Boeing’s Kevin Meehan: 
Active Participation is Key to Adoption of TSCP Solutions

TSCP has been transforming over the past year, signaling a shift in focus and strategy but not objective: to improve and enhance the security of the collaborative environments all TSCP members rely upon to conduct business day to day, to protect sensitive information.

To remain effective and timely, organizational strategies must be examined periodically, and for TSCP, examination means looking closely at where the organization has been, where it intends to go – and how TSCP and its members will get there.

As TSCP continues its transformation, its leadership looks to the executives and senior managers of its platinum members and government organizations to chart TSCP’s course beyond.

Trust Points (TP) recently spoke with Kevin Meehan, The Boeing Company’s CISO, to get his perspective of the business environment that his company faces each day, and how he faces the challenges. The following is an excerpt from that discussion.

TP: The global economic situation continues to stress IT investments. In the area of Secure Collaboration with Industry and Government, what key initiatives and services do you envision will be critical over the next five years? And where is Boeing placing its IT investments, particularly related to security?

MEEHAN: The proliferation of Cloud-based initiatives and the push for Bring Your Own Device (BYOD) are changing the way organizations are thinking about identity management, access control and attribution. I see these challenges continuing to drive key initiatives and services over the next five years.

We have invested in some key initiatives to protect our enterprise from attack. One area of interest to us is authentication and authorization. We continually look for ways to improve these so that we can securely communicate with our partners and customers.

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

MEEHAN: In Information Security our key strategies are focused around investing in our people, ensuring that our systems are highly available, up to date and operating with the latest technology has to offer. We are continually guarding against APT, looking at emerging technologies and ensuring that our long term strategic road map is pointed in the right direction. The framework that drives the alignment of security-based solutions in a constantly changing environment is one that relies heavily on understanding the business drivers and then creating secure, interoperable solutions that are not restrictive to doing business.

TP: What are Boeing’s key objectives related to IT cyber security and identity? Are you pursuing federated access applications internally and/or externally?

MEEHAN: We are enabling federated platforms wherever we can. We have been successful with this with some of our airline customers and suppliers. We’re also evaluating solutions we can use for other methods of two factor authentication. This dramatically improves the security posture for the suppliers, customers. By applying improved methods of authentication and authorization we do try to do as much of it in the background so as not to impose too many steps or restrictions in the process. I try to promote a concept for our customers that "security just happens” and it’s my job to ensure that it does.

TP: What efforts are currently underway and what are best practices or lessons learned in doing data discovery, content classification and data tagging?

MEEHAN: We are leading several efforts within this space. Information Labeling and Handling (ILH) and Intellectual Property Working Group (IPWG) are two of our main initiatives. One of the main points to consider when embarking on these types of initiatives is scalability. It is one thing to have a solid concept; however, it is another thing altogether to operationalize that concept to scale. To be successful in these areas it is critical to be directly involved in the development of international standards, which we are continuing to do.
TP: Are there additional collaborative capabilities that are common across the industry that would benefit from a standardized approach that TSCP should address?

MEEHAN: The current state of collaborative capabilities revolves around the concepts of Identity Management (IdM) and federation. Therefore, we should be looking to address future foreseeable issues, like the next generation of IdM, escalation and de-escalation of privileges, and the role of the aforementioned in relation to procurement from public vendors.

TP: What IT security and cyber challenges or issues are coming down the road for your company? What keeps you up at night?

MEEHAN: One of the main challenges in any large organization for IT security is how effective they are at the operational level. A large part of information security is dependent upon a fast and efficient process for identification, mitigation and remediation of known or potential vulnerabilities.

Like most large organizations, we are working heavily on modernizing our IT infrastructure. We are addressing issues with mobility which establishes a more mature posture from a security standpoint. Right now it's immature within the industry in general. We have seen an increase in reliance on mobile devices which has led to increases in vulnerabilities of these same devices. How do we secure these types of devices so that we can increase our speed of business without sacrificing our security?

TP: What do you see as impediments to Cloud Computing Adoption within the Defense Industry? What areas or programs do you envision going to the cloud?

MEEHAN: There is a real concern that the security and maintenance of the cloud environment will be outsourced, resulting in a loss of control over the end point. That, combined with the motivation of people trying to breach security related to cloud technology, creates a large impediment. Security professionals have to work harder to get ahead of the hackers. I look at cloud as being like Active Server Pages 25 years ago. We need to develop remote wiping and monitoring capabilities and do risk assessments. However, solutions can’t be too difficult for the user.

TP: Looking out 3-5 years, what are your vision and strategic goals that TSCP could help with?

MEEHAN: TSCP can help by soliciting, from its members, ways in which we can securely communicate. A part of secure communications is authentication. One area that TSCP can make an impact in is to aid in the alignment and implementation of concepts like the Trusted Computing Group's (TCG) machine health and NSA-based initiatives like automated policy definitions.

TP: In your opinion, what would be the best approach to adopting TSCP solutions and capabilities?

MEEHAN: The adoption of TSCP solutions and capabilities relies heavily on making sure they align with your internal roadmap. Therefore, to get the most out of TSCP, it is critical to actively participate and develop trusted collaboration with the partners while helping to align TSCP initiatives with your business requirements.

In closing, Kevin asked rhetorically, “Where are the requirements from our customers? What is meaningful and valuable to our customers in the Defense industry?”

He stated, “At Boeing, TSCP is a priority for us. We conduct a monthly TSCP internal call and I’m asking, ‘What are we doing, and when will it be done?’ We need solutions that deliver value to our customers to remain relevant and competitive. It is this focus that will ensure that we remain aligned on providing the most functional, usable and secure solutions for our business.”

Kevin P. Meehan is the vice president of Information Technology (IT) and Chief Information Security Officer for the Boeing Company, responsible for protecting the information and computing resources of the Boeing enterprise. Prior to this assignment, Meehan was vice president of IT Business Systems where he was responsible for developing and maintaining the computing application systems that support Boeing Finance, Human Resources, Corporate, Commercial Capital Business Units as well as the company’s internal systems. Before that he was vice president of IT Operations where he led IT governance, mergers and acquisitions, application, development and sustaining (AD&S) processes, SarbanesOxley (SOX) compliance and the IT long-range business plan. Before joining Boeing, Meehan was at Verizon Wireless, formerly Bell Atlantic Mobile, for 21 years where he held various leadership positions. Meehan was a vice president in IT, leading information security, systems architecture, account management, business development, mergers and acquisitions, and the help desk.

Meehan also held several leadership positions in product development, internet sales, marketing and service, and network product management. Meehan holds several patents for his work in the cellular industry. Before joining Verizon Wireless, Meehan held several financial planning and accounting positions at ARA Services and General Instrument. Meehan received his BS in Finance from St. Joseph’s University in Philadelphia, PA.