On Cyber Patrol September 2009 - The “I” in Information Assurance

There is no argument that teamwork is at the heart of success, especially in the military. But sometimes you can find yourself out there without backup. This lonely moment can take place sitting at a computer in a room filled with teammates. There may be no “I” in Team, but there is one in IA (information assurance). When protecting information, it’s the individual that needs to step up.

In any data security chain you will always find an individual making decisions and taking action. Whether it is using technology-based security tools or following best business practices and rules and regulations, an individual is making choices about what to do. Make the right choice, the mission is successful. Make the wrong choice and critical information and the mission can be at risk.

There are those that argue that technology can ensure data security, not the individual. However, technology-based cyber defense is not perfect. Hackers and other cyber criminals prove that on a daily basis. You can put all the digital locks and technical alarms you want on your data, but the individual is the critical decision point. The actions of one individual can strengthen or weaken the security of military and personally identifying information (PII). It still comes down to the old chestnut that IA stands for individual accountability. Every person within the military, including the civilian workforce and supporting contractors, holds individual keys to information. Locking the door to intruders is each person’s responsibility.

A common excuse is the lack of time we have to “do things right.” In reality, individual accountability in the area of information security comes down to only a few seconds. In those few seconds a person could remove their Common Access Card (CAC) from a card reader, turn on a firewall, not send a text or post something to a web page or blog that contains restricted or PII, recognize a phishing warning sign or not click on a dangerous link in an email. In those same few seconds, a person could also do just the opposite.

One of the most significant threats to data security is not deliberate actions but moments of inconsistency and inattention by an individual. Often these critical moments of lax security procedures and practices happen not in the workplace but at home. Some people are by-the-book strict with security policies and procedures when on duty, but don’t practice those very same security activities at home. That’s because at home people relax and let down their guard in a place of relative safety. But data, particularly PII, may be easily accessed from home in this era of mobile technology. An individual’s awareness of IA must be constant, even in a relaxed situation. The only person that can do what needs to be done, to protect information, which in turn protects lives, looks back at us from the mirror.