I don’t know if you feel the same way, but I’m growing tired of constantly worrying about computing security, cybersecurity, and the like. I have the uneasy feeling that all the warnings, threats, mitigation strategies, and precautions are simply forestalling the inevitable—a massive cyberattack on some critical infrastructure leading to widespread destruction and panic. But I also fear that too much focus on cybersecurity leaves us vulnerable to more conventional attacks.

There are few moments spent working on my computer when I’m not reminded—no, hectored—about computing security. From power on, I need to enter a password to complete the boot sequence, another password to connect via VPN to my network, another password to get to my email client, and more passwords to use any of the many web-based communities to which I belong (including the IEEE Computer Society’s). Many of these passwords age, so I have to keep track of several cryptic tongue-twisters; I’m judicious about not writing them down, saving them in a file, or transmitting them in any way. I’m even paranoid about leaving my office for just a few moments with the door open and the computer on—never mind that the system locks after three minutes of inactivity, which is an annoyance when multitasking. I’m so preoccupied with these security precautions that I often leave behind my keys and cell phone, or forget some other important item when I leave my office.

But I’m not the only person or entity engaged in this form of paranoia. Approximately every 10th email I receive is either immediately deleted or tagged as suspicious by one of two spam filters (on the server and on my laptop). However, the filter isn’t foolproof: sometimes legitimate, important email gets snagged, requiring a manual hunt, and I’m always dismayed to learn that some of my messages end up in a similar state on the recipient’s end. Other emails received from my employer, professional organizations, or friends warn me of imminent scams, malware, and various threats. It’s to the point where I’m afraid to even open messages from unknown senders.

This paranoia has transcended my inbox and manifested itself on the Internet, too—before visiting any web site, I’m “advised” about its security by my site advisory software; an aggressively tuned popup blocker often prohibits the display of certain content without explicit permission. But as with the spam filter, I wonder if I’m missing out on important information that’s blocked erroneously, or if I’m being shortchanged because I decline to visit sites that might be useful to me (and relatively safe). Vendors try to assure that online purchases are “secure,” but their constant reassurances have the opposite effect. I often shy away from patronizing certain vendors out of fear. News sites repeatedly report the same security story: recent hacking incidents by punks, cybercrime, cyberterrorism, and government-sponsored cyberwar. The countermeasures make the news, too. Reading magazines, newspapers, or watching TV news provides no diversion because cyberissues are big news in these more traditional forms of media, too.

I’m sure that my experiences aren’t unique. Our lives have become increasingly tedious, frustrating, and unproductive because of our heightened security awareness. Passwords are forgotten, files lost, work scuttled, and all because of bungled security precautions. In what other endeavors are we so security obsessed? Yes, we have locks on our homes and offices, perhaps alarms, dogs, and even guns. But do we think about security every 30 seconds at home (when not on a computer)?

We’ve become a paranoid cyber society, and I believe we’ve...
reached the point of no return. With our hyperfocus on cybersecurity, what aspects of critical infrastructure are left unsecured? Are we so focused on securing the Internet that we’ve left ourselves more vulnerable in our airports, ports, bridges, and tunnels? What about our food and water supplies and energy infrastructure? All of these systems are vulnerable to cyberattacks of various kinds, but what about conventional attacks by human agents using explosives, chemicals, or biological weapons? Biological attacks can propagate as rapidly as an Internet virus and use a similar pathological mechanism. What would happen if someone combined cyber and conventional attacks?

Does our obsession with cybersecurity come at the expense of reduced physical security? What doors are you leaving open, what keys and cell phones have you left behind while trying to remember your latest password? As IT professionals, we all must be as vigilant in protecting ourselves from the physical threats as we are of the cyber ones. This means managing your physical space carefully, both at home and at work. Be careful whom you invite into your home and work space. Enforce physical access restrictions to the data center. Take precautions when traveling. You should increase your personal paranoia level. I have.

Phillip A. Laplante is professor of software engineering at Pennsylvania State University. His research interests include software project management, software testing, requirements engineering, and open source software systems. Laplante has a PhD from the Stevens Institute of Technology. He’s a fellow of the IEEE and a member of the IEEE Computer Society’s Board of Governors. Contact him at plaplante@psu.edu.