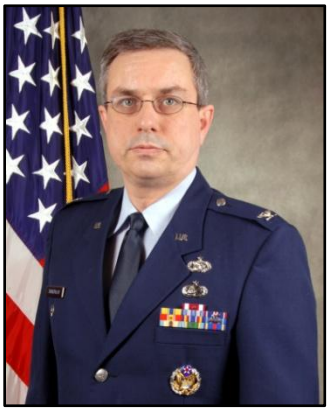
CyberPro

May 2009

Keeping Cyberspace Professionals Informed

CYBER DEFENSE – WHERE DO WE GO FROM HERE?

BY COLONEL GLENN ZIMMERMAN, CISSP



The views expressed in this article are those of the author and do not reflect the official policy or position of the U.S. government, Department of Defense or the United States Air Force. Colonel Glenn Zimmerman is an Air National Guard Officer on active duty with the U.S. Air Force. He is a recognized subject matter expert regarding cyber and a featured presenter at venues around the globe. He has held a variety of positions in Network Operations and Security both in and outside of the military including: director of the Air National Guard (ANG) Network Operations and Security Center (NOSC), Systems Manager in the U.S. District Court, and Senior Infrastructure and Security Consultant with Siemens Business Services. While Director of the ANG NOSC, he was handpicked to be part of the USAF Cyberspace Task Force where he worked to establish the foundation for the Air Force way ahead in cyberspace operations, doctrine and policy. He holds 14 current Information Technology certifications in specializations ranging from operating system and network design to security analysis.

Over the past 15 years, we have witnessed an ever-increasing upward trend in both the variety and quantity of network attacks, intrusions and attempts to damage, degrade or otherwise adversely impact the legitimate use and operation of private, public, commercial and government systems. While the nature of the offensive actions has evolved and adapted to greater levels of flexibility and sophistication, the majority of defensive responses have languished with only incremental and reactive development.

It has been said in various forms "…insanity is the act of doing the same thing over and over again while expecting a different result each time." Unfortunately, much of current cyber defense has fallen into this trap. For purposes of this discussion, I will focus only on the computer network defense aspect of cyber and not assaults or disruptions to other portions of the electromagnetic spectrum.

While malicious actors avail themselves of the latest weaponized tools to employ against our systems, we seem to be mired in a signature-based, whitelist/blacklist, compliance-heavy, regulatory-driven, defensive model which consistently demonstrates its ineffectiveness in combating these threats.

After all this time, why haven't the countless millions of dollars in software solutions and man-hours made our systems significantly safer? Why are our presumably state-of-the-art systems so vulnerable to penetration and degradation? While the tactical level specifics vary across a broad spectrum based on operating systems, applications, hardware platforms, etc., there are some

fundamental underpinnings which drive much of the futility we see on a regular basis in the operational defense of our networks and critical data.

First among these is an overreliance and misplaced faith in an administratively burdensome compliance-based security model. The overarching emphasis of "frameworks" such as DIACAP (DoD Information Assurance Certification and Accreditation Process) drive organizations to a regulatory approach to security – if one can show every process and checklist item is accounted for, by association, the system and applications are secure. Unfortunately, this approach is more prone to ensuring the paperwork is in order rather than securing the systems at risk. Checklists and processes have a place in network defense and information security, but they are only two of several tools which must be employed to be effective. Likewise, the dependence on such a compliance model drives the "patch" mentality as being the panacea for all system vulnerabilities. Nothing could be further from the truth. How does someone "patch" for an unknown vulnerability until it is exploited? How much latency can one safely deal with until the patch is released? These windows of opportunity work strictly on behalf of the intruder or attacker. No number of regulations or after-the-fact patching is going to dissuade or deter those determined to compromise our systems.

Second is the insidious and counterproductive trend toward locking down our systems more tightly to prevent incursions or exfiltrations. As additional onerous restrictions are introduced, we create more holes in our "official" security posture through the "unofficial" creation of workarounds so employees can actually get their work accomplished. The philosophy of "less is more" when applied to system access often carries with it the unintended consequence of less productivity at the same or higher cost. If this approach is completely successful, we will eventually create completely secure networks and systems which no one uses because they are so restrictive and have no productive value. One can liken this approach to holding a palmful of sand and slowly closing the hand to secure the sand. At a crucial point, the pressure on the sand retains it completely in the palm of the hand; add more pressure and it begins to squeeze out between the fingers. Squeeze even harder and more is lost. Similarly, excessively restrictive security policies can become self-defeating as motivated and creative employees develop workarounds to circumvent excessive control.

So, the question becomes "what can we do that is different from what we've done before to make our systems more secure and yet enable them to retain the value which drove their creation in the first place?"

We need to truly understand what happens on and within our systems. Situational awareness or visibility into network functions and traffic is always championed as critical to security. But how many organizations have performed a complete baseline monitoring profile for all their networks, systems and applications for normal, holiday and surge periods such as end-of-year financial closeouts? Very few, if any, have invested the time and resources to do so and yet this level of understanding would permit early detection of anomalous behaviors throughout the system. It would also reveal other potential issues while establishing a vector to attribution and necessary corrective actions. In other words, it would permit proactive rather than reactive mitigation of many threats and reduce reliance on after-the-fact patching as a first line of defense

We also need to leverage the intellectual capital within each organization. Simply put, the IT or IA department does not possess a monopoly on good ideas to protect and secure the enterprise. We must include the "power users" among the respective agencies and business units and collaboratively develop solutions which meet the needs of the users as well as improve security. Worked correctly, the two concepts need not become mutually exclusive, but rather can serve as a foundation for improving user education and transforming them from the role of bystander to stakeholder. This transition to an active participant has the potential to change cyber defense from an IT issue to a personal one as the impacts (both positive and negative) resolve to the individual rather than the organization.

Finally, we must establish and maintain transparency of communication between our peers – both internal and external to our particular system(s). With the high degree of interconnectivity necessary to conduct operations at all levels, it is imperative we not continue to operate as "cylinders of excellence," but rather as collaborative partners who, working together, can improve the functionality and security of our portion of the grid and our partners' as well.

There are those who will decry and rail against the de-emphasis of the compliance model, but practical experience has indicated it demonstrates marginal, if any, effectiveness in its role of establishing secure and usable networks and network systems. Regulations, standard processes and checklists will still be necessary and are even encouraged, but they are not the end solution. Instead, they are fundamental components of a larger and more inclusive approach to cyber defense. We can continue to do what has been done before and see it fail again, or we can acknowledge it is time to move forward and embrace a more realistic and pragmatic approach to securing our respective corners of cyberspace.