Editors: Cynthia Irvine, irvine@nps.edu | Alec Yasinsac, yasinsac@southalabama.edu

NICE: Creating a Cybersecurity Workforce and Aware Public

Celia Paulsen, Ernest McDuffie, William Newhouse, and Patricia Toth | US National Institute of Standards and Technology

In early 2010, US President Barack Obama created the National Initiative for Cybersecurity Education (NICE) as part of expanding the Comprehensive National Cybersecurity Initiative (www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative) from an internal, federal focus to a national activity. NICE aims to create an operational, sustainable, and continually improving program for cybersecurity awareness, education, training, and workforce development that measurably advances the US's long-term cybersecurity posture. Although NICE focuses on the US, it recognizes the international nature of cyberspace and believes that by partnering with multinational companies, international standards organizations, and the global academic community, its actions can have positive effects around the world.

NICE was created with the idea that an important resource in the fight against cyberthreats is people: people who can create the technologies that protect information and resources, people who can recognize cyberthreats and respond to them, and people who understand how to protect themselves and others in cyberspace.

A Community Effort

Over the years, many disparate organizations from industry, academia, and government have recognized a need and started activities to improve the awareness, education, and training of cybertechnology users. Many of these activities have unique target audiences, approaches, motivation, and features. Some emphasize certification, others promote new technologies, and still others focus on cyberethics. All these activities are noteworthy but are often specialized and disconnected from each other. So, educators and trainers have difficulty gaining a holistic view of the available resources and determining exactly what to teach. Consequently, students emerge with inconsistent, unbalanced knowledge and skill sets that might or might not benefit the job for which they're hired.

In cybersecurity, there are no silver bullets; cybersecurity awareness, education, and training are no different. Cyberspace's interconnected and distributed nature consistently demonstrates that a weakness at one point often profoundly affects the security of another point. Because of this, NICE is intentionally a community effort, engaging academia, industry, government, and public participation.

As the lead of NICE, the US National Institute of Standards and Technology (NIST) seeks to connect all existing cybersecurity awareness, education, and training activities to help identify weaknesses

1540-7993/12/$31.00 © 2012 IEEE

and opportunities, share and expand strengths, and bring people together to solve lingering cybersecurity education problems.

Several US federal agencies have joined with NIST to form the NICE team, including the Departments of Homeland Security, Education, Defense, Labor, Justice, and Commerce; the National Science Foundation; the Office of Personnel Management; and the National Security Agency. In addition, various academic, industry, and nongovernment organizations, including some international organizations, have become involved. They share resources, lessons learned, and new ideas through activities hosted by NICE, and they promote and support NICE activities in their various communities. Later, we give some examples of how you can become involved in NICE.

This initiative has four complementary components:

- awareness,
- formal education,
- training and professional development, and
- workforce structure.

The first three components work together to cover the US population's diverse needs. Their activities include informing the public about how to avoid cybersecurity threats, improving cybersecurity education in both lower- and higher-level schools, and training cybersecurity professionals more effectively.

The workforce structure component provides a technical foundation for NICE by defining the cybersecurity workforce and creating a recruitment and retention strategy. One of its most recent accomplishments is the *NICE Cybersecurity Workforce Framework* (http://csrc.nist.gov/nice/framework).

The Framework

One of the more pressing problems NICE has faced is inconsistency in definitions and descriptions of cybersecurity work. This inconsistency makes it difficult to set job requirements, identify needs, and provide training and professional-development opportunities.

In response, dozens of academic, industry, government, and nongovernment organizations and subject matter experts collaborated to create the *NICE Cybersecurity Workforce Framework*. This draft document organizes cybersecurity work and workers into seven high-level categories and 31 specialty areas. Each specialty area has a list of associated knowledge, skills, and abilities (KSAs); tasks; and competency areas.

This collaboration aimed to codify cybersecurity talent; define the cybersecurity workforce in common terms; and tie the workforce's various jobs, competencies, and responsibilities into a common architecture. The framework provides a structure and common lexicon to describe the cybersecurity workforce at its most basic levels. As such, it's intended to be comprehensive and flexible. It aims not to replace existing organizational frameworks but to be layered on top, allowing organizations to better map their current and future workforce to constantly evolving cybersecurity requirements. It strives to capture every possible cybersecurity skill or competency and sort them into specialty areas related to cybersecurity. Additionally, the framework shows how cybersecurity applies to more than just traditional information assurance fields. Cybersecurity KSAs are needed in a variety of jobs, including legal advisor, contracting officer, chief information officer, and software engineer.

Organizations can choose which KSAs and tasks apply to a specific work role. Because cybersecurity workers often play multiple roles in their organization and throughout their careers, workers can and should find themselves in more than one specialty area. For example, a system administrator might conduct some tasks under both system administration and knowledge management specialty areas but won't use all the KSAs in each.

This competency-based framework expedites and gives rigor to workforce baselining, gap analysis, training catalogs, professional development resources, and more. Over time, NICE will continually update the framework as a living document to ensure it remains relevant and current. The close connections between NICE and the cybersecurity community will facilitate this process.

Educate and Employ

Educators and trainers can use the framework to help answer these critical questions:

- What am I preparing my students for?
- What knowledge and skills do they need?
- What should I be teaching?

By mapping out which KSAs and specialty areas to cover, educators and trainers can better understand how their students are prepared for careers in cybersecurity. When mapping curricula, it's important to take into account required and optional courses, within and outside the traditional computer science, computer engineering, information systems management, or information assurance topic areas.

Educators and trainers might be surprised at how many or how few of the KSAs their curricula or training content covers. Occasionally, they might find that, although they expertly cover one or more competencies such as computer languages or infrastructure design, these competencies cover only a small portion of the KSAs. Conversely, they might find that some of their programs that are not directed toward cybersecurity professions cover many KSAs in a specialty area.

KSAs often overlap and draw from several disciplines. So, identifying what knowledge and skills are needed for an individual to advance in a cybersecurity career might not be easy. Many educators and trainers might choose to focus on specific specialty areas, ensuring their students obtain all the KSAs listed in those areas. Others might first let students decide what career path they want and then select the courses for them that best cover the necessary KSAs. Schools and training organizations, by mapping their curricula to the framework, will produce a better-prepared person for the workforce. Hiring organizations, by mapping their cybersecurity needs to the framework, will be able to identify the cybersecurity skills they want in an employee.

> **NICE has partnered with community centers, school districts, and colleges and universities around the US to help run Cyber Citizen Forums.**

US colleges and universities looking to teach cybersecurity can also use the framework to help them qualify as a Center of Academic Excellence in Information Assurance Education (CAE/IAE; www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml). Gaining the CAE/IAE designation gives institutions prestige in the US cybersecurity education sphere. By the end of 2011, 145 academic institutions had received this designation (www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml). The standards used by the Committee on National Security Systems to determine CAE/IAE qualification are being mapped to the framework. This will allow educators to understand qualification requirements and describe their programs using a common lexicon and architecture.

Changing curricula or training content to teach cybersecurity in alignment with the framework can be simpler than you might realize. Instructors frequently can insert KSAs into existing courses, including courses that deal with seemingly unrelated topics such as enterprise architecture or computer language. For example, business management or software development courses could cover information assurance. Instructors could expand a basic networking course to include information on intrusion detection system tools and applications. Each school or training organization will likely structure and teach the KSAs differently. However they do the mapping, it will help ensure that the appropriate KSAs are taught.

Inform and Engage

In addition, educators and trainers can use the framework to generate interest in cybersecurity. Many people don't realize the variety of cybersecurity fields or that they might already have many of the skills needed for a job function.

For example, the framework shows that a worker performing in the incident response specialty area might

- inspect a hard drive,
- identify vulnerabilities and make recommendations for remediation, and
- coordinate with and provide expert technical support to network technicians to resolve incidents.

An educator or trainer could use this information to describe to students how somebody in this specialty area might be like a detective, investigating incidents and then figuring out how to resolve them. This might sound especially appealing to some students who otherwise would have shied away from cybersecurity.

Some educators and trainers might find that their students already have many of the KSAs for a specialty area. For example, when looking at the list of vulnerability assessment and management KSAs, students at any grade level could find they already have knowledge of data backups, basic system-hardening techniques, and network architecture concepts. So, this specialty area and the associated cybersecurity jobs might be especially appealing to them. Having some or all of the KSAs for a specialty area gives students an idea of what sorts of positions they might enjoy and provides a solid foundation on which to build.

Getting Involved

NICE and its partner organizations provide a number of convenient opportunities for individuals and groups to help improve the cyber behavior, skills, and knowledge of technology users everywhere.

The Stop.Think.Connect. campaign (www.dhs.gov/files/events/stop-think-connect.shtm) seeks to increase understanding among the general US population about cyberthreats and how to be more secure online. Friends of the Campaign is a consortium of individuals and organizations who distribute campaign materials, blog about issues, and help teach about cybersecurity issues.

Similarly, NICE has partnered with community centers, school districts, and colleges and universities around the US to help run Cyber Citizen Forums. These forums teach basic cybersecurity skills, start dialogues on cybersecurity education, and encourage community involvement in cybersecurity awareness and training. Anyone can host a forum and tailor it to his or her needs. Information, posters, banners, presentations, and other materials to help you run a forum are available for free at www.dhs.gov/files/events/stop-think-connect-get-involved.shtm. Recent forums have taken place in Florida, Arizona, and Massachusetts, with positive feedback.

For high school and college educators as well as government and industry representatives looking to interest students in cybersecurity, one increasingly employed tool is competitions. Examples include the

- CyberPatriot National High School Cyber Defense Competition (www.uscyberpatriot.org),
- US Cyber Challenge (http://workforce.cisecurity.org),
- DC3 (Department of Defense Cyber Crime Center) Digital Forensics Challenge (www.dc3.mil/challenge), and
- National Collegiate Cyber Defense Competition (www.nationalccdc.org).

These and other competitions provide exciting environments for students to learn about cybersecurity and gain hands-on experience. NICE is working to expand such competitions' use and usefulness and correlate them to the framework. Often, skills used in cybersecurity competitions directly correspond to KSAs in one or more specialty areas.

At Advanced Technological Education centers (ATE; http://atecenters.org), secondary schools, community colleges, universities, industry, and government agencies collaborate to

- support curriculum development,
- support professional development of secondary school and college faculties,
- develop career pathways, and
- carry out other related activities.

By working together, these organizations avoid unnecessary duplication of effort and promote easier transitions between academic and career levels. ATE programs include CyberWatch (www.cyberwatchcenter.org), the Center for System Security and Information Assurance (www.cssia.org), and the Cyber Security Education Consortium (www.cseconline.org).

At the annual NICE Workshop, educators, trainers, and other interested parties can join with industry and government personnel to discuss cybersecurity education issues, raise concerns, and discover resources. Last year, more than 300 attendees represented a broad array of organizations, from the University of Puerto Rico to the National Security Agency to Microsoft. Topics discussed ranged from cybersecurity competitions to certification to formalized curricula. The next workshop is scheduled for fall 2012.

To find out more, visit http://nist.gov/nice, and join in the conversation on Twitter by using the #nistnice and #cybersecurity hashtags. ■

Acknowledgments

Any mention of commercial products in this article is for information only; it doesn't imply US National Institute of Standards and Technology recommendation or endorsement.

Celia Paulsen is a technical advisor for the National Initiative for Cybersecurity Education at the US National Institute of Standards and Technology. Contact her at celia.paulsen@nist.gov.

Ernest McDuffie is the lead for the National Initiative for Cybersecurity Education at the US National Institute of Standards and Technology. Contact him at ernest.mcduffie@nist.gov.

William Newhouse is the program manager for the National Initiative for Cybersecurity Education at the US National Institute of Standards and Technology. Contact him at william.newhouse@nist.gov.

Patricia Toth is a technical advisor for the National Initiative for Cybersecurity Education at the US National Institute of Standards and Technology. Contact her at patricia.toth@nist.gov.

cn *Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.*