CyberPro

January 12, 2012

*Keeping Cyberspace Professionals Informed*

# Senior Leader Perspective: Paul Nguyen, Knowledge Consulting Group

NSCI recently had the opportunity to interview Paul Nguyen who serves as the Vice President of Cyber Solutions for Knowledge Consulting Group (KCG), where he advises federal Chief Information Officers (CIO) and Chief Information Security Officers (CISO) on various cybersecurity issues. He is responsible for the delivery of cybersecurity and advisory services to customers in the federal civilian market and commercial sector.

Paul brings over 12 years of experience as a seasoned cybersecurity practitioner for the federal government and commercial sector, including several Fortune 100 companies.

Prior to KCG, Paul served as Director of Federal Solutions for Neohapsis, where he led the development of their federal practice. His responsibilities included the development of a go-to-market strategy for cybersecurity services to the federal government and overseeing the delivery of client engagements. Before Neohapsis, he served as the federal CISO at the Court Services and Offender Supervision Agency, where he was the recipient of the first *Federal Computer Week* Rising Star Award for his program. He was also previously a Manager for Deloitte & Touche's Security and Privacy Services practice overseeing all Department of Justice cybersecurity and privacy contracts, which included serving as an advisor to the CIO and CISO. He also brings a pedigree as an attack/exploitation practitioner with renowned firms such as @stake, Symantec, and Neohapsis.

Paul received a Bachelor of Science in Business Administration, Finance and a Master of Science in Information Technology Management from Carnegie Mellon University. He also holds certifications for Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA) and Certified in Government and Enterprise IT (CGEIT).

**NSCI: Can you tell us a little bit about KCG and your key cybersecurity products and/or services?**

**Nguyen:** KCG is unique in that we have been providing cyber security services as a sole focus since 2000 which provides us a long history and deep expertise in this space. Since that time, KCG has worked to become the government's trusted advisor for cyber security and brings over 250 security professionals delivering cyber security strategy, governance, risk management, compliance, operations, and high-end security assessment services as a part of our portfolio.

**NSCI: There continues to be talk of needing more and better cyberspace professionals. What does KCG offer that can help with this challenge?**

**Nguyen:** Since our singular focus is Cybersecurity services, KCG has developed a deep pool of expertise and cyber security professionals that we can deliver on-demand. A part of keeping and retaining this

talent focuses on continually developing these professionals through training and our KCG Cyber Academy. The KCG Cyber Academy is an in-house training program with a vast curriculum ranging from specialized training such as ArcSight to simulated cyber ranges for training offensive security professionals. Our commitment to training and career development has allowed KCG to evolve and mature its workforce to meet any of our customer's needs.

**NSCI: What are some of the keys to successful cybersecurity risk analysis and response? What are the critical challenges?**

**Nguyen:** Cybersecurity risk analysis and response requires the right skill set and experience to effectively assess risk. When I evaluate the talent to join my Cyber Attack & Penetration Division (CAPD) which is a highly specialized offensive security and forensics team, we evaluate a professional's ability to execute what I call "logical extrapolation". Logical extrapolation is a learned skill that allows an assessor to derive the exploitation path of compromising a system or application by correlating multiple vulnerabilities to truly identify risk. A lot of times, assessors tend to look at vulnerabilities in a two-dimensional plane and looking at each vulnerability as a singular source of risk which is never the true representation of risk. I believe the technical expertise of an assessor becomes critical in executing the logical extrapolation and giving senior management a true understanding of risk and the vulnerabilities that are truly significant.

**NSCI: How do we actually measure (i.e. quantify) cybersecurity risk, damage, and progress?**

**Nguyen:** It's an interesting topic that has been heavily debated over the last decade. In my opinion, Cybersecurity functions very much like insurance in that we are preparing and planning for potential cyber attacks and incidents and determining the likelihood and impact of these events. In the insurance industry, there exists a wealth of actuarial data collected over hundreds of years to determine the likelihood of events such as floods, earthquakes etc… The same cannot be said of Cybersecurity in terms of these data points that can support the measurement of security due to the infancy of the discipline but also the complex nature.

However, we can measure security in qualitative terms relative to risk with some quantitative measures applicable at the operational level. CISOs constantly battle decisions around risk management and it boils down to dollars and cents for their budgets. Where do I invest my budget? What will yield the greatest return in risk reduction?

These are questions that need to be answered using as much empirical risk data as possible as opposed to "gut" decisions. At the end of the day, we need to have more risk intelligence to be able to make these informed risk management decisions based upon salient data points.

**NSCI: What do you see as the keys to better educating organizations and individuals on cybersecurity threats and vulnerabilities?**

**Nguyen:** From an organizational perspective, I believe there needs to be more information sharing than there is today. There are several initiatives to facilitate this objective but this goes back to my previous point about harnessing the global threat data to make better risk management decisions. There are regulations on the Federal government side for incident disclosures and sharing of threat information through US-CERT but this needs to expand nationally and even globally.

For individuals, universities and our education system are taking greater strides in providing the proper curriculums to form the foundation of a Cybersecurity professional. I attended Carnegie Mellon University in the late 90s and at the time I learned how to be a proficient engineer and developer but the core concepts of security weren't embedded in those curriculums. From my own experience before I become a security professional, I'm certain I wrote my fair share of insecure code. I also think for existing Cybersecurity professionals, there needs to be a more broad-based focus on job rotations to get a better perspective on threats and vulnerabilities. For example, a penetration tester can gain valuable experience understanding the exploitation of vulnerabilities and emulating potential cyber attacks but it would also be useful to have them rotate in positions on the other side defending these attacks in a security operations center. I would argue Cybersecurity is one of the broadest disciplines in IT requiring a professional to understand a wide range of technologies, policies, and processes.

**NSCI: How would you say the government is doing with regards to collaborating with industry to improve cybersecurity? Any recommendations for improvement?**

**Nguyen:** I truly believe we're taking the right steps in forming the public and private partnership especially on the threat information sharing side. It isn't quite mature yet but at any given moment, some entity is under attack whether it's government or industry. The ability to strategically and tactically defend the nation as a whole becomes critical.

**NSCI: What kind of improvements do we need in forensics capabilities to ensure rapid assessment and/or attribution is possible?**

**Nguyen:** In terms of forensic capabilities, I think a lot of organizations vary in their maturity for this type of capability. Forensics is not as heavily utilized as it could be but I believe this comes more from a focus and lack of maturity in other areas. To improve our forensic capabilities, I believe it starts with detection and our ability to collect the data points for us to first identify an incident through artifacts such as logs, data trails, and other evidentiary capabilities. This forms a solid foundation for forensics to improve response times and attribution. The investigation will only be as good as the underlying data and speed is of the essence for these cyber attacks that could have wide-ranging impacts.

**NSCI: It seems to take a lot of time to identify when cyber exploitation is taking place, and even longer to attribute it. How can this be automated to ensure a more timely response?**

**Nguyen:** As I had mentioned previously, I believe organizations and Federal agencies are looking at solutions that can more efficiently aggregate the underlying threat, risk, and vulnerability data to better correlate the attack path of these attacks as a part of our core business in the last 7 years. Organizations suffer from a flood of data generated every second and the ability to find the proverbial "needle in the haystack" becomes critical in quickly identifying cyber attacks for the mere fact of curbing the potential impact. In my experience and through past forensic engagements, cyber exploitation can lay dormant for months without any detection and choose the right time to exfiltrate data unseen by the organization. Automating this capability through a SIEM or other data aggregation/correlation engine becomes critical just by the sheer volume of data that needs to be analyzed.

**NSCI: How do you distinguish / draw the line between cyber exploitation and attack?**

**Nguyen:** I believe there is a very fine line between the two but the motive and intention varies. The means by which they are executed may be similar but the motive and intention will vary. A cyber attack focuses on a more destructive intent and motivation to disrupt or degrade the technology infrastructure of a target which is more overt. Cyber exploitation tends to be more covert and focused on stealing digital assets or exfiltration of data. The implications and impact may vary based upon the intent and motivation of the threat actor.

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

**Nguyen:** I truly believe Cybersecurity is an ever-evolving dilemma that is a constant chess match between attackers and defenders. At the end of the day, we as defenders of our digital environments must be diligent in pushing our programs forward and increasing our awareness and risk intelligence becomes the critical factor for success.

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