IT: SECUR IT

Here there be DRAGONS

By the time faithful *Connexions* readers get this issue, the Department will have opened up access to the Internet through the firewall, negating the current requirement for outbound user accounts and passwords. Practically, this means that John and Jane Q. Employee will now be able to use their favourite browser to their hearts' content to leap and soar their way across the vastness of the World Wide Web.

Previous articles on information technology security have focussed on specific threats inherent in the "wired" world — viruses, malicious software, hackers, etc. Of no less concern are things that don't seem like threats and weren't intended to be.

For example, a departmental user recently used his browser to go to a company's WWW site, and there obtained the latest evaluation copy of their software product. During the installation process of this software, his hard drive was erased and he lost all the data that was on it. Was this a virus? No. Was it malicious software? The makers didn't think so. Was it a hacker? Nope. Was it something that we ordinarily would have thought of as a threat to our assets (both physical, in the sense of the hard drive, and intellectual, in the sense of the data that was on the hard drive)? Er, uh, well, actually, now that you've mentioned it.... yes.

The Department has lost some assets — the fact that it's intellectual property as opposed to something we normally think of as a little more tangible, such as a desk, does not alter this fact. As a departmental employee, you have a responsibility to safeguard departmental assets under your control. This includes files on your hard drive, on your floppy diskettes, in your e-mail folders, etc. As such, you must take reasonable steps to ensure that threats to these assets are minimized.

Here are some quick things to remember in your CyberDiplomatic travels:

- If you require software that is not supplied by the Department as a "corporate standard," you must ensure that you use properly purchased and licensed copies.
- Take reasonable precautions with anything you obtain from the Internet - scan software for viruses before you install and run it.
- Ask for help if you are not reasonably comfortable with installing software in your desktop environment. To the degree they are able and available, SIGNET Systems Administrators may offer some assistance. Realize that they are not obligated, and in many cases are unable, to provide any support for non-departmental standard software.
- Conduct yourself with prudence and caution on the Internet, recognizing that anything you do will be represented to the outside world as the actions of a departmental employee (at a minimum, your departmental address will be communicated to each and every site you visit and each site enroute). Make sure that any statements you make on the Internet are identified as your own personal views, unless you have explicit authority to represent the Department.

Back in the annals of maritime exploration, European cartographers used to mark unknown waters with the warning "Here there be dragons!" With a grain of salt, and an ounce or two of common sense, there's no reason you can't navigate the Internet without worrying about falling off the edge of the world.

CONNEXIONS is published monthly by the Client Services Division (SXC) and distributed in Canada and at missions abroad to all employees of the Department of Foreign Affairs and International Trade. It is available on the Intranet under What's New.

Units wishing to have a notice published in *CONNEXIONS* should forward the text to SXC with a memo signed at the director level. All readers are invited to send via ICONDESK (Suggestions) draft articles they wish to have published.