

Network Security versus Personal Computing: Which Will Win?

I start by recalling a simpler time, back when personal computing and networking were thought to be compatible. This may lead you to think that these paragraphs are a paean to the good old days and that therefore I am a naively nostalgic geezer. But they aren't, and I'm not. Hear me out. Higher education has a tough choice ahead, and its origins lie back in a simpler time.

My first personal computer—let's define "personal computer" as one that is not shared with others and that the user can equip and configure as he or she sees fit—was a two-floppy Rainbow, a short-lived Digital product with its own peculiar version of DOS. On my desk, the Rainbow joined a Lear Siegler ADM-3 smart terminal ("smart" then meant that remote hosts could move the cursor around on the terminal screen), which had a direct hard-wired serial connection to a Digital time-sharing computer, a PDP-11, if I recall correctly. Using my ADM-3 terminal, I could edit the content of files on the PDP-11 and instruct that computer to compile, execute, or process them in various predetermined ways. The dominant use for my terminal was entering, editing, and analyzing statistical data. Until the Rainbow arrived, I also used the terminal to enter text, to sprinkle it with text-processing commands, and to process the result into printed reports.

With my new Rainbow, in contrast, I could use a word-processing program, usually Final Word, to see and manipulate on the screen how my report would actually look when printed. The software was on one removable floppy disk; the report files were on another. By removing the word-processing disk from the Rain-

bow and substituting a VisiCalc disk, I could do some limited data analysis and prepare well-formatted tables and graphs. My large raw statistical datasets and software remained on the PDP-11, accessible only through the ADM-3.

Early personal computing, for me and many others, thus comprised a few applications, but only one at a time; early networking comprised a single physical pathway from terminal to host. There was no conflict between the two. But two screens on one desk seemed silly, and so did physically removing disks to use different software; the time-shared PDP-11 had long before moved to shared storage and multiple applications running at once. Soon personal computing and networking evolved. Inexpensive hard-disk drives did away with physical application switching, terminal emulators did away with terminals like my ADM-3, and protocol-based networking did away with physically hard-wired networking. In time, multiple simultaneous applications on personal computers came to communicate in myriad ways with all kinds of other computers and devices, rather than simply emulate a "terminal" talking to "hosts."

The protocols for managing communication over shared networks became more complex, going beyond simple routing and transmission to manage competing demands on capacity and to accommodate creative new applications. Functionality and convenience expanded dramatically. Personal computing and shared networking had married, in due course creating the networked personal computer, client-server computing, and the Internet. The marriage

was a great success, a truly transformational innovation. Yet in retrospect, the seeds of today's conflict were evident already: the goals for personal-computing progress were user flexibility, autonomy, and control, whereas the goal for networking progress was automated management of a shared resource. One sought autonomy, the other authority.

Let's return to the present. My mother, far from a technophile, uses a 2-GHz E-Machines computer with a flat screen, a color printer, a DVD player, a CD burner, an Ethernet connector, and a built-in modem. The computer is set up just the way she likes it. She typically runs at least four applications simultaneously: the AOL suite (mostly Web browsing, e-mail, and instant messaging), a word-processor, a database, and a graphics viewer. She enjoys the kind of flexible multitasking that I could only dream about with the Rainbow. Since for the moment the only connection from my mother's computer to the outside world is dial-up AOL, the network rarely intrudes—even though through AOL she uses myriad servers and services worldwide to bring her e-mail, instant messages, Web pages, financial information, and electronic commerce.

But soon my mother will add DSL service to her setup—real networking, which puts her computer on the Internet all the time. No longer will the telephone system stand between her and the Internet. This will bring great speed to her Internet interactions, but it will also bring danger. My longstanding advice to her about virus-checkers, firewalls, and backup—none of which she understands or, frankly, should have to understand—will

suddenly become less academic. Her software will begin updating itself at night. She'll be leaving her computer on all the time, even when she's not using it. Subtly but suddenly, she will be at the mercy of every network malefactor her ISP lets near her machine. More important, her failure to consider and respond to these new threats and risks will jeopardize others. Her ISP—not to mention her son, daughters, friends, and other advisors—will be telling her that she has to do this or that, lest disaster strike. Either her autonomy will shrink, or the quality of her

community provides unprecedented access to very diverse services, but its price is compliance with network and computing standards. My mother would hate having her computer on the University of Chicago's network. My networking staff would too.

It should have been clear, back when my ADM-3 gave way to my personal computer, and long before my mother had to choose between good networking and simple computing, that progress hinged on compatibility between two fundamentally incompatible trends: increasing

personal computing to maximize security. The typical ISP limits security commitments to minimize constraints on its customers. The typical college or university does neither. It thus finds itself spending exponentially more on network management, incident response, and small-scale disaster recovery. And the typical college or university CIO—someone like me—receives an increasingly vituperative array of how-dare-you-tell-me-what-to-do e-mails and voice-mails. More problematic and expensive in the long run, the typical college or university finds itself using hor-

rendously complicated mechanisms to induce computing homogeneity and network security in its environment while publicly celebrating free choice and individual or departmental autonomy.

Obviously, this unmitigated conflict cannot continue. Equally obviously, given the legal and substantive risks, network security and therefore authority will trump autonomy and personal computing. Colleges and universities will impose increasingly stringent requirements on network users, using both policy and technology to reduce risk. The challenge, at this point, is rhetorical rather than technological. Colleges and universities should be focusing not on whether security requirements will constrain users—generally

the focus today—but rather on how to find the right balance among rewards, punishments, and technology, how to frame the issues so that users understand them and come to consensus, how to maintain functionality in the face of restriction, how to compare fixed and probabilistic costs and benefits, and how to maintain participatory governance when understanding options requires technological sophistication.



citizenship will decline. Personal computing will conflict with networking.

Yet my mother is lucky: she's not on the University of Chicago network. If she were, her choices would be limited by policy rather than advice. To run a computer without virus protection or a host firewall, for example, or to use a simple password, or to not keep application software updated, is to invite compromise by outsiders. Compromise, all but certain for the inattentive, guarantees that one's computer will be removed from the network for attacking others; even vulnerability to compromise, if detected by my network-security staff, can lead to this result. The high-speed networking interconnecting the University of Chicago

capability and autonomy on the personal computer; and increasing security and manageability on the shared network. You can't have network security if people have unconstrained personal computers on your network. If you have network security, then you aren't allowing unconstrained personal computing. Perhaps uniquely among large organizations in today's technologically intensive world, colleges and universities have pretended this conflict doesn't exist. Those of us in higher education want not only to give our constituents license to do what they will but also to protect them from the predictable consequences of their choices. We can't do both.

The typical corporation limits per-

Gregory A. Jackson is Vice-President and Chief Information Officer at the University of Chicago. He is the Viewpoints department editor for *EDUCAUSE Review*.

