The full-disclosure debate continues with the second part of a contribution from Prof Ric Steinberger, CISSP, CISM. In the first part, he discussed the effects of full disclosure on companies of different sizes. In this concluding section, he tells us about an interesting case study of those effects.

***

A few years ago, I [Ric] worked for a large US-based software vendor, which I will call the PQR Corporation. A European-based researcher had been sending lots of information about vulnerabilities in PQR’s products to PQR product security staff. PQR had not been especially proactive in responding, either in releasing patched products or in communicating with the researcher. This situation led the researcher to fully disclose technical details of many of the vulnerabilities he had discovered, and this caught the attention of a large number of PQR’s most important customers. Not surprisingly, the trade press picked up the story and much unwelcome PR was generated. The net outcome was that, after much internal strategizing, PQR agreed to issue quarterly patch releases to all customers and promised to promptly fix all known security vulnerabilities.

Normally, that would be the end of the story. But PQR had established a fairly new hosting service where customers could run their PQR applications and store their data (thus saving them the expense of using their own data center). PQR’s hosting service was not suitably prepared for these quarterly patch releases, and the first time one was released, the operations staff was not ready to apply them. Failing to apply PQR-released patches in a timely manner in PQR’s own hosting center would have been unacceptable. Thus, after many meetings, tests, and other preparations, the PQR operations staff began deploying PQR patches inside the company’s data center. Overall, a good outcome for PQR and its customers, and one that might not have happened without full disclosure. But there were many stressful days at PQR before this happened.

In summary, it seems to me, agreeing with Bruce Schneier, that full disclosure generally does what it is intended to do: forces software vendors to promptly correct security vulnerabilities. But whether full disclosure is always the optimal strategy that ethical vulnerability researchers should use remains uncertain, especially when the companies are small and the software products are not widely used.

***

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.