The full-disclosure debate continues with a contribution from Prof Ric Steinberger, CISSP, CISM. As usual with contributions to this newsletter, the rest of this article is entirely his with minor edits:

***

One of the most consistent and brilliant writers on the topic of vulnerability disclosure is Bruce Schneier. For many years he has argued that the _only way_ to force software publishers to _promptly_ fix security vulnerabilities in their products is to publicly publish the technical details of the vulnerabilities. His recent article in _CSO Magazine_ summarizes his ideas <http://www.csoonline.com/read/020107/col_sec.html>. Scheier’s position is at one ideological end of the spectrum. The other end would be that researchers who discover vulnerabilities should privately contact the software vendor and tell no one else nor take any other actions.

My own position is that there is no “always correct” response that vulnerability researchers should follow. There are situations where, after repeated communications by the discover of a vulnerability with a large software vendor, that vendor refuses to acknowledge the vulnerabilities or refuses to agree to release patches by a specific date. Sometimes, in frustration, the researcher resorts to full disclosure). In many cases, this has the effect of forcing the software vendor to reprioritize, and to develop and release appropriate patches. One would hope that in most cases software vendors are more willing to act quickly when they are notified of vulnerabilities in their products. Bruce Schneier pursues his full disclosure position because in many cases, large software vendors have not acknowledged or responded promptly.

Full disclosure may work with larger vendors in the sense that it usually forces them to respond more rapidly to vulnerabilities in their own products than they otherwise would. This is generally a good thing for customers, and one could argue, this is what the vendors should be doing anyway without being blackmailed through full disclosure. But is full disclosure also an appropriate approach towards small to mid-sized software vendors? In many cases, these companies have many fewer resources (and customers), and are far less able to quickly respond to identified vulnerabilities. The optimal solution would seem to be that these companies should welcome _private_ disclosures of product vulnerabilities and work cordially with the discovers to develop patches. Of course not every software vendor is able or willing to do this, and thus may be forced to confront the consequences of full disclosure.

(In our next column, Prof Steinberger continues with an interesting case study of full disclosure.)

***

Ric Steinberger, CISSP, CISM is Adjunct Professor of Information Assurance in the MSIA Program at Norwich University and the founder and president of Sierra Computer Strategies
(SCS), an information security consulting firm. Prior to forming SCS, Mr. Steinberger worked for several Silicon Valley high technology companies including SRI International, SRI Consulting, Nuance Communications, and Security Portal.

* * *


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 Richard Steinberger & 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.