IT SECURITY CORNER

SECUR IT

Privacy? Do we *need* privacy?

Computer security professionals will often refer to *confidentiality, integrity* and *availability* as the three basic concerns that form the nucleus of any serious study of computer security. Of these three, ***confidentiality*** is the concept most often tied to security, with *integrity* and *availability* looked at by laypeople as strict "system" issues. The reality, of course, is that all three are equally and vitally important security concerns.

Confidentiality is really a two-sided coin. You are probably familiar with the concept of having to safeguard information on computer systems because it's sensitive or "in the National Interest," and you certainly realize that harm could come to some interest if the information were divulged to the "wrong" people.

Less often realized, though, is that ***confidentiality*** involves "right to privacy" issues. The reality of corporate computing environments worldwide tends to run a range between two stereotypical extremes, with one pole being comprised of companies who insist that a company's system(s) are the property of the company and that everything done on them must be directly related to business the company does, and the other pole being the exact opposite, where the company exerts no (and may not wish to exert any) control whatsoever.

Let's presume that most corporations aren't at either extreme end of the spectrum, but rather fall somewhere in between those two poles. Most reasonable people would probably agree that the company has a right to expect that the equipment it provides will be used for company business, and also that the company will be flexible, and "human" enough, to realize that, from time to time, the equipment may get used for personal purposes that do not interfere, or cause a conflict of interest, with company business.

So where does the Department of Foreign Affairs and International Trade stand on this? Certainly, for official departmental work, it is expected that employees will process, store and transmit data on systems approved for those purposes, and respect the sensitivity limitations of those systems. Do not use SIGNET-D (the "designated" version of SIGNET, and what you have on your desktop – as opposed to the "classified" version of SIGNET – or SIGNET-C) to process, store or transmit anything above the sensitivity of PROTECTED-A. The system absolutely does not provide adequate enough measures to safeguard material of a higher level of sensitivity. Ask yourself if you would be comfortable reading the information on the front page of tomorrow's newspaper. If the answer to this question is no, do not process it on SIGNET-D. SIGNET-D was never supposed to, never designed to, and does not adquately safeguard anything more sensitive than PROTECTED-A – and it does that job quite well.

But what about "personal" stuff? How many people do you think *ought* to be able to read your e-mail? How many people *can* read your e-mail? What expectation of privacy should you have if you choose to process information on SIGNET-D, if you choose to print on SIGNET-D, and/or if you choose to save data on floppy disks, your local C: drive, your I: drive or your H: drive? Presume that you don't have much privacy at all on SIGNET-D. Certainly, if you're going to be processing something that's personally sensitive, your best bet is probably to save your data to floppy diskettes and store those in a secure place.

There are certain things that every SIGNET-D user ought to know in order to make informed choices about what sort of stuff they are doing on the system:

1. System Administrators usually have deity-like powers and can do, see and read everything. This doesn't mean they do read everything, merely that they can. In reality, System Administrators, like all of us, have their own share of work to do and are far too busy to be poking and prying.

2. A lot of SIGNET-D traffic (particularly e-mail destined for or between Missions) gets bounced off completely unencrypted satellites. Practically anybody with a satellite dish can get SIGNET-D traffic and read it in the clear to their heart's content.

3. When you mark your e-mail as PROTECTED, the system does not process it differently. Think of that designation as being a handling instruction to the recipient, not to the system.

4. Presume that your data is "unsecure" if you store it on your local C: drive. We've heard too many stories from people who left their computers turned off on Friday evenings, only to return Monday mornings to find games they've never heard of suddenly on their systems. People are using your computers, and will get access to any files you store there.

5. Presume that your I: and H: drives are unsecure. Your whole Branch has access to your I: drive, and lots of System Administrators have access to your H: drive.

6. Don't ever think "well, I'm only going to print...", because the reality of printing on SIGNET-D means that the "print job" leaves your computer, travels down your network cable to the server - where it stays until the printer you wanted to send it to says "okay, I'm ready, let me have it", and is thus accessible by people who have no need-to-know.

7. Don't ever presume that "nobody will read this...", because the fact of the matter is that there are lots of people who, for whatever reasons, do go looking for things to find on the system – whether they're people who are targetting you specifically or whether they just have far too much time on their hands and the same curiousity that proved fatal to the cat.

Sounds like a fairly unsecure system, doesn't it? Truth is, that's absolutely correct. It was never meant, nor designed, to be secure - and it does its job admirably. What is critically important is that users know this, which then allows them to make appropriate decisions. In these days of increased computer connectivity, what with the Internet and McLuhan's "global village", you can never get enough answers on the security of information – particularly any information about you.