INFOSEC, Quality Assurance and Extortion

by M. E. Kabay, PhD, CISSP
Professor of Computer Information Systems
Norwich University, Northfield, VT

I was having a chat with a student at the latest Common Body of Knowledge (CBK) review course in Washington DC this week. The eight-day CBK course is from the (ISC)^2, the body that controls the CISSP designation (Certified Information Systems Security Professional). [For more information about the (ISC)^2 and the CISSP, visit < http://www.isc2.org >.]

Anyway, in our conversation, the student and I started off discussing the issue of full disclosure of security vulnerabilities, complete with technical details and even exploit code. I argued that there were better ways to contribute to security than to make powerful exploits available even to cyberspace sociopaths and even children. But then we shifted the discussion to 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 [see < http://catless.ncl.ac.uk/Risks/ for html and < ftp://ftp.sri.com/risks/ >for text], 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 is not the first case where someone has 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 guilty of 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 7th 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.

Corporations have to shoulder their share of the blame for the frustration felt by users who fruitlessly batter at their doors to get a hearing. Yes, corporations do have priorities for using limited resources, but the frustration comes from not being listened to. From experience in technical support, I'd say that the critical elements in gaining the cooperation of users who are experiencing difficulties are

! paying attention to the calls for help or for repairs;
! having a systematic method for tracking all calls and correlating problems so that you know what is causing most of the trouble;
! a system for assigning priorities to specific fixes or repairs;
! reliable, frequent communications with the people who called in the trouble report;
! involving the callers in solving the problem if possible.

The worst thing a company can do is brush off a trouble report; the next worst is to claim that they will resolve the problem when in fact there is no intention to do so. Honesty is essential in all our work, and especially when dealing with clients and with the public at large.

When I was an operating-systems and performance specialist for Hewlett Packard in the early 1980s, it always seemed wonderful to me that HP consistently published a complete list of all the known problems they had registered for their products. The Systems Status Bulletin was published quarterly, with biweekly updates; it was a compendium of all the problems that had been localized in every software product the company made, with patch numbers for those that were fixed, release numbers for patches that had been integrated into installation releases, and workarounds if possible for those problems that were not yet fixed.

I recommend this honest and complete approach to all companies, especially those working with security products.

Finally, users and specialists should understand that using the threat of publishing detailed exploits – or actually publishing them – is a crude, extreme and unprofessional approach to resolving a problem. Instead, try to build pressure using a graded series of actions instead of jumping to threats:

! define a timetable for acceptable responses that takes into account the severity of the security hole – don't ask for instant repairs on a minor item;
! contact higher levels of management at the vendor firm to discuss the issue;
! get the cooperation of upper management in your own firms, if appropriate;
! arrange for face-to-face meetings between the top managers of your firm and those of the vendor firm;
! contact your professional colleagues for joint letters pressing for a solution;
! raise the issues in professional forums (USENET, mailing lists, professional association meetings) without giving enough details in public that would allow instant exploits by the black-hat crowd;
! set up a BOF at an upcoming meeting specifically to discuss solutions and workarounds to a longstanding or fundamental design problem;
! look for alternative suppliers – and make sure that you do so openly by telling your supplier you are not satisfied with their product quality or their service;
! contact certifying bodies to withdraw certification of products that remain unrepaired for a long time after notification;
! get your corporate counsel involved to discuss possible legal action for breach of contract if possible;

! publish public attacks, again without giving away too much detail.

In summary, I think that a sound approach to preventing extortion in our business involves making it unnecessary by establishing norms for professional, collaborative responses to reports of vulnerabilities. The other powerful tool we can use is peer pressure: let's establish a consensus about not trying to extort compliance with our own priorities when we run into trouble with software and systems. But in any case, demanding money to avoid publication of a vulnerability is just plain sleazy.

In the world of INFOSEC, we need people who are the equivalent of blood donors, not blood suckers.

* * *