A traveling dean needs some sensitive data immediately. Reading tables over the phone won’t work. A messenger is slow and expensive. You could fax, but hey, the data are on your computer already, so you decide to e-mail them.

Are you right to trust e-mail for this private, sensitive communication? Some say “no”–computers aren’t secure; hackers can penetrate mail servers, and strangers on the Internet can read e-mail in passing. On the other hand, in practice each of these risks is small—certainly no greater than those in campus paper files, you’re probably okay. This is because a message’s separate packets out of that stream. Each of these presents forbidding obstacles to anyone trying to eavesdrop. So is e-mail security. First, tell everyone—e-mail users, system operators, and network architects alike—about the reasonable measures that they and their correspondents should take. Second, encourage every- one to exercise the same care with e-mail that they do with other conversations. Third, encourage IT practices and architectures that improve rather than degrade privacy. Fourth, begin thinking about encryption. If a message is encrypted, even if I learn the risks I list above—interception, unauthorized retrieval from servers, even stolen computers—become much less important.

Most of all, the continuing trust-worthiness of e-mail depends on the continuing application of common sense by you, by your e-mail correspondents, and by your IT people. Private e-mail generally stays private, especially in transit. It arrives promptly and is useful form. It is trust-worthy. You were right.

Gregory A. Jackson is Chief Information Officer at the University of Chicago (e-mail: gjackso@uchicago.edu)