

On Cyber Patrol July 2007 Lost information – The Human Factor



If history has taught us anything, it is that as communication technologies become more sophisticated so do the methods of interception. The strategy is the same: intercept the message at its most vulnerable point. That point has evolved from a well-placed set of ears at a tavern to increasingly ingenious ways to intercept wire, radio and satellite transmissions.

Opposing forces throughout the ages of military conflict have tried every means possible to prevent compromised communications. Encryption, protected communication channels, and precise policies and procedures are just a few methods used to confound enemy snoopers. Even though advances in communication technology have given us increasingly intricate ways to protect information, in time, technology can be compromised. The trick is to always stay one step ahead of the enemy's interception capabilities.

Yet, no matter how effective the technology, there is one critical factor that can be the fatal flaw in any information assurance strategy: the human factor.

No method is foolproof for one simple reason. There's a human at both ends of the communications link. It is at those two critical points – sending and receiving – that the most common weakness is found: lack of common sense. Common sense tells you that if there are safeguards put in place to protect information, then those safeguards are only effective if used correctly. This means using only approved communication devices and methods. It means not finding ways around these protections for reasons of convenience or personal goals. Compromised communications equals lost lives. It's that simple. Always has been, always will be.

Intelligence gathering through history is based on the effective collection and analysis of many small bits of data. Much of this intel is gathered not from official military communications, but from the casual comment or the "I'm OK" message to family and loved ones that inadvertently includes operational information. It used to be that enemy agents recruited spys to gather information. Now they simply have to read blogs available to the entire Internet community looking for operational security violations.

While we Americans have been raised with the right and resources to enjoy the freedom of free speech, we need to remember this freedom comes with a responsibility. That responsibility is to be smart about what we say and how we say it. In times of conflict, this responsibility becomes even more important. We must all keep in mind that someone is always listening.

