CyberPro

March 22, 2012

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: MARC NOBLE, (ISC)²

NSCI recently had the opportunity to interview Marc Noble, currently the Director of Government Affairs for (ISC)². (ISC)² is the globally recognized Gold Standard for certifying information security professionals. Prior to his role at (ISC)², Mr. Noble worked as an Information Assurance Engineer for MITRE Corp., and held the offices of Chief Information Security Officer and Deputy Chief Information Officer at the U.S. Federal Communications Commission. Over the course of a 30-year government career, Marc also served as Senior Information Security Analyst, Administrative Office of the U.S. Courts and as a Management and Systems Analyst at the U.S. General Services Administration.

In a volunteer capacity, Mr. Noble currently serves as a member of the (ISC)²'s Government Advisory Board for Cyber Security (GABCS) and U.S. Government Executive Writers Bureau as well as Senior Vice President of the Northern Virginia Chapter of the Information Systems Security Association (ISSA-NOVA).

NSCI: Can you give us an overview of (ISC)² and tell us about any cyber-related goals the organization has for 2012?

Noble: In 1989, (ISC)²® was formed by a passionate, dedicated group of volunteers who set out on a quest to create standards for information security best practices, leadership and ethics. Twenty-two years later, with the addition of management and staff, expansion of global efforts and a continual emphasis on developing and improving industry standards, (ISC)² is now the largest not-for-profit membership body of certified information security professionals worldwide, with over 80,000 members in more than 135 countries, recognized as the Gold Standard of information security credentials.

As we move into 2012, (ISC)² stands committed to making the cyber world a safer place for everyone by building, supporting, advocating for and protecting communities around the globe - current information security communities, future information security communities and civic communities. Advocating for the information security professional communities we serve and the people they protect will be our focus in 2012. It is in this spirit that we launched the (ISC)² Foundation at the end of 2011. The Foundation is devoted to making the cyber world a safer place for everyone by supporting cyber security education and awareness in the community.

NSCI: What collaboration takes place between (ISC)² and the Department of Homeland Security, Department of Defense, and/or Department of Education regarding cybersecurity?

Noble: In 2004, the Department of Defense (DoD) officially unveiled its 8570.1 directive, a program that requires every one of its information security employees to receive a professional certification that's accredited under the global ANSI/ISO/IEC Standard 17024. This mandate was undertaken in pursuit of one clear goal: To ensure that the right people with the right skills were matched to the right job in the right environment. DoD's initiative validated the need for a well-trained, professionalized information

security workforce to guard effectively against emerging threats and identified it as a critical and distinct profession.

Over the years, (ISC)2 has worked closely with the Defense-wide Information Assurance Program (DIAP) to support the implementation of 8570. This cooperative arrangement offers plenty of lessons for other federal agencies and even foreign governments that are considering implementing their own enterprise-wide mandates for a professionalized information security workforce. (ISC)^2 is committed to supporting DoD in any program that helps government organizations around the world recognize that they, too, need to invest in their information security workforce.

Specifically in support of the 8570 mandate, (ISC)^2 submitted the CISSP certification for ISO Standard 17024 evaluation and accreditation. In 2004, it became the first information security credential to be accredited under the global ANSI/ISO/IEC Standard 17024 and since has received accreditation for six more of its certifications, with six considered DoD 8570-approved certifications. Our organization is also supporting this DoD initiative by developing education materials that explained the goals and requirements of the program to DoD personnel, including a Frequently Asked Questions document and a fact sheet; creating programs that helped the DoD meet its goals such as the (ISC)^2 eLearning educational program; Web-based seminars with live instructors; an online assessment tool, the StudISCope self-assessment; dedicated CBK Review Seminars and exams at diverse DoD locations. (ISC)^2 also participates in the U.S. Defense Activity for Non Traditional Education Support (DANTES) Program, which reimburses DoD personnel in the Army National Guard, Army Reserve and Air Force Reserve for certification exam costs. Many of our exams, in fact, are offered at DANTES testing centers.
In summary, this unique relationship is working and is one that has a larger significance for the broader information security community.

(ISC)^2 has also been a long-time supporter of DHS' National Cyber Security Awareness Month (NCSAM) in the United States, which is celebrated annually in October by the National Cyber Security Alliance (NCSA). Throughout the month, (ISC)^2 supports NCSAM globally by: recognizing information security leadership in the U.S. federal government at its eighth annual GISLA Gala; posting security awareness tips on its social media sites and blog throughout the month of October; and recognizing the first Executive Women's Forum's Cyber Security Schools Challenge winner in the individual category, U.S. Safe and Secure Online volunteer, Gary Alu, CISSP, for reaching more students than any other single Challenge participant.

(ISC)^2 is working closely with DHS to socialize the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework in coordinating with other certification bodies and associations and its members.

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

Noble: Keep in mind that my perspective is from cyber security workforce perspective. My opinion is that government and industry must develop a unified approach to the problem that marries the ideas

and viewpoints of all stakeholders, including cybersecurity education groups, certification bodies and their members, professional groups, cybersecurity innovators, academia and legislators. At a grassroots level, there are several subsets of these communities that are working toward this purpose, however, to date, NICE represents an initiative that covers the broadest interest in collaboration with the greatest number of groups.

NSCI: Regarding cybersecurity, where would you like to see more government involvement? Where would you like to see less involvement?

Noble: (ISC)^2 believes it is essential that government and industry cooperate to meet the demands of securing the national infrastructure. This should be a public/private partnership, where all parties have equal footing, not government regulating the security practices of industries. The government should work with the industries involved to develop a managed risk profile that meets each industries needs so that the proper controls can be determined by an industry so cost-efficient solutions can be implemented without being too burdensome on an industry. This is a tenuous balance for the government, which tends to view its role as a leader rather than a partner.

NSCI: Where would you like to see the government focus their cybersecurity efforts in 2012?

Noble: Without a doubt, building the next generation of information security professionals is where I would like to see the government focus its cyber security efforts. But without the government gaining a greater understanding of the cybersecurity profession, it will be difficult for agencies to recruit and hire the right talent and to develop a pipeline of future talent.

With its recent draft Framework, the NICE Initiative lays the groundwork for greater understanding of the profession by developing a common language regarding the work requirements of cybersecurity professionals. But there is one thing government has not yet addressed - it still does not recognize the information security profession as a separate and distinct career field.

In 2012, I would like to see the Office of Personnel Management take a leadership role and create a professional job series for the cybersecurity workforce and see the Office of Management and Budget put in place a directive that all departments and agencies employ the same professional certifications that the Department of Defense requires in Directive 8570.1.

NSCI: We seem to have made tremendous progress the last few years in cybersecurity training and education. Industry, academia, and government all seem to be increasing their efforts. What would you like to see over the next few years?

Noble: I would like to see an ongoing commitment by industry, governments and academia to provide 1) awareness programs for children 2) scholarships for students from high school through post-graduate work 3) research that illuminates the information security issues facing governments, private industry, educators, the information security profession and society.

NSCI: Nearly everyone has paid a lot of attention to educating and training the cyber workforce. How are we doing at educating the cyber citizen who routinely uses the Internet, but doesn't necessarily have a cybersecurity job?

Noble: We believe that an understanding of security of computers and communications is essential to real-world survival. In order to ensure that we have a qualified, skilled future cyber security workforce, we need to make security awareness, education and certification a year-round, lifelong pursuit.

In terms of progress, I can only speak for my organization. At (ISC)², we believe that in order for us to thrive as a digital society, security education should be a requirement for all students in the classroom, starting in primary school. We need to think of security education as not just an elective but as a requirement for any student – elementary school, middle school, high school or college – who plans to turn on a computer or mobile device. And, security-savvy users means less work for security professionals. We support cyber security awareness initiatives around the globe each year, including Safer Internet Day in Europe, Clean PC Day in Hong Kong, and National Cyber Security Awareness Month (NCSAM) in the United States. We also invest our resources in the following efforts:

Security Awareness Month (NCSAM) in the United States. We also invest our resources in the following efforts:

- Growing our Safe and Secure Online program. Our member volunteers have reached nearly 70,000 students in four countries where we have active programs, and we hope to double that number by 2013 and to reach parents with our new materials geared specifically for their needs.
- Providing US$140,000 in scholarship opportunities to qualifying undergraduate and graduate students.
- Facilitating access to communities of practice and other professional development resources, such as the Associate of (ISC)² program, which allows those early in their information security careers a chance to test their knowledge as they work to gain the work experience required to become certified. We recently expanded our Associate of (ISC)² program for the CSSLP and CAP credentials.
- Advocating for the profession and the people in it at the local and national levels through outreach, research, and collaboration with groups like eSkills (UK), the National Initiative for Cybersecurity Education (NICE - US), US Cyber Challenge, the Cooperative Research Centre (Australia), the Career Technical Education Foundation (US), and the Cybersecurity Credentials Collaborative (C3) (global)

- Opening our SSCP® credential/knowledge base to college and university programs worldwide in an effort to establish these seven domains as the standard, accepted knowledge-base of postgraduate education worldwide for future information security practitioners.

- Supporting scholarships for the 25 winners of the "Capture the Flag" (CTF) competition at the US Cyber Camps held nationwide. The CTF competition offered high school and college students from across the United States the opportunity to learn and compete against their peers in this virtual cyber war game. The CTF event is part of MITRE's Science, Technology, Engineering and Mathematics (STEM) outreach program.

- Teaming up with CTEF and Sypris Electronics to develop, establish and host a new cyber security curriculum for local and national high school students. The curriculum was co-developed by Sypris, MITRE, and CTEF and supported by (ISC)². Students get hands-on training, learning from cyber experts in a real-world cyber lab. Students who completed the program and passed the (ISC)² SSCP certification exam became an Associate of (ISC)².

NSCI: Cybersecurity is obviously an international challenge. How does (ISC)² work with international stakeholders?

Noble: (ISC)²'s membership consists of the top information security professionals in the world. We have six advisory boards, representing the needs of information security and secure software professionals in Asia-Pacific, Europe/Middle East/Africa, Latin America, North America, US government and application security. These groups meet regularly and consist of senior-level volunteers who advise (ISC)² on the needs of the local information security community. We also launched a Chapter Program last year to provide information security professionals around the world a forum to network, share knowledge and strengthen communities with local, like-minded professionals. We're also a founding organization of the Cybersecurity Credentials Collaborative (C3), a global group whose purpose is to provide a forum for collaboration among vendor-neutral information security and privacy and related IT disciplines certification bodies that will result in the advancement of IT careers, a more prepared workforce, greater insight into how certifications are developed, and how they meet the IT needs for organizations, including governments, private enterprises, educational institutions, and the public at large.

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

Noble: Children represent the workforce of the future. We can even look to their online attitudes and behaviors as predictors of their practices in the workplace. It is essential that we introduce them to safe and secure online practices and as cyber security as an exciting, rewarding, stable yet upwardly mobile career field at an early age to ensure the future of the profession and the security of our society.

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