On July 30, 2007, Vauhini Vara published an article in the _Wall Street Journal_ (WSJ) entitled, “Ten Things Your IT Department Won’t Tell You.” <http://online.wsj.com/public/article_print/SB118539543272477927.html> The author explains that office workers like to use corporate-supplied equipment to “keep up with our lives. We do birthday shopping, check out funny clips on YouTube and catch up with friends by email or instant message.” Alas, she continues, “Our employers sometimes don't like it. Partly, they want us to work while we're at work. And partly, they're afraid that what we're doing compromises the company's computer network -- putting the company at risk in a host of ways.” Therefore, she explains, she has asked various experts for ways “to get around the IT departments.”

The ten topics she investigates are as follows:

1. How to send giant files.
2. How to use software that your company won’t let you download.
3. How to visit the Web sites your company blocks.
4. How to clear your tracks on your work laptop.
5. How to search for your work documents from home.
6. How to store work files online.
7. How to keep your privacy when using Web e-mail.
8. How to access your work e-mail remotely when your company won’t spring for a Blackberry.
9. How to access your personal e-mail on your Blackberry.
10. How to look like you’re working.

Vara provides each topic with these sections:

- The Problem
- The Trick
- The Risk
- How to Stay Safe.

I don’t want to get into a discussion of full disclosure of security vulnerabilities here, nor to claim that what Vara has done is in any way illegal. What she and her publication have done, however, is beyond my personal standards for publication in a legitimate, respected newspaper. The motivations behind her detailed instructions are much closer to the dreck published in criminal-hacker publications than in any professional publication I can imagine.

The author’s focus is on escaping the consequences for violating security policies. For example, in the section on visiting forbidden Web sites using corporate systems, she writes that “the main risk is getting caught by your boss.” As a second-rank risk, she mentions the possibility that “Online bad guys sometimes buy Web addresses that are misspellings of popular sites, then use them to infect visitors' computers…” Her priorities are to protect people who put the organization at risk and only secondarily to warn the potential rule-breakers of threats to their employer’s data security.
Vara’s “How to Stay Safe” sections are astonishing in their insouciance. For example, her “safety” measures for violating appropriate-use policies include this advice for attempting to wipe audit trails: “Clear your private data as often as possible. Better yet, don't use your work computer to do anything you wouldn't want your boss to know about.” The first sentence clearly condones the misuse of corporate equipment and encourages dissimulation and dishonesty as a safety measure. The second defines the issue entirely in terms of self-protection, with no hint that there might be issues of rights and duties involved.

I invite readers to read Vara’s article for themselves and then to join me in a short series of columns as I analyze her work from an ethical standpoint. I will take the opportunity to illustrate a straightforward process for making ethical decisions that I think would have ensured that Vara’s article not be published – if the editors of the Wall Street Journal actually care about ethical decision-making.

My editor Jeff Caruso kindly pointed out a vigorous blog entry on August 3rd by Network World writer Linda Musthaler about the Vara article bluntly entitled “At the WSJ, the idiots are running the asylum.”<http://www.networkworld.com/community/node/18101> Ms Musthaler points out that the WSJ published a follow-up article by Vara that could conceivably be an attempt to compensate for her scandalous “Ten Tips,” but I’ll let you judge for yourselves.

More next time.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekebay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 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.