Northrop Grumman's Art Lofton :

Teaming and Collaboration Result in Actionable Solutions

Art Lofton is sector vice president, Information Technology Solutions, and chief information officer for Northrop Grumman Aerospace Systems, a premier provider of manned and unmanned aircraft, space systems and advanced technologies critical to our nation's security.

Lofton is responsible for establishing the strategic direction and leadership of all information system and information technology activities for the Aerospace Systems sector. Previously, he had the role of sector vice president, Information Technology, and chief information officer for the former Integrated Systems sector.

Prior to assuming the assignment of chief information officer, Lofton served as deputy program manager for the Long Range Strike program at Integrated Systems. He was responsible for the successful integration of projects, programs, integrated product teams (IPT), and infrastructure responsibilities across the IPT in support of the customer for execution of LRS upgrades, support and depot activities.

Lofton also served as director of Operations Rapid Development and Production Processes. His areas of responsibility included the rapid development elements of Quality, Manufacturing, Materiel, Lean and Six Sigma, Facilities, Planning and Control, and Information Technology and production processes.

Previous assignments include director, Operations Strategic Planning and Integration, responsible for long-range and annual operating strategic planning, advanced manufacturing technology development and process integration across Operations; and manager of Strategic Planning and Integration for Advanced Systems Development.

Lofton joined Northrop Grumman as a flight test engineer on the B-2 program in 1990 and held management positions of increasing responsibility. This includes his role as the site manager for Integrated Systems at Hill Air Force Base, Utah, in a partnering venture with the Air Force while executing the B-2 composites statement of work. In addition, he served in several positions on the B-2 program, including manager of Production Support; B-2 Block 30 IPT leader; manager of the air vehicle managers, foreign object elimination, and IMPCA; and manager of Production Flight Operations.

Lofton has a Bachelor of Science in mechanical engineering from Carnegie Mellon University. He completed several advanced management programs, including the Program Management Seminar and Advanced Program Management Course.

Trust Points recently spoke with Art Lofton, Northrop Grumman VP, and heard his thoughts on the Cloud, mobility, and how these and other newer technologies may affect the crafting and delivery of solutions for Defense IT.

TP: What key initiatives and services do you envision will be critical over the next five years? In what areas is Northrop Grumman placing its IT investments, particularly related to security?

There will continue to be pressures on the defense budget. And there will continue to be increasing need to protect data - intellectual property - and to protect the systems we produce for our customers. By collaborating on solutions, teaming with our government, industry and international partners, using the right architecture to achieve those goals as opposed to each trying to figure it out on our own in isolation, we can achieve the economies of scale and synergies needed.

TSCP members compete against each other in some cases and partner with each other when we can achieve synergies and pass on cost savings; we are also subcontracted to each other in a third continuum, and we have to also consider our associates in our respective supply chains, the secondary and tertiary suppliers who should be involved. It's essential to get to a standard approach, to leverage the collaboration that results to drive the cost of business down while the pressure continues to rise as hackers and similar entities get smarter and more creative.

TP: Technology solutions are driven by business drivers that tie to a corporate strategic plan. How is Northrop Grumman managing its strategic plan to align solutions with the constant change in business requirements, given the increased speed of technical change and the introduction of new innovative solutions? What goals and objectives in the corporate strategic plan are directly related to your IT strategic plan?

Northrop Grumman has four primary business sectors: Aerospace Systems, Electronic Systems, Information Systems and Technical Services. In addition an internal organization, Enterprise Shared Services, essentially serves as a fifth sector providing a suite of internal services that includes IT, HR, and business management, among others. IT is an embedded thread throughout the enterprise ecosystem that supports those operating sectors across the enterprise with a common and cohesive approach that enables them to conduct business efficiently. We look into the future needs of the business in our long range strategic planning process to try to anticipate the needs of the organization.

TP: Are there additional collaborative capabilities that are common across the industry that would benefit from a standardized approach that TSCP should address?

TSCP has done an excellent job of developing demonstrations that reflect real world objectives and real world capabilities. For example, TSCP members worked with NASA to demonstrate the common credentialing that enables their collaboration; they showed how to connect the dots from the trust perspective, which is invaluable. The demonstrations actively show rather than passively describe solutions in slideshow presentations. With so much time spent going through the steps as the demos are constructed, figuring out the unexpected or the unintended consequences and the nuances of the unknown are invaluable. The teams work through the issues and get beyond them, resulting in achievable, actionable solutions. Demos allow people to see a solution; touch it, feel it, and then embrace it while also reducing risks and costs during implementation.

TP: What security challenges are unique to Northrop Grumman that keep you up at night?

I don't think that it's anything unique to Northrop Grumman; we all face the same challenges. We know that past strategies of just keeping people out by putting up barriers, fences, are going by the wayside. What keeps me up at night are the same issues that other CIOs have, which is why seeking solutions together rather than in isolation really is critically important.

TP: What areas or programs do you envision going to the cloud?

There are different definitions, different views of the cloud. Strategically, cloud-based services, for example, software as a service, makes sense. It's an efficient model - being able to provide people with what they need when they need it instead of standalone resources that have low utilization. The cloud also has some inherent security benefits where data is protected in a more centralized rather than distributed manner.

Cloud security is a major investment area at Northrop Grumman. Our Trusted Cloud approach takes defense-in-depth one step further. Since the challenge with cloud security is that the "perimeter" is blurred, classic defense-in-depth will not be sufficient. Cloud requires a new approach to security including protecting the data rather than the perimeter (Information Cloaking) and building "trust relationships" between entities. "Identity is the new Perimeter," and for cloud, Identity needs to be interoperable and portable between clouds.

TP: Having said that, do you see any impediments to adoption of cloud computing within the defense industry?

Securing risk in cloud computing is generally a factor of the type of cloud that meets the mission's needs. For instance, a private cloud, which is seen as more secure but also more costly than the public cloud, may be right. Vulnerabilities do exist but they are addressable. It's imperative that both private and public cloud systems be designed with security upfront so customers are comfortable with using it to store their sensitive data and important analytics.

The Defense industry has a set of requirements for security and IT protection that are unique and sets it apart from some other industries. There is a natural concern and conservatism. The public cloud can really benefit from leveraging the low cost of ownership. I see a larger use for the Private Cloud. But down the road, strategies and methodologies for protecting the data itself, whether data at rest or data in motion, will need to be addressed.

TP: What impact do you see mobile devices having on secure collaboration in your organization?

Many of the obstacles to using mobile devices are coming down, expanding their value to our work environments. The use of messaging tools, including social media, has changed our culture. A good example is the increase in the use of instant messaging on our enterprise computer systems. Mobile devices have enabled the convergence of information and affected how we operate: we are able to work from home; we have on-demand data: information, content, everywhere, anywhere across device-agnostic platforms. Across industries, you can see huge benefits and advantages to mobility. Not that long ago, we traveled from one place to another to sit down and meet face-to-face to share and to collaborate. Now, our phones are mobile computing devices that, along with our laptop computers, provide significant opportunity for seamless collaboration across the board, leveraging best practices so that people with like interests can communicate from wherever they are. People are able to share content of all types, in all forms, including videos. That cooperation and collaboration, while leveraging best practices, continues to evolve.

TP: How is Northrop Grumman using social media?

We are on Facebook, YouTube and Twitter. We also have an internal social media capability, MySite, we introduced a little over a year ago. Northrop Grumman also has an internal wiki and I have personally hosted blogs and live webchats with employees across the company.

TP: What are you hearing from your customers about their goals and concerns?

The customer environment today is "technically acceptable – lowest cost." No extra frills. If you have the base requirements, then there will be a situation where some of those things are not going to be encouraged or incentivized then you won't see them come to fruition. If the customer says, "I don't need power windows, I just want manual roll-up windows as the base requirements," some of those features aren't encouraged or incentivized.

TP: What government compliance areas and/or specific areas of challenge should TSCP address in the next two years?

I've been a vocal proponent of developing relationships for a long time to address compliance issues. I believe that the next step is to get key people who are responsible and accountable for procurement and acquisition of the systems involved; where people are asking, "How can I meet my mission objectives for data protection and identity management?"

TP: Are any of those kinds of things happening right now?

If you asked some of the key program stakeholders if they know TSCP, and if so, are they or would they consider an affiliation with TSCP, we might not get the report card that we want. I believe that TSCP has made some significant accomplishments over the last couple years, especially with the focus on value producing demos. That being said, I think there is still an overall lack of awareness across the areas of the "customer" responsible for program acquisition and execution. The opportunity for TSCP is to provide a common framework that can be utilized as a requirement in the program RFPs. I believe that will drive the broader adoption and recognition of the contributions that TSCP has made in the Trusted Identity space.

Executive Summary:

In 2009, TSCP published its Transglobal Security Collaboration Program Strategy: 2009-2011. TSCP is in the process of reviewing and validating the strategy as well as updating its priorities and deliverables for 2013-2015. As part of this process, the Leadership Advisory Group consulted with member executives to ascertain their positions and opinions on key developments and challenges facing the security environment in the Defense IT industry. Member executives also were asked what role TSCP should play going forward in supporting a common approach to resolving these challenges. In addition to the interviews, executives and the Leadership Advisory Group participated in a facilitated session to discuss the results and provide additional input. The results and recommendations will be used as the starting point for updating goals and objectives for the revised TSCP strategy. This white paper presents the results of the interviews and facilitated session.

TSCP would like to thank Iana Bohmer and Deloitte & Touche, LLP, a TSCP Member, for the dedicated work in conducting the executive interviews, facilitating the executive session and producing this white paper.