CyberPro

Volume 7, Edition 13
June 26, 2014

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Lance Dubsky, CISO, National Geospatial-Intelligence Agency

NSCI recently had the opportunity to interview Lance Dubsky, Chief Information Security Officer for the National Geospatial-Intelligence Agency (NGA). Lance leads the agency's information security program and is responsible for IT Security of the global enterprise. As the senior risk executive, he continuously monitors and manages the risk posture of the agency through performance, measures, metrics and enterprise risk processes for mission, infrastructure, business and financial systems.

NSCI: What are NGA's cyber-related priorities for 2014?

Dubsky: My top priorities are IT, IT, and IT! …and being realistic. The best way to address cyber-related challenges is to first address the root cause of the problem. Ineffective management of IT creates vulnerabilities. My perspective is that when you manage IT effectively, you reduce your cyber-related challenges and you reduce your risk posture. My priorities this year include:

- Creating one IT acquisition process that is transparent and adjudicates every new requirement with the organizational vision and future IT architecture.
- Integrating the organization's risk management process into the acquisition process by defining entry and exit criteria to include required risk management artifacts for each acquisition milestone.
- Adopting the NIST Risk Management Framework and transform our risk management processes to be focused on all aspects of testing and verifying compliance with security controls.
- Increasing our ability to manage change on key interfaces within the IT infrastructure
- Evolving our Cyber Security Operations Cell (CSOC)
- Moving to a "enterprise security as a service" model based on delivering the NIST Special Publication (NIST SP) 800-53 technical controls as an enterprise service
- Creating the IT Security Career Service based on the National Initiative for Cyber Security Education (NICE)

Developing the CSOC was one of the agency's key initiatives in 2013, and we are advancing those efforts in 2014. Our goal is to unite all cyber functions into one integrated organization, the CSOC, that operates as a corporate entity. We will continue to evolve the CSOC by addressing initiatives focused on people, process and technology.

- People. We will work to develop training standards for each of the cyber analyst position to ensure staff and contractors are trained and qualified.
- Process. We will develop repeatable methodologies for how we address cyber events, manage incidents and perform each aspect of the cyber defense mission.

- Technology. In FY2013, a number of cyber defense investments were defined and approved. The implementation of these investments will begin in late FY14, early FY15. Developing the "To Be CND Architecture" will guide future investments.

NSCI: How is NGA doing at implementing continuous monitoring and achieving its objectives? Any lessons learned for others?

Dubsky: Continuous monitoring is not new; in fact, continuous monitoring has been a key part of certifying and accrediting systems since the Orange Book era. For the past 20 years, as systems have been certified and accredited, organizations were responsible for periodically testing and performing independent verification and validation activities to ensure the systems maintain compliance.

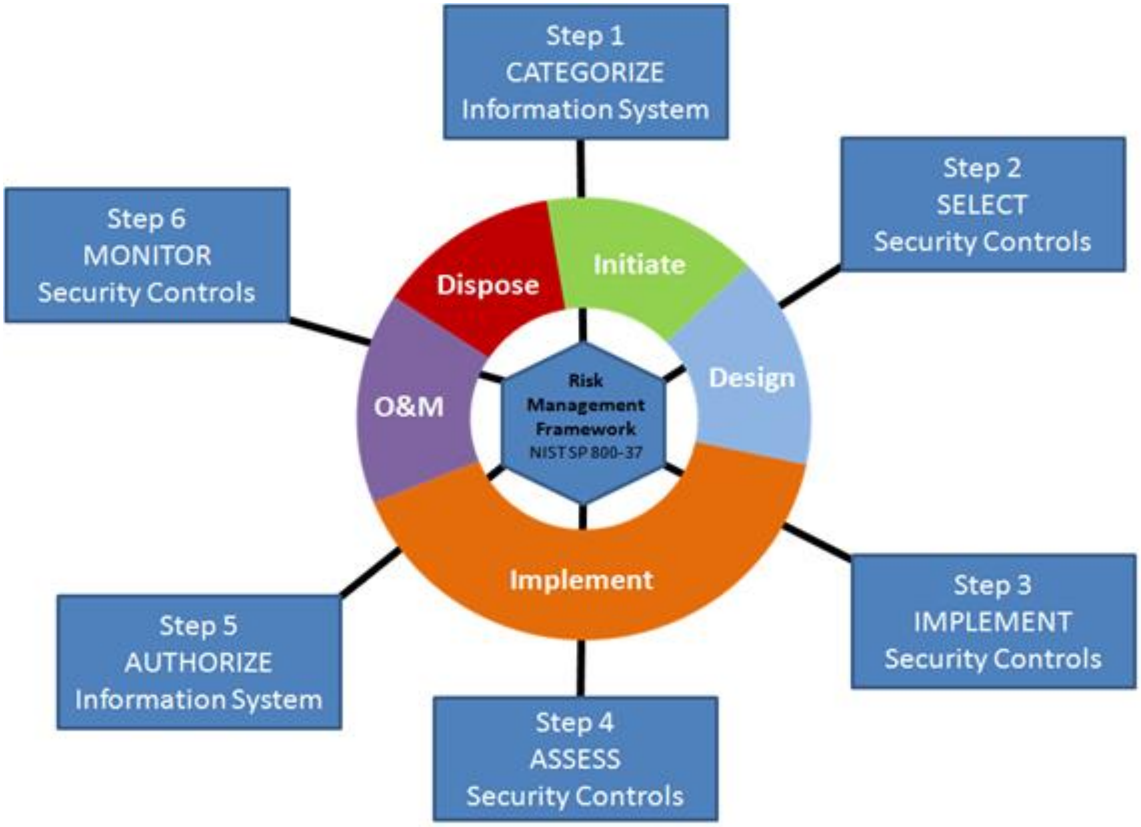

Table: NIST SP 800-37, Risk Management Framework

The increased focus on continuous monitoring, step 6 of the risk management framework, is imperative to how a system maintains its authorization and continues to operate within the original risk acceptance.

Today, our implementation of continuous monitoring exists in two major phases: legacy (existing) systems and future systems. NGA is in the process now of evaluating every authorized system against 85 critical controls and will define during this phase whether the control is met by an enterprise service, the system owner, or the CIO, the frequency of the controls, any associated acceptance of risk, and how reporting will be accomplished. This is a long process and is dependent on how well your existing body of evidence has been maintained. For future systems, the continuous monitoring model will be focused on enterprise security as a service. NGA is currently evaluating the services that provide for the NIST SP 800-53 technical controls and key operational controls, their effectiveness and highlighting gaps which I term as unfulfilled requirements.

Lessons learned for continuous monitoring:

- Be realistic with your strategy. If you are an agency with 1,000 systems and you try to continuously monitor every control, the total number of controls is between 400,000 and 600,000. It's not realistic to monitor that many controls.
- Be realistic with defining critical controls. If you cannot monitor all security controls, then monitor the ones that provide an indication of whether your risk posture has changed or not.
- Be realistic with the risk you have already accepted. Trying to force legacy systems that have been accredited for several years into a new model when the only funding available for the system is operations and maintenance is not feasible.
- Focus on the future: Enterprise Security as a Service. In this way, you can ensure all future acquisitions use enterprise services (identity and access management, audit, intrusion detection, etc.) which will enable you to automate continuous monitoring to a significant degree.

NSCI: What would you like to see in the area of continuous monitoring that's not currently available?

Dubsky: One of my key focus areas is enterprise security as a service. In my CISO role I have risk management responsibilities and since we are using NIST SP 800-53 as the control catalogue it would be advantageous to have tools that depict the health of these control families at the Enterprise. Of course, meeting all of the technical controls does not compensate for good security hygiene such as timely patching, hardening systems, and proper configurations.

What I would like to see is a series of dashboards that presents analytics from the collected input from our tools. In addition, while many products today are very good, some do not work well in virtual infrastructures or handle large volumes of data. Evolving current capabilities to handle Cloud, Virtual Infrastructures is essential.

NSCI: How does NGA ensure its employees remain aware / ahead of the cybersecurity threat?

Dubsky: The Intelligence Community is a partnership, so sharing cybersecurity threat information between agencies has become the norm. The U.S. Cyber Command and the successor to the IC's Incident Response Center, the IC ITE Security Coordination Center (SCC), also provides threat information. Our CSOC participates in NSA Threat Operation Center (NTOC) daily threat briefing. I believe a key to our staying in front of the threat, is our partnership with industry. Our industrial partners perform a lot of research on the advanced persistent threat, mitigations, and how to develop tools focused on driving down the time to detect threats. All of these together help keep cybersecurity professionals aware, and our security training helps keep NGA employees informed on the typical attack vectors that they are most exposed to.

NSCI: What kinds of benefits have accompanied standing up the NGA Cyber Security Operations Cell?

Dubsky: The goal of standing up the CSOC this past August (2013) was to increase cyber situational awareness across each functional area (incident response, cyber analysis, focused operations, and counterintelligence), to gain synergy from working more closely together, to speed up the escalation of cyber incident reporting, to de-conflict investments, and to gain efficiency. As we are only nine months into this transition, the current benefits include faster responses to cyber events, escalation of event reporting, and process improvement in the CND Service Provider construct. I'm looking forward to seeing how our capabilities evolve as we introduce new technology and our training program matures.

NSCI: How would you describe the maturity of current cybersecurity measures and metrics?

Dubsky: Our CSOC produces the standard cybersecurity measures and metrics for reporting to Cyber Command and to the newly created Intelligence Community Information Technology Environment (IC ITE) SCC. As we implement new capabilities and expand our analytics we expect to gain a better understanding of our cyber posture. Capturing the right metrics will certainly help us in our decision making.

NSCI: Given cyber professionals are "high demand, low density", how does NGA recruit and retain top cyber talent?

Dubsky: NGA is a great organization with an important mission, and great leadership. This alone is a big attraction for many job seekers. We are focused on obtaining the top talent. This occasionally is a struggle due to competition around the beltway and dwindling budgets. High quality, "high demand" cyber talent requires a salary commensurate with their qualification. Basically, you have to pay to get the right talent. Another option we use is to look internally and create a path for junior personnel to receive training on the job and through internal training programs. Finally, when we have open government positions we seek to recruit talented personnel that are trained in computer science or related fields, and have the interest and enthusiasm for cyber security. As you know, Cyber Security is a growth area and we expect a steady stream of new talent to flow into NGA.

NSCI: What technology(s) would you most like to see that would significantly improve cybersecurity?

Dubsky: With the increased use of virtual technologies, traditional security technologies such as intrusion detection and prevention are less effective, so we would like to see more emerging technologies addressing security for virtual systems. Today, many cyber attacks are exploiting vulnerabilities in applications, and we have challenges with dynamic data that is manipulated and changed on the fly. To address this, we would like to see more technologies that provide security solutions that address the need for dynamically changing security control at an attribute and otherwise granular level.

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