

Making Information Assurance (IA) Routine Gives Soldiers the Edge

April 2006



For those that have played organized sports there is a good chance that at some point they have heard a coach say, "don't telegraph what you are going to do." Reading plays, stealing signs, and anticipating strategies all go towards gaining an advantage, an advantage that could significantly affect the outcome of the game. Lapsing in information security (IA) is the same as telegraphing a pass. But in the warfighter's game it won't cost you the state championship. It could cost you your life.

In all forms of completion from a friendly game of poker to the serious confrontation of armed combat each side or player is always looking for an insight into what the opponent is going to do. You watch for patterns in play, physical clues and moments of distraction when something slips that lets you know the other side's intentions. Adhering to information security regulations and protocols is the same as a pitcher and catcher holding their gloves over their mouths as they talk strategy on the mound.

If information is being transmitted in any electronic format there are opponents doing their best to listen in. Protecting information saves lives. For this reason alone all military personnel need to make information and cyber security part of the routine, not a special effort. It needs to be as automatic as cleaning your gear, setting a perimeter and keeping your head down.

But there are challenges to this that must be overcome. Warfighters in harm's way are on the watch for ambushes and IEDs. IA often comes as an afterthought when bullets and shrapnel are flying. Yet in the heat of battle training and discipline saves lives and accomplishes missions. That is why IA needs to be part of a soldier's gut instincts and trained reactions.

Back in garrison not dealing with the constant stress of war, the challenge is far different, but just as dangerous. Boredom and complacency can cause the IA guard to be let down. But stateside, and in secure facilities far from the war zone, information that could help the enemy is constantly flowing. Our opponents are listening to our routine conversations and communications, both official and personnel. We cannot be fooled. They are sophisticated, diligent and effective in their methods. That's why the attention paid to securing our cyber communications can never be too much. Even with all the other orders and regulation to follow, letting critical information out can easily make all our efforts in other areas useless.

The solution is surprisingly simple. All military personnel, their families and friends need to make IA part of their everyday life. Securing passwords must be as routine as brushing your teeth. Not engaging in risky computer activities must be the same as locking the house at night. Not revealing any usable information on blogs or in chat rooms is as critical as your kids not talking to strangers.

A soldier's personal life has many security behaviors that are done without a second thought. They have been ingrained into their daily routine. These activities keep families and loved ones safe. By adopting this same attitude in their professional military lives soldiers can keep fellow soldiers safe. We need to keep our opponents in cyber space constantly guessing. Don't let them in the huddle.