Growing The Analyst Is Just the Beginning

By: Tony Jordan, Director of Analytics, OPS Consulting LLC

November 2013

Today we see more and more attacks to our personal and corporate digital fingerprints, yet little is being done to prevent further intrusions. However, the OPS Consulting 'Growing the Analyst' curriculum, developed by Department of Defense contract analysts, is a foundational template for participants to build the knowledge, skills and abilities that are required to become a Cyber Analyst in today's fast paced net environments. This curriculum focuses on both technical proficiency and non-technical core competencies that create practitioners that are job ready as soon as they finish training.

The Government Is Trying to Stay Ahead of the Curve

A recent House Bill has been approved aiming to bolster DHS's cyber security workforce. The House Homeland Security Committee amended the Homeland Security Cyber security Boots-on-the-Ground Act to expand DHS' outreach to candidates for IT security jobs by creating a tuition-for-work fellowship and a program to recruit military veterans and unemployed IT specialists for DHS employment.

GovInfoSecurity reports that provisions in the bill include:

- A requirement for DHS to provide contractors with frequent training on how to protect sensitive and classified information related to their assignments. "This provision is responsive to the known vulnerabilities associated with the over-reliance on contractors as underscored by the Edward Snowden case," said the bill's sponsor, Representative Yvette Clarke (D-New York).
- The bill would require DHS to adopt occupation classifications for employees performing activities within DHS' cybersecurity initiatives; DHS would be required to share the classifications with other federal agencies.
- DHS will develop strategies to enhance readiness, capacity training, and recruitment and

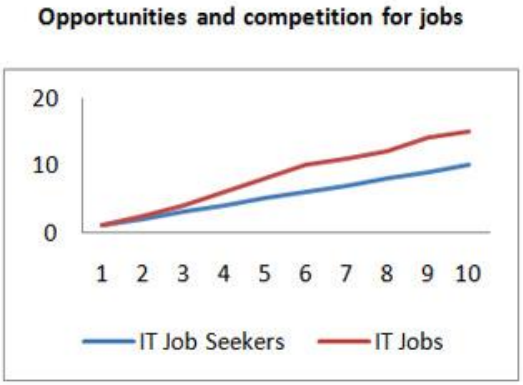
retention of the DHS cybersecurity workforce. A multi-phased recruitment plan and a ten-year projection of federal workforce needs would be developed by DHS as part of the bill.

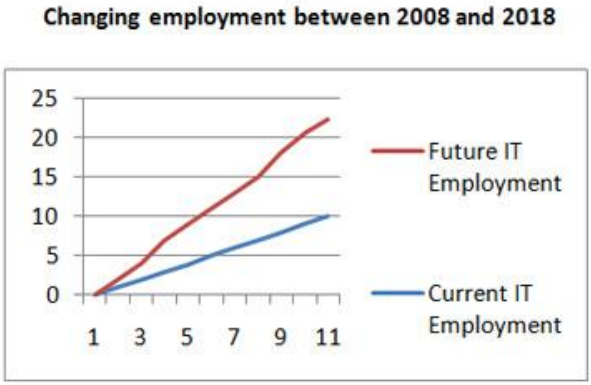
● DHS' chief human capital officer and chief information officer will assess the readiness and capacity of DHS to meet its mission to protect public and private-sector IT systems.

● The DHS secretary will update congress on the development and implementation of cybersecurity strategies, assessments, and training.

Not All Education Pertains to the Workforce You're Pursuing

One of the most difficult impasses when going through the educational processes is finding a curriculum that will not only give the student the knowledge of the topics of interest, but also the application of those subjects. Too often the main focus of education is only on "concepts" without real work application, while concepts are vitally important it can be a disservice to the end goal of certifying qualified personal in a timely and impactful way. The educational focus needs to reflect the same sentiments as the students who go through the process, to have knowledge and application of the subjects they are learning. This concept will in turn generate a more qualified candidate, who has real experience in the field they are looking to enter.





You Don't Need to Work for DoD to See the Cyber Solutions Right in Front of You

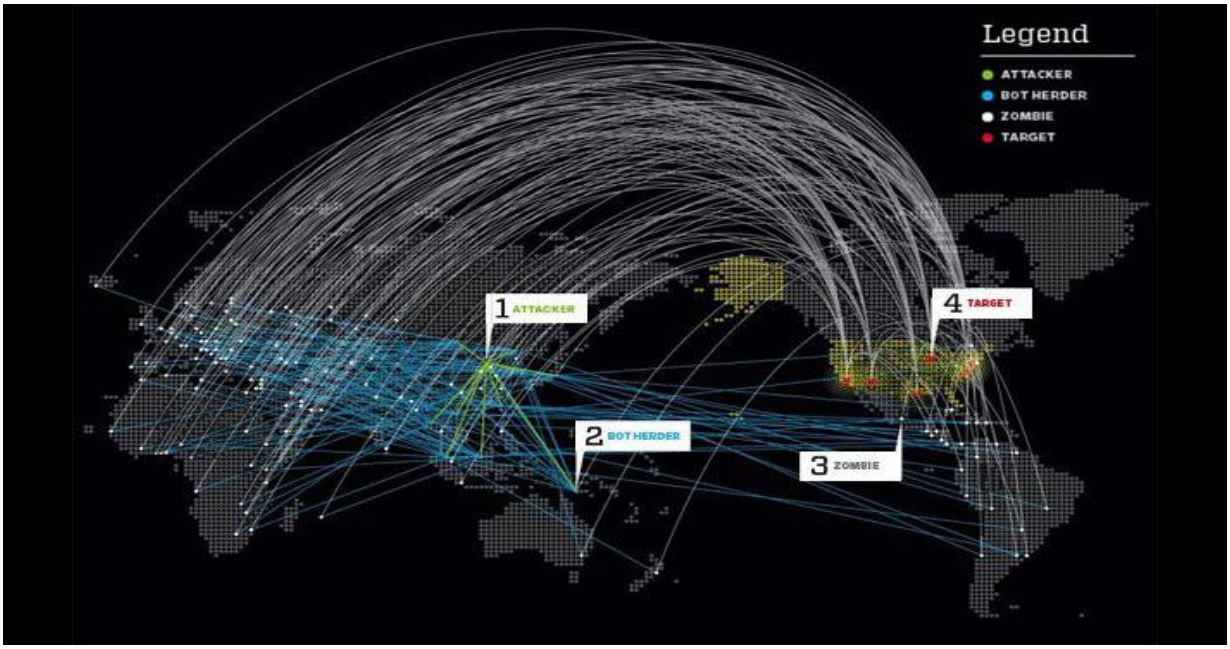
Contrary to the belief that the government possesses the majority of responsibility for the secure cyber realm, it actually falls on each and every one of us, just as importantly. Attempted denial of service attacks not only happen on a national level, but hit closer to home on local internet service providers. These attacks are looking to vacuum as much personal information as possible. All this is happening while the everyday "normal" user, thinks that their "internet is just running slow." Cyber threats are around us at a constant, so recognition of those threats is the quintessential first step to prevention.

GAO Threat Table

Threat	Description
Bot-network operators	Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power - impacts that could affect the daily lives of U.S. citizens across the country.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once

	required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, who execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations who distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434 (Washington, D.C.: May, 2005).



So How Do We Bridge the Gap Between Concept and Application

As the need for cyber security continues to grow, we need to ensure that students currently in the workforce or about to enter it have the practical experience not just the knowledge. Taking students through a full gambit of "what to expect" while in the field is the catalyst to a workforce who stays ahead of the threat. Through the use of curriculum developed around real-time exercises and instructors who are field experienced in Cyber Analytics, as well as network intrusion and detection; students will be at the front edge of the job market and their peers who just possess textbook knowledge.

Now How Does OPS Consulting Meet the Need of Tomorrow's Cyber Threat

Our Growing the Analyst curriculum has gained a substantial amount of traction within industry, as well as governmental partnerships, and we believe it to be a foundational keystone in the development of a career analyst. We have taken analysts within industry and developed a course that does something no other program offers, and that is putting real world application to knowledge gained. Our 3 leveled curriculum are described as follows:

Level I

The kickoff course to "Growing the Analyst," will allow students to gain the knowledge and skills required to perform the duties of a digital network analysts, learn about computer topologies and devices, network communications protocols and addressing, and how to identify devices within a network. Use Python programming language to write simple programs. Learn routing concepts and protocols and how to analyze a router configuration for network mapping purposes, and identify tools and techniques for open source research that will assist with network reconnaissance and analysis.

Level II

The secondary course of the cyber analyst curriculum, builds upon concepts covered in level I. The course dives deep into networking fundamentals to give the student in depth knowledge of how computer networks function. All concepts from the level I curriculum will be enhanced to provide the student a deeper knowledge of network devices, routing/internet protocols, and critical thinking. The student will be able to demonstrate what they have learned, through computer labs and practical exercises designed by industry analysts.

Level III Participants will demonstrate the knowledge and skills acquired through levels I and II of the cyber analyst curriculum. Following a brief review of concepts, tools, and techniques covered in previous levels of the cyber analyst program, participants will be assigned a target. Once the participants are assigned a target they will begin researching their target using data mining techniques taught in previous lesson. In a simulated environment, the participants will review traffic entering and leaving their target network and will document their findings. Following the external network monitoring phase, Participants will monitor internal network traffic, document their findings, and build a network map. After all phases of reconnaissance are complete, participants will create a target package and present the package to instructors in both written and oral formats.

In Summary

For educational partners, business owners, and governmental organizations, with limited time and resources, coupling real world experience with classroom instruction can be a big challenge. Developing the right framework for execution of education and training is imperative to be an effective, leading institution.

By understanding how to fully prepare a student for entering the cyber analyst workforce, we can truly state they have the tools to hit the ground running. There is no one-size-fits-all solution. However, faster and more qualified results will be displayed by soliciting help from qualified experts in the cyber analytics industry who have experience in real-time.

The OPS Consulting Drive

OPS Consulting uses the power of technology and the science of engineering to help guide its clients toward high-value and high-performance customized systems engineering, software development and business management solutions. To help you achieve mission objectives successfully, we join your team to learn everything we can, and then we develop and execute a comprehensive plan to steer your objectives in the right direction and achieve your goals.

Since our founding in 1999, we have grown quickly due to a strong corporate culture that advocates team work and professionalism, integrity in all we do, and a focus on delivering exceptional customer-focused results quickly and efficiently.

Please feel free to contact me via email at tonyjordan@opsconsulting.com or call 443-545-9812