Responsible Vulnerability Disclosure
by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In a previous column, I pointed out that some people have threatened companies with full disclosure of security flaws unless they were paid money to provide the details of those flaws privately. I wrote that this behavior seemed to me to come pretty close to extortion.

But isn't it normal for someone to charge for access to their knowledge? Why shouldn't someone offer to trade their pointers on a vulnerability in exchange for money? Isn't that what consultants and employees do all the time? After all, when a security specialist is working for an employer or for a client, how is getting paid for their penetration testing or advice on quality assurance or recommendations on security policy any different from offering to tell a firm about a security vulnerability in return for a fee?

One way of thinking about the difference is to think about ordinary life. Haven't we all pulled up next to a car and notified the driver that their brake lights don't work? Would you refuse to tell the driver about their brake lights unless they paid you a fee? How would you feel if someone said, "If you give me <a large amount of money> I'll tell you about a dangerous problem with the safety system of your car." Would you perceive the offer as a legitimate invitation to engage in a commercial transaction? I wouldn't. I make it a personal hobby to spot cars with all their brake lights out and to tell the drivers about it as soon as it is safe to do so. I figure that my Goody Two-Shoes hobby may have saved a few lives in my thirty years of driving.

There are many faithful contributors to RISKS, BUGTRAQ and other lists who routinely warn software companies about problems at no cost. I personally know many security experts who have warned companies about threats and vulnerabilities without expecting monetary reward; indeed, many people speak at conferences for no pay at all to share their knowledge and experience freely with colleagues. Thousands of individual professionals, scholars, non-profit organizations and companies and government agencies contribute countless pages of useful information on the Web at no cost to the recipient.

The warnings are often carefully structured so that enough information is provided to help identify the vulnerability but not enough to let the clueless wannabees launch attacks using precise scripts.

These folks are doing the cyberspace equivalent of giving blood. I am sorry that there are people whose economic circumstances make it reasonable to sell their blood, but that doesn't change my admiration for those who donate blood freely (I'm into my 8th gallon).

So returning to extortion, I think the issue here is the sense of community. Those of us who feel that we are all in the battle against computer crime together feel the same obligation to help a vendor or a system improve as we do towards other drivers who have burned-out brake lights. I see this spirit of collegiality whenever I'm talking to colleagues who are in one sense direct competition for my employer – yet we feel a camaraderie in trying to fight computer crime and abuse. Rarely have I seen hostility among consultants working for different firms, let alone with that thin line of security professionals in corporations, government departments and other organizations who work day after day to protect the interests of their employers and their
stakeholders.

Unfortunately, some of us feel isolated and excluded from the wider society. Anomic people do not feel the sense of connectedness that makes it feel good and right to share knowledge freely. For people who feel like outsiders -- for example, some of those involved in the criminal hacker subculture -- helping others altruistically may not make emotional sense. For these folks, an argument to consider is that helping others as a professional courtesy is a far better way of forging one's reputation as a trustworthy and helpful resource than trying to extort payment by withholding information.

* * *

In the next and final part of this series, I'll look at practical guidelines for companies and for users on reporting and handling vulnerabilities.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 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.