



## Opportunity Knocks

**My weary friends who work in IT** feel like they've had more than their fair share of opportunity lately. Opportunity to deal with the Blaster, Nachi and Sobig.F worms that filled inboxes and network pipes far and wide. And, for those in the Northeast, opportunity to test their UPSs and contingency plans thanks to the biggest blackout in North American history. (The blackout caused more than a few gray hairs for the IT people at our offices in New York and on Long Island, though luckily our labs were spared.) It's been a learning experience, to say the least.

The Sobig.F virus exacerbated an already pervasive spam problem. On Wednesday, Aug. 20, 454 messages were sent to my e-mail address, according to our server logs. After making their way through our tiers of spam and virus protection, 86 of those messages got to my inbox. That's a ratio of about 5 to 1. (Incidentally, only 21 of those messages were press releases. Note to vendors: These were not classified as spam.)

When the workaround becomes more work than it's worth, it's time for us to demand or develop a real solution. Have we finally reached that point? Will the next round of the Sobig virus force us get off our butts and solve the underlying problem? What *is* that problem? And what is the solution?

Ultimately, most IT problems stem from a combination of technical and social issues, and so do the potential solutions.

### Quality Counts

**On the technology side**, it comes down to quality. How good is our hardware at handling a significant power surge or excessive environmental factors, such as heat and humidity. Is our software buggy? Are the vendors releasing patches faster than we can test and implement them?

Often the answers to these questions come down to specific decisions vendors made during product design and development. Netgear hardcoded a University of Wisconsin SNTF server address into several hundred thousand of its routers, for instance, effectively creating a DDoS on the school's network this summer—see [www.cs.wisc.edu/~plonka/netgear-sntp](http://www.cs.wisc.edu/~plonka/netgear-sntp) for details. (If you bought a

Netgear router recently, please update your firmware now to advance the bug-removal effort for my alma mater!)

Protocol quality counts, too. Take SMTP. It's an aging protocol that was designed for more trusting networks than those we run today. It has characteristics that make it easy for people to spoof e-mail addresses and disguise their origins, facilitating spam and viruses. NETWORK COMPUTING lab director Ron Anderson said it best: "The great thing about SMTP is it allows a free flow of information everywhere. The terrible thing about SMTP is it allows a free flow of information everywhere." The IRTF's Anti-Spam Research Group ([www.irtf.org/charters/asrg.html](http://www.irtf.org/charters/asrg.html)) is actively working on ways to combat this problem.

Even protocols designed with security in mind have their problems. WEP (Wired Equivalent Privacy), for example, is not as secure as originally hoped. We're betting on 802.1x, though.

### Human Nature

**We're all responsible** for being good network citizens, not only for the health of our systems but for the well being of the Internet community as a whole. Every action, or inaction, can have unintended consequences. Security patching, for example, is an imperfect process aimed at fixing imperfect products, and sometimes a patch that solves one problem causes another. This makes automated patching a bad idea for those running mission-critical services. They must go through a quality-assurance process with each patch.

To make matters worse, virus and attack writers know they can rely on human curiosity. Until we can convince users to resist the temptation to open unrecognizable e-mail attachments, e-mail-distributed viruses will remain a force to be reckoned with.

Meanwhile, we need to insist that our software and hardware providers produce the highest-quality products possible. And if they don't, we have to start making tough choices about whether to stick with them. **NWC**



Most IT problems stem from a combination of technical and social issues—and so do the potential solutions.



Mike Lee is NETWORK COMPUTING's editor. Write to him at [mlee@nwc.com](mailto:mlee@nwc.com)