsor could be responsible to the point of agreeing with all of them. But advertisement on the discussion-group page <http://www.securityfocus.com/archive/105/445936> could be mistakenly interpreted endorsement of the pro-hacker conference.

As for hacker conventions in general, whether it’s DEFCON, Blackhat, PAKCON, or even Al-QuedaCON (fictional), the point is the same: it is disreputable and counter-productive for security professionals to associate with those who handle the health of our networks with flippant disregard.

I leave you with this analogy: Publishing exploit details is like having public safety advocates publishing locations of playgrounds where children are not safe because they are not supervised by adults; although child safety may improve in the long run, the possibility of direct harm by pedophiles makes this approach unwise. We are in the business of information safety and our organizations’ data are like our children.

* * *

Tim Malcolm Vetter, CISSP is an information security strategy analyst in the Midwest who has been working in the healthcare and consumer product goods vertical markets for the past several
years.

* * *


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:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 Timothy C. MalcomVetter & 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.