Some years ago, I was having a chat with a student and we started talking about people who release details of vulnerabilities to pressure software firms for rapid fixes to problems. The student felt that releasing details of security vulnerabilities was a good way of forcing companies to pay attention to weaknesses. He told me that in his company, where he is a security administrator, he and his colleagues told a major vendor about what they considered a serious vulnerability in a firewall. Months went by without action. Finally they lost their patience and posted full details of the vulnerability in an appropriate USENET group – and the problem was fixed within days.

I said this smacked of extortion and told him about various times when computer security specialists had actually gone further than merely posting information but actually demanded payment NOT to do so. For example, in the RISKS DIGEST 20.82, a correspondent wrote about a case of quality assurance failure in the Paris subway system. Peter Wayner <pcw@flyzone.com> wrote:

"The *Times* (London) reported on 26 Feb 2000 that Serge Humpich, a hacker, was convicted of fraud and given a suspended sentence. The young man discovered how to trick the Carte Bleue system and claimed he could have gone on an unlimited spending spree. Instead he hired lawyers and negotiated with the company that runs the system for payment in return for detailing the problems. The company turned around and prosecuted him for fraud after they arranged for him to demonstrate the system. What a brilliant way to discourage folks from rooting around in a system _and_ reporting security flaws! I wouldn't be surprised if their system proves to be so impervious that the number of bug reports drop to zero. What a wonderful solution for creating bugfree code!"

I can see the author's point: punishing people for pointing out quality assurance flaws is hardly going to encourage wide contribution to quality assurance. However, it seems to me that the issue was not the identification of a security flaw; the problem was that M. Humpich tried to get payment for his knowledge of the security flaw he found by withholding that information unless he were paid.

This was not the first case where someone tried to get payment for information about a bug they have discovered. In June of 1997, Christian Orellana, a Danish computer consultant, threatened to release information to the press about a serious security weakness in Netscape Navigator unless he were paid more than the $1,000 prize offered by Netscape to encourage independent quality assurance tests. His message included the words, "I think the person most suited for handling this is somebody in charge of the company checkbook. . . . I'll leave it to you to estimate what impact that would have on Netscape stocks." His actions were almost universally reviled by professional security specialists. Ironically, Netscape already had a program in place to reward volunteers who notified them of bugs. They refused to pay the consultant the $1,000 honorarium he would have received had he not demanded the larger payment.

Now, extortion is defined as "the act or an instance of inducing or attempting to induce someone
to do something by threats, real or false criminal accusations, or violence." It seems to me that the men in both stories above were coming pretty close to extortion.

* * *

In the next column, I’ll put the idea of demanding money for information about a security weakness in a wider context.

* * *

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.