Redefining Information Assurance compliance

By LTC Christopher Quick

Global connectivity and the speed at which information is transmitted around the earth have fundamentally altered our world, and we cannot go back to how things were.

Cyberspace has and will continue changing the way we all conduct our Profession of Arms. This applies to everyone--the Infantryman, the Signaler, the intelligence analyst and the commander in the field.

Global connectivity and the speed at which information is transmitted around the earth have fundamentally altered our world, and we cannot go back to how things were.

Technology continues evolving to meet today's threats while simultaneously building toward the future. Our task is to understand the dynamics driving this rapid change and stay ahead of the malefactors loitering in the shadows and acting to impede our progress.

The keys to information assurance are understanding and mitigating risks.

We can accomplish this by implementing standards, correcting deficiencies, and enforcing modes of user behavior, currently known as compliance. The discipline and standards bedrock undergirding our Army must be carried forward into the cyberspace domain.

Compliance in Information Assurance is one of Army Cyber Command's most pressing and important mission imperatives. It is a multi-dimensional term subject to wide interpretation in its application.

Driving this vital imperative are cyberspace threats that are real, growing, sophisticated, and evolving. As we work to take full advantage of cyberspace's potential, we must recognize existing and future threats and appreciate their ability to prevent us from operating freely. Threats include a wide set of actors with digital devices or computers trying to improperly access our enterprise with nefarious intent.

Trend analysis indicates the number and sophistication of attempts to exploit our networks will continue to increase and mature. We must anticipate the evolution of these threats. Every time we enter the network, regardless of where we are, we are in a contested environment in which we must fight to maintain our freedom to operate.

Since its creation, Army Cyber Command has actively focused on operationalizing Computer Network Operations. IA compliance is a key part of this process.

However, there are unique challenges in doing so, including the volume of IA threats and vulnerabilities, the escalating pace and sophistication of emerging threats, the distributed and dispersed state of current Army networks, a general lack of security training and awareness, and a traditional lack of leadership understanding and involvement in actively implementing required IA implementations.

In addition, the command has worked to reduce the frequency and systemic causes of costly IA compliance failures, such as unauthorized disclosures of classified information (UDCI, formerly known as "spillage"). In all, operational emphasis on Information Assurance compliance has led to tangible improvements in security and user awareness. Much, however, is still required of Army Cyber Command, the cyberspace community of interest, and Army leadership to mitigate risk and deny adversaries access to the Army's sensitive information.

Why Information Assurance Compliance?

The better question to ask is why compliance with Army orders and directives? The primary reason for enforcing

(Continued on page 38)

(Continued from page 37)

Army-wide standards and user norms is the need for a strong defense. Protecting information and guaranteeing transportation through cyberspace is essential to how our Army fights.

The ability to operate when degraded or disrupted provides significant advantages to the side that can gain, protect, and exploit advantages in the contested cyberspace domain. The advantage will go to whoever best mitigates the loss of intellectual capital and reduces the number of vulnerabilities.

In some cases improved defense results directly from short term actions taken to diminish known threats, such as the application of a vendor patch. In other cases, improved defense results from the gradual implementation of enterprise-wide applications that move the LandWarNet (the Army's network) toward a more uniform and interoperable network.

For example, migrating to a common Windows platform or synchronizing the tuning of Host Based Security System may not give the immediate appearance of defense; but these important actions promote a more automated and thus more responsive network. Without these common configurations, the network cannot effectively feed the emerging common operational pictures, such as IT asset management or continuous monitoring.

We can neither afford the loss of critical information, nor afford the cost of remediation. A clear example of this is in the area of UDCI, where an entirely avoidable act can result in a sizeable remediation price tag for the unit involved. This year remediation costs exceeded $700,000. That is unacceptable.

Most important, however, is that complying with orders and directives is not voluntary. As with any Army operation or task, orders and directives must be followed. Just as with any mission or operation, failure to accomplish assigned tasks can jeopardize the overall mission. This is critically important in cyberspace operations because cyber enables mission command.

A new breed of order identifies the most widespread and potentially debilitating vulnerabilities in the Army and mandates they be addressed immediately.

What is Army Cyber Command doing?

Army Cyber Command is actively moving forward with operationalizing IA compliance by regimenting the orders process and helping commanders mitigate risk by prioritizing vulnerability remediation to address the most critical enterprise vulnerabilities first. This process allows field commanders to see risks in operational terms so they can understand impacts to their units and take action based on operational needs.

Consider the case of the UDCIs described above. Since reaching a monthly high in February 2011, poor user behavior has declined 50% to the end of October 2011. Command emphasis and outreach reduced the frequency and severity of these events; more work, however, is required. Commanders at all levels have come together with a common sense of urgency to correct the problem.

Where orders implementation is concerned, one process in particular is putting a fine point on compliance. Dubbed the "High Risk Vulnerability List," this new breed of order identifies the most widespread and potentially debilitating vulnerabilities in the Army and mandates they be addressed immediately. Their status is reviewed weekly, with focus on a manageable set of vulnerabilities versus the full continuum of active vendor patches. Anecdotal responses from the field have been positive, as this "High Risk" order estab-

lishes a common priority of effort based on command direction.

Cyberspace operations orders also work well in high profile cases where the Army must act immediately and decisively in the face of emerging threats. On the heels of the Wikileaks incident in late 2010, for example, Army Cyber Command issued the single codifying order that aligned all mitigation actions; units subsequently reported full compliance within weeks of the release of the order. This single recognized orders process continues to pay dividends across a broad range of deliberate actions, from Enterprise E-mail to the patching and scanning of Army systems.

Army Cyber Command has also established a recurring command forum for the assessment of other compliance indicators. The monthly Cyberspace Operations Readiness Report brings all components together to discuss the status of orders implementation, cyber security training, "High Risk" vulnerability implementation, and the results of external inspection.

It is this last compliance element where Army Cyber Command stands poised to make a fundamental difference. For too long the Army's information security inspections have been "fire and forget" events that might have received attention early on, but then faded into obscurity soon afterward. Army Cyber Command has taken the lead role in de-conflicting the numerous IA inspections pending at any given time by various organizations (e.g., Defense Information Systems Agency, Command Cyber Readiness Inspections, Inspector General, and Army G3), and is aligning the full Army audience to a concise list of candidate sites. Army Cyber Command will also ensure the thorough follow up of any significant findings through sustained contact with the affected organizations.

In addition to influencing assessments and their results, Army Cyber Command wants to improve the integrity of its IA compliance reports and statistics, both through manual and automated means. Today, compliance reporting is largely done through semi-automated methods (e.g., machine scanning with "stubby pencil" analysis), but command emphasis is now on a fully automated reporting structure. With the enterprise tools now available to perform these scanning and reporting functions, it makes little sense to wait for the "ultimate" reporting structure. Rather, Army Cyber Command is reaching aggressively for the "low hanging fruit," things that can be leveraged today.

The Way Ahead

Standards must be clear and enforced. Discipline is a military hallmark and we must be as disciplined on our network as we are with our weapon systems. By making IA compliance a commander's priority exercised through educated users who understand their role in the defense of the network, we will better promote a strong defense of our networks.

The continued cultivation of an environment where the standard is strong compliance, the protection of information, and the guaranteed transport of information through cyberspace will make serious and lasting improvements for the security and efficiency of Army networks.

While resourcing and technical constraints deter rapid, uniform compliance, Army Cyber Command will continue to push to change the conditions and the mindset within the Army so compliance becomes second nature.

As in any defense, adversaries will find and exploit our weakness. To counter this we must treat compliance like a weapon system and be ready to defend and protect against a threat that is real, growing and evolving. In the end, compliance with orders and directives in IA is no different than with any Army operation, task, or directive. Leaders actively engage to ensure mission accomplishment, no matter the operational domain. Maintaining the freedom to operate in cyberspace is everyone's business. Army Cyber Command is committed to supporting commands and enabling mission command.

LTC Christopher R. Quick *is currently the Director of Strategic Communications for the U.S. Army Cyber Command / Second Army at Fort Belvoir, Va. His assignments include Fire Support Officer, Battery Executive Officer, Brigade Assistant Operations Officer, and Brigade Fire Direction Officer. He commanded a Battery with 1st Battalion, 17th Field Artillery. He served in the 41st Signal Battalion, 1st Signal Brigade as a Battalion Automations Officer. LTC Quick served as Brigade Information Operations Officer with the 2nd Brigade, 101st Airborne, where he served a tour in Iraq. He has served on the Army Staff within the Army G3/5/7 in DAMO-ODI and served on the Army Cyber Task Forces as the lead action officer for the development of Army Cyber Command. LTC Quick holds a B.S. degree from Park University in Kansas City, Mo. and an M.S in Computer Science and another in Information Operations from the Naval Post Graduate School in Monterey, Calif.*