CyberPro

Volume 7, Edition 7
April 3, 2014

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Mark Nehmer, Defense Security Service

NSCI recently had the opportunity to interview Mark Nehmer, Associate Deputy Director, Cybersecurity, Counterintelligence, at Defense Security Service (DSS). The DSS mission is to support national security and the warfighter by securing the nation's technological base, and overseeing the protection of U.S. and foreign classified information in the hands of industry. Mr. Nehmer is the Project Manager for the DSS Cybersecurity, Counterintelligence initiative. Prior to joining DSS, Mr. Nehmer was the J65 Division Chief, Risk Management/C4 Analysis and Strategy, United States Cyber Command (USCYBERCOM), responsible for analysis of current and future DoD and Federal risk management and C4 instructions, directives and implementations, and development of strategies for and on behalf of the USCYBERCOM J6, Command and DoD leadership teams. Previously, he worked as a contractor, performing as the Senior IT Analyst for the stand-up for USCYBERCOM on behalf of Joint Task Force – Global Network Operations (JTF-GNO). He accepted an executive-level Government Service appointment as the Senior Advisor for Command, Control, Communications and Computer Systems in December 2009. Mark holds Bachelor degrees in History and Economics from the University of Michigan and Master of Business Administration with a dual concentration in Finance and Information Systems from Fontbonne University where he graduated Magna Cum Laude.

NSCI: From your experience developing and implementing information security policy and guidance at U.S. Cyber Command, what are some of the key opportunities and challenges you see?

Nehmer: *(BACKGROUND)* This is something that has been front and center on my mind for a number of years, so this first answer will be expansive: There are a number of very good on-going efforts across government and private sector with the goal of minimizing the impact of malicious cyber activities from various sources, including insider threats. While the DoD and Intelligence Community (IC) do a relatively good job of anticipating, repelling and ejecting malicious activities, while minimizing any impact, the remainder of the Federal Government is not quite as good and the rest of the collective "We The People" (with a few exceptions), less so. I describe what the DoD and IC are able to accomplish in this area as "Getting to the Left of Boom".

We spend a lot of time, money and brain-power trying to fix our own houses, neglecting the fundamental truth that collectively, We are much stronger than any of us are individually. The information we all need to understand and thwart the threats is segregated by design and shared very painfully among a limited set of partners. The challenge I see is a lack of ubiquitous voluntary and directed connectivity…sharing of actionable information. This sharing gap is having an unnecessary effect on the entire fabric. I envision a nation-wide public/private sharing framework that could help the collective We begin doing a better job of mutually supporting each other's cybersecurity objectives.

We are all over the map when it comes to the mix of tools and talent at our disposal. The result is a very wide range of effectiveness against advanced and persistent threats posed by malicious activities from hackers, criminals, terrorists and nation-states. A small subset of We that has the best tools and talent is currently able to proclaim that they are typically at the "Left of Boom", when it comes to early discovery of malicious activities from known advanced actors. Unfortunately, too many of We are at the other end of the scale, lacking the expertise even if they had access tools (technical and intelligence), leaving them in a position of being exploited/attacked/hacked (pick your term) without knowing it until the damage has been done. Some of We never know that they have been had until some of the other We come and tell them.

The majority of We discover a problem far to the right of the boom and spend tremendous time, effort and money trying to stop the "bleeding", figure out what happened and how to prevent it from happening again in the future. In IT terms, this is often referred to as an Information Assurance (IA) or defense only approach. Experts at the "left end" of the skills/tools continuum will tell you that an IA only approach is a losing strategy and will only prevent the exact same thing from happening the exact same way, and nothing else. We need to do better. We need to act collectively to get more of us to the Left of Boom.

(CHALLENGE) Anyone who has worked in government or large business for a long time will tell you that there is a strong preference for the status quo. Any attempt to perturb the current rhythm is typically met with skepticism and often with outright hostility. The term that comes to mind is "rice bowls" and the momentum seems to favor protecting them vice taking a risk on making a significant change and potentially improving the outcomes. "Getting to the Left of Boom" is a VERY big idea with a far-reaching scope, requiring the cooperation of a broad mix of government and private sector entities. The last time the Federal Government was mostly successful trying to do something like this was the Federal Highway Act of 1956.That took the collective will of the general population who could see a day when they could travel the country to visit family, for vacation and/or for business. They demanded their representatives at all levels of government work together to make that vision a reality. This cooperative and directive information sharing and training idea is no less of an undertaking.

(OPPORTUNITIES) There are a number of opportunities to leverage the existing authorities and capabilities both across the federal government and more importantly in partnership with State, Local, Territorial and Tribal governments and with industry. No individual part of the government or industry has the existing authorities, expertise and/or capacity to get us to the left of boom. It will have to take a whole of nation approach to stand a chance. For this to happen on a voluntary basis, there has to be a business imperative to act.

Following the recently publicized events at Target and Neiman-Marcus, I believe now is the time to ask for and expect to get support from both the public and private sectors…a whole of nation approach. We should look for and encourage those opportunities.

NSCI: How is the DSS addressing cybersecurity training and awareness for its employees and the Department of Defense industry?

Nehmer: Training is a tricky thing. In a tight budget climate, training used to be the first thing to go. Not any more, as leaders understand the importance of keeping technical skills sharp. Most entities in and out of the government still find it difficult to put travel dollars on top of tuition, books and time away from an important job. Fortunately, DSS provides security education and training for the DoD and industry under the National Industrial Security Program (NISP) through a variety of formats, including resident, on-site and virtual courses. DSS sees the traditional and cyber disciplines as intrinsically linked, when it comes to a comprehensive security program so the agency offers a wide variety, including: Industrial, Information, Personnel, and Physical security disciplines, as well as other security related areas such as Special Access Programs.

NSCI: What challenges does the DSS face in recruiting and retaining highly skilled cyber talent given the limited availability and current fiscal environment?

Nehmer: And I thought training was tricky! Like the rest of the government, we can't compete with the private sector for top cyber talent when it comes to money, so we have to rely on something else. Most of us come to work for the government and stay for the mission. We believe that what we are doing makes our nation a safer and more prosperous place to live. DSS is the entity that helps other entities, both in and out of the government, protect the technological advantage of the United States. When we are recruiting people, we look for the ones that "see" the mission and embrace the possibility of serving the nation with little or no public recognition (we are a predominantly civilian force). The ones with vision, in addition to technical skills, are the best, most enduring candidates.

NSCI: What do you see as the most important step(s) the DSS could take towards better protecting government and military information systems?

Nehmer: DSS has a variety of missions, most of which involve the timely analysis and exchange of information. We perform security assessments and help our industrial partners discover areas where they may be vulnerable to internal and external threats. We keep our government partners informed of the indications and warnings of adversarial activities in the field that may impact their missions, so they are enabled to make more informed risk decisions.

NSCI: What are some of the differences in cyber policy and language between the DSS and defense industry? How are these being addressed?

Nehmer: The defense industry is interested in delivering uncompromised quality products for a fair price at a profit. The government is interested in purchasing uncompromised quality products for the best price possible. This price friction causes competition and, unfortunately in the past, cybersecurity was often an afterthought. The market place would prefer policy language that relies on the free market to deliver what is demanded. The government believes that language needs to specify the security measures (controls) that are required for each type of purchase. Personally, I think there is a balance to be found. I believe it starts with incentivizing "good behavior". I think the contract award process should consider each company's history of or, if no history with government contracts exists, evaluate the characteristics of their ability to; deliver uncompromised quality products. We are all used to our personal credit score, maybe there is a set of criteria that could be developed, reported and evaluated based on a company's risk posture (including cyber and physical). Maybe that could help level the playing field by rewarding those companies that put into practice extraordinary measures to secure their products and information before and after selling it to the government.

There are efforts across the government to look at ways to increase the security posture of our industrial partners without over-burdensome regulations. I think the things that the government can give business they will value the most are clarity, consistency and stability. A number of us are working on that.

NSCI: What are the most common cyber-related vulnerabilities you have seen during its work with the defense industry?

Nehmer: From my personal experience: People. We can work very hard to put in the best firewalls and intrusion detection systems, but people making mistakes in spite of their mandatory training are still the biggest vulnerability to our defense industry and government partners.

NSCI: Is there anything else you'd like to add?

Nehmer: I will leave you with a final thought. This is not a static threat. There are a great number of very talented people in the world that will always want what we have spent our blood, sweat and tears to create and protect. None of us have a chance of thwarting them as individual entities. It is only the collective We that stand a chance of moving our great nation a little to the left of boom.

NSCI: Thank you very much for taking the time to visit with us.

[Author's Note: The opinions expressed herein are those of the author's, and are not necessarily the official views of, or endorsed by, the U.S. Government or the Department of Defense.]