CyberPro

Volume 7, Edition 6
March 20, 2014

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Dr. S. Gulu Gambhir, Chief Technology Officer, Leidos

NSCI recently had the opportunity to interview Dr. S. Gulu Gambhir. Gulu Gambhir is Chief Technology Officer, SVP for Leidos – a 23,000 employee science and technology solutions leader working to address some of the world's toughest challenges in national security, health, and engineering. The company supports vital missions for our government and the commercial sector, develops innovative solutions to drive better outcomes, and defends our Nation's digital and physical infrastructure from new world threats.

NSCI: Let's start with the recent spin-off of SAIC and the resulting two companies – Leidos and SAIC. What impact has that had on your cybersecurity-related efforts?

Gambhir: The actual separation into two companies was the culmination of a lot of planning and a lot of attention from the management team. As for the cybersecurity capability, a great majority of that capability from the legacy company is in Leidos, the parent company from the separation. This includes all of our work with the National Security Agency, and cybersecurity efforts in the federal, civil, and commercial markets. The Security Operations Center (SOC) that was part of the company and used internally and for customers is now part of Leidos, and we provide SOC services to SAIC.

NSCI: Can you tell us about a few key products Leidos offers to improve cybersecurity?

Gambhir: We're very strong in several dimensions of cybersecurity, starting with people. We have more than 2,500 certified security professionals that cover all major dimensions of cybersecurity. Our principal offerings are in the areas of secure development and software assurance, accredited testing and evaluation, critical infrastructure, and analytics and threat operations. Our accredited testing and evaluation labs provide the full slate of Common Criteria, FIPS 140-2, FEDRAMP, and NIST PIV accreditation activities.

NSCI: In an area where demand exceeds supply, how does an organization develop, recruit and retain cybersecurity experts?

Gambhir: As I mentioned, our business is built on people. Recruiting, developing, and of course retaining, highly qualified and skilled staff is central to our success. Leidos offers both in-house training and vendor supplied training to our employees. For our in-house training we use our cyber defense training platform CyberNEXS to allow our cyber experts to train on a live network with live attacks. We sponsor many technical sessions that employees can attend both during lunch time talks and after hours.

We make a concerted effort to utilize diverse tactics to recruit the best candidates available. Social media has emerged as a huge asset for our recruiting efforts. We see LinkedIn as an incredibly valuable platform for recruiting because it not only allows our staffing team to search for potential employees, but it also lets candidates get to know Leidos through our corporate page and employee profiles. We also see value in traditional outreach like job fairs, a user-friendly career portal on our website, and advertising and branding campaigns like our recent cyber-focused radio campaign with ads on WTOP and FederalNewsRadio. When recruiting we let potential hires know about the great cybersecurity work that we currently do, the work we have done, the R&D efforts we have, and the opportunities that we afford to be thought leaders in cybersecurity. Our talented cadre of cybersecurity staff plays a critical role in attracting new peers.

We also support STEM initiatives to develop the skills and capabilities of the next generation of workers. We see this as an investment in a well-educated and skilled workforce that will benefit the company, and the country as a whole, for many generations.

NSCI: Let's talk about internal research and development (IR&D) for a minute. How have declining budgets impacted Leidos' cybersecurity IR&D efforts and the ability to stay one step ahead of the threat? Any cybersecurity IR&D efforts you'd like to briefly mention?

Gambhir: Our R&D investment as a fraction of our overall sales has been fairly constant over the last few years, in spite of pressures on our government customer budgets. Our leadership team believes that our R&D investments are critical to creating solutions to our customers' most challenging problems. One way to make our investment dollars go farther is the set of partnerships we have established. For example, we have partnered with the University of California San Diego SuperComputer Center (SDSC) to identify threats to microgrids and recommend mitigations for securing these new energy systems.

A cybersecurity R&D investment we've been making is the development of machine learning-based algorithms, not reliant on the known signatures that many commercial cyber tools use, to detect threats. We're in the process of performing validation and comparison testing now in an operational context.

We are also doing research into methods for automating the identification of vulnerabilities in software binaries using a combination of statistical methods and machine learning. While this research is only in the beginning stages, it is highly relevant to the capability improvements required to enable enhanced cyber security defense capabilities overall.

NSCI: The health industry is obviously changing. What are the cybersecurity challenges and opportunities you see in that area?

Gambhir: We are seeing an increased level of interest in cybersecurity in healthcare. This is due both to changes in the regulatory environment, and to very real changes in the nature of the threat. Regulatory drivers include Meaningful Use requirements for an annual HIPAA security assessment and the go-live of HIPAA Omnibus Final Rule. In particular, the Omnibus Rule has broadened the conditions under which a breach is reportable and for which fines can be assessed.

Fines for security breaches have dramatically increased resulting in a heightened awareness and engagement of healthcare governing boards in cybersecurity issues. As fines and penalties from breaches are paid out from already slim margins, the financial position of the organization can change dramatically post-breach. This can negatively impact bond ratings, capital investments, and abnormal churn of patient populations from their organizations.

Another reason is the sheer value of the medical record against other forms of individually identifiable information which has begun to draw the attention and interest of external threats, like hackers. Our cyber experts tell me that medical record data is worth $50 on the black market, much more than Social Security numbers ($3), credit card information ($1.50), date of birth ($3), or mother's maiden name ($6).

Last but not least, a key motivating factor for cybersecurity readiness in healthcare is the healthcare organization’s commitment to protecting their patients’ information and the negative impact breaches have on patient care as patients distrust their provider and may withhold information or delay seeking treatment.

As a result of this increased focus on cybersecurity in healthcare, we see a significant opportunity to offer our current healthcare clients cyber services which draw upon our prior federal and commercial expertise, appropriately customized for the needs of our clients.

NSCI: What do you see as the most pressing cybersecurity threats in the next few years?

Gambhir: Across all of the platforms that we are reliant on today—personal computers, the internet, mobile devices, financial systems, and automobiles to name just a few— we expect continued growth of sophisticated threats. The ‘internet of things’ is exciting in many ways, offering unprecedented convenience, but also introducing opportunities for those that would seek to exploit these advances. The threat posed by insiders – those with trusted access to systems – is one of the most difficult to defend. Adopting Bring Your Own Device (BYOD) is generally popular with employees, but also generally increases vulnerability.

NSCI: What are the top 2 or 3 technology challenges you think we need to tackle to improve cybersecurity incident prevention, detection, and/or response?

Gambhir: I see a few challenges, and related opportunities, in the areas of information sharing, use of encryption, and use of multi-layered defense.

One of the most effective tools to use against cyber threats is information sharing. This has proven difficult especially among government agencies and organizations like banks and utilities. This communication barrier is often imposed by legal regulation or a desire to not bring exploits to public attention. Part of our challenge is to work with the appropriate levels of government to overcome these barriers through regulation, legislation or some third party broker that can guarantee the anonymity and security of data and sources.

We still see organizations today that have not identified, and protected, their most sensitive data. Use of encryption for the most sensitive data is a must. What’s equally important is that organizations understand and apply the best practices associated with the use of encryption and protect the cryptographic keys that support encryption operations. We have been designing approaches that tackles these problem areas for the past 30 years.

Lastly, not all enterprises use a multi-layered approach to network defense. By using a data-centric security approach, through a combination of zoned defenses and proper application of encryption technologies, organizations can significantly improve their cybersecurity posture. The mindset of assuming that there are malicious attackers inside your network is a good one and drives the need to ensure that these attackers are not able to jump from less sensitive domains to more sensitive domains. Architecting your enterprise to take advantage of zoned defenses is a good approach to segment off your critical data stores and administrative capabilities.

NSCI: What capability improvements do we need to enable more rapid cybersecurity incident identification, assessment and/or attribution?

Gambhir: For more rapid identification of cybersecurity incidents, security analysts must first be able to make efficient use of the volumes of data generated by current event monitoring systems to sift through the ever increasing sets of false positives. This is the bringing together of "big data" methods and traditional cybersecurity tools. At the RSA conference this year, I saw the theme of "big data" meets cybersecurity; for us, these are two areas in which we have had significant capability for some time now. Building enhanced intelligence capabilities into these systems is a good start.
In addition, technology that supports the prediction of probable cyber incidents before they happen will provide analysts with the time needed to take proactive actions against potential misuse. We have been working on capabilities that provide this predictive intelligence through the use of advanced technologies.

Walking around the floor of the RSA Conference last month, it was evident that the proliferation of cybersecurity tools is scaling with the growth in threats. I don't think any single vendor has a complete solution. The key is to bring the most appropriate tools together at the right time and place and in a business model that meets the market's evolving buying habits. We see a cybersercurity environment in both the government and commercial sectors where costs move from a CAPEX to and OPEX model, which enables faster adoption of new and evolving tools.

NSCI: I'll wrap up with this. Are there any Leidos cybersecurity-related successes you'd like to highlight?

Gambhir: We help protect our nation's most critical infrastructure with our cybersecurity efforts for clients ranging from nuclear power plants, banking and financial institutions, healthcare organizations, as well as defense and intelligence community clients. We have defended and supported our clients with cybersecurity incident response and recovery for many years. Recently, our team was called in to help several clients with APT (Advanced Persistent Threats) and ransomware infections in their networks. We helped identify the initial exploitation points, determined the scope of the initial incidents and ongoing activities in order to mitigate further damage to these networks, hosts and resident data. In almost all of these cases, our team of experts delivered analysis results and mitigated the compromise within hours of being onsite.

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

Gambhir: Another theme which runs through multiple questions concerns the challenge we face in balancing personal privacy against the potential need to more intrusively monitor various communications. The privacy issue will become increasingly complicated as we see greater use of personal cyber devices like Google Glass, smart watches, and wireless payment technologies. Broader adoption of internet based services that use wireless communications and are augmented by virtual reality technologies will greatly increase the "vulnerable surface area" in both the public and private markets. Preventing loss of PII, reputation, intellectual property or money will be much more difficult as we see the "Internet of Things" become even more pervasive. Getting ahead of these threats would potentially entail a deeper, more intrusive type of monitoring by security providers, and this is likely to be met with pushback by the public. Working through this will not be a trivial exercise and we need to prepare strategies for this sooner rather than later.

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