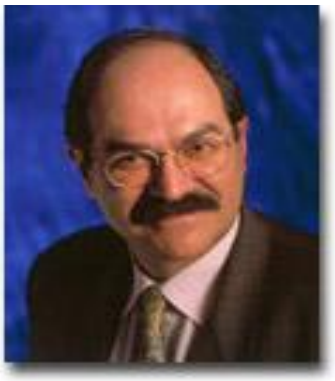
CyberPro

March 24, 2011

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: PANOS ANASTASSIADIS



NSCI's Charles Winstead recently had the opportunity to interview Panos Anastassiadis, Chief Operating Officer of Cyveillance, Inc. Over the last 15 years, Mr. Anastassiadis has established a reputation for creative thinking and leadership in a constantly evolving world of online security, forging the way for an innovative intelligence-led approach to enterprise security. He joined Cyveillance 10 years ago and through his guidance and vision has provided Cyveillance with a strong foundation to establish itself as a world leader in cyber-intelligence leading to the 2009 acquisition by QinetiQ North America. Prior to Cyveillance he served in senior executive positions for several global companies including Merant, Legent, UCCEL and Cincom. Mr Anastassiadis also sits on the board of several leading technology companies and industry associations.

NSCI: Can you tell us a little bit about the capabilities Cyveillance offers?

Anastassiadis: What we provide is cyber security through advanced indications and warnings of various threats that we detect on the open Internet. For 15 years, Cyveillance has led the industry as an innovative developer of cyber security and intelligence solutions. Through our proprietary technology platform and support from expert analysts, Cyveillance enables proactive cyber threat detection and early warnings to ensure immediate and effective prevention and mitigation of those threats. Cyveillance is a wholly-owned subsidiary of QinetiQ North America, a $3 billion organization focused on the government market, and continues to deliver Internet risk and threat intelligence to commercial organizations worldwide while also providing QinetiQ North America with the technology and expertise to enhance its innovative government-focused cyber security solutions.

Through continuous, comprehensive Internet monitoring and sophisticated intelligence analysis, our proactive solutions are delivered to our customers through a SaaS model and focus on protecting against fraud, identity theft, intellectual property and data loss, as well as secure social media monitoring and compliance issues.

NSCI: Let's talk about compliance and reporting for a minute. Compliance implies there are some set standards or expectations to comply with. How do you think government is doing in collaborating with industry regarding standards? From a reporting perspective, what are your thoughts on the efforts to update FISMA?

Anastassiadis: Standards as a whole are good and can help organizations set at least a minimum baseline for information security. The big challenge today is staying one step ahead of the criminals

targeting valuable enterprise data. They have unlimited resources - technology, money, and the ability to entice talented tech professionals into their dark endeavors. When new and better technologies are established to protect data, the criminals step up their efforts to circumvent them. Both industry and government must be relentless in their efforts to protect against cyber-criminals and monitor those efforts to ensure all proper steps are being taken. There always needs to be some form of accountability along the way. They also need to ensure that they educate their entire organizations to make them aware of the everyday vulnerabilities and how everyone plays a critical role in information security; it's not just a technology challenge or solution.

NSCI: What do you think are the keys to reducing cybersecurity threats such as malware and identity theft? How would you describe the "lanes in the road" regarding what government should do versus what industry should do?

Anastassiadis: Instead of the classic identity theft threats we are used to, there are new forms of attacks utilizing social engineering with the objective to go beyond typical money based schemes. These new attacks are using social engineering to target organization's confidential data and intellectual property. With online criminals no longer simply motivated by quick monetary rewards, they will go after anything that can be monetized, meaning that the commercial industry is no longer the top target. That being said, both government and industry need to take similar approaches to deploy technologies that can effectively thwart these schemes and advanced persistent threats.

NSCI: How do you think we move from almost entirely reacting to cybersecurity threats towards a more proactive, predictive model?

Anastassiadis: As a company that has always focused on implementing a proactive approach to security, we are constantly working with our clients to position them to effectively deal with these threats before they become a problem. Traditional approaches to cyber security are all based around the notion of hardening the perimeter, hardening the firewall, and locking down the network. We are different than that. What we do is provide advanced indications and warnings of threats in the wild before they hit your perimeter. As these threats continue to grow in sophistication and volume, organizations need to look beyond traditional security methods. Using proactive cyber intelligence to supplement inside the firewall technologies allows for a more complete and comprehensive security posture.

NSCI: What do you see as the biggest cybersecurity threats in the next year or two?

Anastassiadis: With the advent of Web 2.0, social media and IPv6, these technologies provide an increased opportunity for advanced persistent threats that enterprises are just not used to dealing with. What makes these threats even more dangerous as we look to identify future threats is the proliferation of smart mobile devices. Mobile devices open up a whole new set of attack vectors that reinforce the need for organizations to look beyond the perimeter.

NSCI: It is popular to say that security should be built-in to an application rather than "bolted on" after the fact. Given your background in bringing technology to market, how do you balance that with the time and cost constraints surrounding cybersecurity?

Anastassiadis: Classic perimeter protection is not sufficient because you are focused on being reactionary. The best way to insure a cost effective security program is to identify threats before they materialize. Every asset has its own vulnerability profile. The key is to create a risk model based on what real threats are there, not necessarily what assets you have. If you focus too much on protecting everything, you will miss other threats. And this is what criminals are counting on. You can't protect against everything and if you try you will run the risk of stretching your security net too thin – resulting in time consuming and expensive operations that are not fully effective. Our approach at Cyveillance is not based on reactionary information; rather it is based on actual data and chatter that talks about potential threats. We use our unique capabilities to find and identify the various types of threats online. We look at the composite data and this helps us identify trends and provide valuable information to help the markets stay ahead of online criminals. The key is to focus on what is a threat and not waste valuable time and resources on protecting assets that are not currently vulnerable.

NSCI: There is a lot of talk and attention being given to improving cyber situational awareness. Any advice on the key processes and technologies that should be a part of the solution?

Anastassiadis: In the context of cyber, "situational awareness" not only reflects the cyber environment critical to decision-makers, but also has to include the employee or individual. In the current environment, individuals have so much personal power, choice and availability to access and post online data. The awareness has to go beyond the systems and the perimeter to actually include the individual. Firewalls, IDS, ingress/egress, web filters and anti-virus software are all necessary but can't stop an individual from using their own smart phone to post, text, surf, upload, download, photograph, videotape, etc. All these things are achieved without once having to touch the organization's assets or perimeter. So…what can be done? Education and monitoring must be instituted across organizations. The more your employees and senior management understand the impact and complexities of the cyber environment, the better off they will be in protecting their personal security and the security of the organization. Companies need to realize that cyber situational awareness also includes the understanding of socio-cultural shifts in communications between persons and how that affects antiquated processes. Old policies, procedures and processes need to be revisited to take into consideration new ways of data dissemination (i.e. cyber personas, online behavior, virtual assets, or anonymous chat, VoIP, blogs, Twitter, Instant Messenger, etc.).

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

Anastassiadis: I would just like to reiterate the importance of proactive cyber intelligence. There is a major misconception that if information is out in the open that it is not worth anything. That could not be farther from the truth. While organizations know what type of information they want to keep under lock and key, it is the information that is left unsecure that can be gathered and combined to orchestrate social engineered attacks. It's sometimes difficult to grasp how much information is readily

available on the open Internet. I'm reminded of the comment by Thomas Fingar, Former Deputy Director of National Intelligence when he said "*Open source intelligence can provide up to 90% of the information needed to meet most U.S. intelligence needs*." The only way to stay ahead of the criminals is to make sure you have a complete understanding of what information is out there and how it can be used against you.

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