Cyberspace Education and Training

Larry K. McKee, Jr., NSCI;
Jim Ed Crouch, NSCI
July 6, 2010

National Security Cyberspace Institute, Inc. (NSCI)

Through the combination of research and education, NSCI supports public and private clients aiming to increase cyberspace awareness, interest, knowledge, and/or capabilities. NSCI is committed to helping increase security in cyberspace whenever and wherever possible. NSCI publishes a bi-weekly newsletter (*CyberPro*), has published numerous whitepapers on various cyberspace topics, maintains an online cyber reference library, and has established an email distribution list for sharing cyber-related resumes to interested parties. NSCI is a small, veteran-owned business headquartered in Virginia.

Issues

Over the past few years, the increasing numbers and sophistication of attacks in cyberspace have caused higher-level attention from throughout government, industry, academia, and the public at large. A recent statement from Max Stier, president and CEO of the Partnership for Public Service, points to that level of interest: "President Obama has declared cyber-security to be 'one of the most serious economic and national security challenges we face as a nation' and has pledged to address these threats. The only way to get it done is to build a vibrant, highly trained and dedicated federal cyber-security work force." In spite of this emphasis, the U.S. government continues to fall short in recruiting and retaining information technology professionals to meet our expanding requirements. Even with a 57 percent growth in the federal IT workforce over the past eight years, hiring gaps still exist, primarily because of three factors: (1) a dramatic increase in our dependency on technology to deliver goods and services; (2) the current and impending retirements of members of the baby boom generation; and (3) declining interest by U.S. students in the science, math, technology, and engineering disciplines.

So how bad is our shortage? Rep. Michael Arcuri, D.-N.Y., said on the House floor that the government alone will need to recruit and hire up to 1000 more cybersecurity workers each year in order to address potential threats.[1] Compare this to the number currently being trained: 80 cybersecurity professionals a year within DoD,[2] and about 120 scholarships funded for entry-level positions in other government departments and agencies.[3] This shortage is not only one of sheer numbers; there's also a quality deficit. According to Alan Paller of the SANS Institute, an organization that educates and trains system administrators and computer engineers, schools aren't turning out enough students with the technical know-how to defend critical networks. "This shortage is as tough as the shortage of scientific people we had in the 1950s," Paller says. "The country has about 1,000 people that could compete in a cyber competition at a high level today. We actually need between 20,000 and 30,000."

The Partnership for Public Service has launched a new program designed to recruit, hire and retain entry-level information technology workers in the federal government. The program, called FedRecruit: IT Pilot Program, is designed to help agencies meet the need to fill what the Partnership estimates will be about 11,000 technology job openings during the next three years.[4]

The rising demand for skilled cyber professionals has resulted in a very competitive recruiting environment, not only between the public and private sector but also among the various departments and agencies within the federal government, and internationally. With the need for trained people increasing virtually every day, how can we grow the pool of cyber warriors available to meet this need?

For starters, we need to get them interested early – perhaps as early as middle school – in the IT-related disciplines. Given the fact that our current generation of young people have grown up as "digital natives," this

[1] Cyber Workforce Take in House Bill; NextGov; Brittany Ballenstedt; February 4, 2010; http://wiredworkplace.nextgov.com/2010/02/house_passes_cyber_workforce_reforms.php
[2] James Lewis, Director of CSIS Technology and Public Policy Program
[3] http://ourpublicservice.org/OPS/documents/IT%20Issue%20Brief%20Final.pdf
[4] http://ourpublicservice.org/OPS/documents/IT%20Issue%20Brief%20Final.pdf

Larry K. McKee, Jr., NSCI;
Jim Ed Crouch, NSCI
July 6, 2010

would seem to be an easy task. However, there is a big difference between being a proficient user of IT and having the skills and training necessary to be described as a cyber professional. As our public schools continue to drift away from traditional education curricula, we face a significant challenge in reversing that trend and restoring science and math to their rightful places of importance. Nonetheless, an increased awareness campaign directed at the public at large can pay secondary benefits in terms of garnering interest from young people in protecting their own pieces of cyberspace. This could result in follow-on interest in cyber as a career. And even without that additional benefit, there is a critical need to strengthen what many consider the weakest link in the security chain – the general public. We simply must push for a concerted education effort that establishes a relationship between the general public and cybersecurity in all aspects of our lives.

The threat is certainly not insignificant. For example, The Black Hawk Safety Net, a large cyber recruiting and training web site hosted in China, offered instruction on cyber attacks and sold Trojan software, which allows outside access to a computer when remotely installed. Established in 2005, the site had recruited more than 12,000 paid and 170,000 free members and collected more than 7 million yuan ($1.02 million) in membership fees prior to its shutdown in February, 2010.[5] These cyber attackers are finding the United States and other high-tech countries to be target-rich environments. Because anyone can gain access to the internet without training in security, their computers can easily be targeted, even becoming "botnets" that can carry out the plans of criminals or rival nations. According to Richard Harknett and James Stever of the University of Cincinnati, "Most users are unaware that not only is their computer data vulnerable, but that their insecure access to cyberspace can be exploited by others turning them into unwitting agents of coordinated cyber threats [both criminal and disruptive attacks]."[6] Vice Admiral Carl Mauney, Deputy Commander of U.S. Strategic Command, succinctly says it best: "Ignorance is our biggest vulnerability." To combat the threat, we must decrease our vulnerability by ensuring a better-informed general public to complement a larger, better-trained force of cybersecurity professionals. Harknett and Stever go on to say, "Cybersecurity must become a national civic responsibility."[7]

The laws of supply and demand apply to the costs of hiring cyber professionals just as they do in other areas of the market. Because of this, government organizations have a tough time competing with the private sector. Moreover, the competition for top-level talent extends across the entire spectrum, not only between government and commercial entities, but also internally within the two sectors and internationally. While there is something to be said for American patriotism and the security of being a government employee, neither of these are likely to overcome significant compensation differences between the public and private sectors.

Along with the other federal departments, DOD has been unable to fill its requirement for experienced information assurance professionals, primarily because of the huge unmet need for training.[8] There are no uniform, government-wide certification standards and no federal career path for cybersecurity specialists. There is insufficient training for workers to upgrade skills, inadequately funded federal scholarship programs to lay a foundation for a talent pipeline, a cumbersome and lengthy federal hiring process, and a lack of in-house capability at many agencies to properly manage contractors.[9] To date, no one in the government has been tasked with assessing the cybersecurity workforce, how many people will be needed across the federal system in the short and long term, what skills are necessary and how top talent will be obtained. This lack of trained defenders of our

[5] China: Large hacker training Web site shut down; http://www.cnn.com/2010/TECH/02/08/china.hackers/index.html
[6] Richard Harknett and James Stever; University of Cincinnati Political Science Department; The Cybersecurity Triad: Government, Private Sector Partners and the Engaged Cybersecurity Citizen
[7] Richard Harknett and James Stever; University of Cincinnati Political Science Department; The Cybersecurity Triad: Government, Private Sector Partners and the Engaged Cybersecurity Citizen
[8] The Cyber Workforce Gap; Federal Computer Weekly; Sean Gallagher; http://fcw.com/articles/2010/01/25/cover-story-long-cyber-march.aspx
[9] Add workforce woes to cybersecurity chief's agenda; Max Stier; December 24, 2009; http://fcw.com/articles/2009/12/24/max-stier-howard-schmidt-cybersecurity-workforce.aspx

Larry K. McKee, Jr., NSCI;
Jim Ed Crouch, NSCI
July 6, 2010

networks is leading to serious gaps in protection and significant losses of intelligence, resulting in an adverse impact on our national security.

From technicians to policy makers, the shortage extends throughout most organizations – both private and public – struggling to fill the growing demand. The intensity of the competition has sparked a bidding war among agencies and contractors for a small pool of special talent: skilled technicians with security clearances.

Because cyberspace is a relatively new domain for criminals and other bad actors, most federal information technology managers do not know what advanced skills are needed to combat cyberattacks, said Karen Evans, information technology administrator in the Bush administration. However, a consensus appears to be emerging with federal IT leaders focusing on specialties including computer network engineering, forensics, software development, defense, vulnerability, and protocol analysis, intrusion detection, and, in the case of the military and intelligence communities, digital exploitation and attack.[10] They are finding these positions very difficult to fill.

The U.S. Cyber Challenge, a nationwide series of competitions, aims at identifying young people with exceptional computer skills and inspiring them to join the country's woefully understaffed ranks of cybersecurity specialists needed to protect systems used by the military, industry and everyday people.[11] Organizers of the event say that without competitions of this type, hackers' skills often go unrecognized or unappreciated by those around them and sometimes even by themselves.

In August 2009, Homeland Security Secretary Janet Napolitano warned that our government must move quickly from a cyber 1.0 world to cyber 3.0 and beyond if we are to protect federal computer networks from attacks. This means building a highly skilled workforce, Napolitano acknowledged. "How do we grow our own cyber experts who will work within a government framework, and how do we make sure we will recruit and retain top talent?" she asked.[12]

Contributing to the problem has been a lack of high-level leadership, with no one in charge of assessing and planning government-wide workforce needs. A comprehensive, integrated strategy is needed to overcome the talent deficit. The administration must assess its short- and long-term workforce needs, develop a government-wide blueprint to recruit, hire and retain top cybersecurity talent, and then aggressively implement it. This plan should provide guidance on the appropriate roles for civil servants and private contractors. Government should lead a campaign to encourage universities to offer, and students to pursue, cybersecurity educational programs.[13]

Internationally, the U.S. is lagging the fight. In a recent competition jointly sponsored by the National Security Agency and software developer TopCoder, programmers from China and Russia dominated on everything from writing algorithms to designing components. Of the 70 people advancing to the finals from a field of 4,200, 20 were from China, 10 from Russia and only two from the US.[14] China, North Korea, and other countries have well-developed graduate education programs in cyber warfare.[15] Additionally, these nations send students to

---

[10] Panel Passes Cyber Workforce Reform; Federal Times; Max Stier; September 14, 2009; http://www.federaltimes.com/index.php?S=4273437
[11] Cyber Challenge tests nation's top hackers; Jeanne Meserve and Mike M. Ahlers; http://www.cnn.com/2009/TECH/12/21/cyber.challenge.hackers/index.html
[12] Panel Passes Cyber Workforce Reform; Federal Times; Max Stier; September 14, 2009; http://www.federaltimes.com/index.php?S=4273437
[13] Panel Passes Cyber Workforce Reform; Federal Times; Max Stier; September 14, 2009; http://www.federaltimes.com/index.php?S=4273437
[14] US geeks struggle in NSA hacking contest; TechWorld; Patrick Thibodeau,June 9, 2009; http://www.techworld.com/news/index.cfm?RSS&NewsID=117142
[15] Timothy L. Thomas, *Dragon Bytes: Chinese Information-War Theory and Practice from 1995–2003* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 18–23; and Senator Mary Landrieu, "Combating Threats from Cyberspace," *Hill*, 17 June 2008, http://thehill.com/op-eds/combating-threats

Larry K. McKee, Jr., NSCI;
Jim Ed Crouch, NSCI
July 6, 2010

America's finest graduate institutions for master's and doctoral degrees in cyber-related disciplines such as computer science, computer engineering, and electrical engineering.[16]

In a commentary for *Federal Computer Week*, Stier says, "Clearly there is a need for more effective policies, sophisticated software and better information technology management. But there is also an urgent need to close the technical skill gap, a task that will require a coordinated federal effort to recruit, hire and train professionals in computer network engineering, forensics, software development, defense, vulnerability and protocol analysis, intrusion detection, and, in the case of the military and intelligence communities, digital exploitation and attack."[17]

Calling for action, Stier writes in the *Federal Times*, "The time is overdue for the government to commit the resources and exert the leadership to build and nurture a highly skilled cyber workforce."[18]

Ideas

In their research paper, "The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen" Harknett and Stever argue that even if responsibility for cybersecurity is successfully moved to the Executive Office of the President, much more reorganization and governance changes will be required to implement cybersecurity policy effectively throughout the American federal system.

However, even with an engaged and energetic government, our security will suffer without an equally engaged and knowledgeable public. As Harknett and Stever point out, "The ubiquity of computer technology throughout the civilian population will require full societal engagement if the national objective is a secure cyberspace...The general population must be engaged as active security providers, not simply beneficiaries of security policy, because their practices often create the threats to which government responds..."[19]

Harknett and Stever say that as the digital environment grows in scale and scope, "so too will the need for a cyber civic culture to emerge to manage it." Comparing today's cyber threat to the mobilization of the general public to face the nuclear threat of the 1950s, they have this to say: "Ironically, because the citizenry is less conscious of the cyber than the nuclear threat (as national security threat), a much greater degree of civic mobilization and understanding will be required to face this 21st Century challenge."[20]

As the public becomes more aware of the threat posed by hackers, criminals, or nation-states with malicious intentions, we should see a rising interest in cybersecurity as a profession. A number of colleges across the country have begun to add cyber-related programs in response to the increasing demand for these types of individuals. Polytechnic Institute of New York University has created a master's degree in cybersecurity; Georgia Tech offers a master's degree in information security online; Carnegie Mellon in Pittsburgh; Purdue in West Lafayette, Ind.; and George Mason in Fairfax, Va., are among other universities with master's programs in cybersecurity.[21]

Beyond the college programs, there are a number of private and public organizations stepping up to the plate on cybersecurity. The U.S. House of Representatives has passed The Cybersecurity Enhancement Act, which provides a strengthened role for the National Institute of Standards and Technology in shaping the way the federal government and the nation address cybersecurity. The bill also addresses the Scholarship for Service program,

---

[16] Cyber ACTS/SAASS; Air & Space Power Journal - Winter 2009; December 1, 2009; Major Paul D. Williams
[17] Add workforce woes to cybersecurity chief's agenda; Max Stier; December 24, 2009; http://fcw.com/articles/2009/12/24/max-stier-howard-schmidt-cybersecurity-workforce.aspx
[18] Government should help widen cyber knowledge; Max Stier; http://www.federaltimes.com/article/20090914/ADOP06/909140302/1037/ADOP00
[19] Richard Harknett and James Stever; University of Cincinnati Political Science Department; The Cybersecurity Triad: Government, Private Sector Partners and the Engaged Cybersecurity Citizen
[20] Mobilizing the Public on Cybersecurity; Phil Leggiere; http://www.hstoday.us/content/view/12082/149/
[21] Wanted: 'Cyber Ninjas'; New York Times; Christopher Drew; http://www.nytimes.com/2010/01/03/education/edlife/03cybersecurity.html

which provides funding – $108.7 million over a five-year period – to colleges and universities to award scholarships to students in the information assurance and computer security fields in exchange for their service in the federal government after they have completed their training. After graduating, students will be required to serve in the government for a period equal to their length of scholarship.[22]

National Security Agency (NSA) Information Assurance Centers of Academic Excellence provide NSA partnerships with over 100 universities around the country who are teaching the kind of skills NSA needs. The National Science Foundation has awarded a $2.7 million grant to an eight-state consortium of technology centers and community colleges that is working to block cyber attacks and stop the loss of high-tech jobs in the U.S. The three-year grant to the Cyber Security Education Consortium will help train a new generation of cyber warriors whose job it will be to prevent potentially crippling Internet-based attacks and stop the drain of knowledge and jobs to nations such as China and India, where 2 million technological workers have U.S.-related jobs, the officials said. Programs funded by the grant will offer cyber education security and work force development training at two-year institutions in the eight states. The consortium's primary objective is to provide high-quality cyber security programs in at least 19 metropolitan areas within the eight-state region and provide advanced cyber skills to 2,500 students and 3,000 workers to halt the outsourcing of high-tech jobs.[23]

In the private sector Lockheed Martin has a talent management strategy to support cyber security workforce demands. The cyber profession begins with talent sourcing and recruitment and continues with certification, training, and mentoring, to move professionals along an established career track.[24] Lockheed Martin has also created a Cyber University, which facilitates training and certification using a blended delivery approach from instructional-led training to professional study groups, lunch-time seminars, and communities of practice. Current and new employees are able to leverage cyber security training and education to include CISSP certification, Security +, and technology training from Lockheed Martin Cyber Security Alliance Partners Cisco and McAfee.[25]

Raytheon has two programs aimed at keeping its cybersecurity business competitive and constantly refreshed with new talent. One is aimed at making the good even better, while the other program hopes to convince middle-school students how important math is to their future. Both are concerned with creating the cyber warriors of today and tomorrow.[26]

The Department of Defense has begun to pick up the pace in cyber recruitment, education, and training. DOD Directive 8750 mandates that military personnel, civilian employees and government contractors be certified as information assurance professionals before they can have administrative access to DOD networks and systems. As stated in the most recent Quadrennial Defense Review, "The Department will redouble its efforts to imbue its personnel with a greater appreciation for the threats and vulnerabilities in the cyber domain and to give them the skills to counter those threats and reduce those vulnerabilities at the user and system administrator levels. DOD is also growing its cadre of cyber experts to protect and defend its information networks..."[27]

One example of DOD's efforts is the two-day "Cyberdawn" exercise, one of the country's premier electronic war games. The chance to test their cyberskills has attracted groups from private companies as well as the U.S. military.

---

[22] Learn to Hack on the Government's Dime; Michael Cheek; http://www.thenewnewinternet.com/2010/02/05/learn-to-hack-on-the-governments-dime/
[23] Cyber Consortium Gets $2.7 Million Grant; Enterprise Security; By Tim Talley; October 16, 2009; http://www.enterprise-security-today.com/story.xhtml?story_id=69519
[24] Lockheed Martin Invests In Cyber Security Talent And Workforce Development; January 20, 2010; http://www.darkreading.com/security/government/showArticle.jhtml?articleID=222301688
[25] Lockheed Martin Invests In Cyber Security Talent And Workforce Development; January 20, 2010; http://www.darkreading.com/security/government/showArticle.jhtml?articleID=222301688
[26] Raytheon Pushes Math and Science, Both Critical to Cybersecurity It Says; Matthew Harwood; June 12, 2009; http://www.securitymanagement.com/news/raytheon-pushes-math-and-science-both-critical-cybersecurity-it-says-005756
[27] Depart of Defense Quadrennial Defense Review; January 26, 2010

Larry K. McKee, Jr., NSCI;
Jim Ed Crouch, NSCI
July 6, 2010

Teams take part in the game in the hopes of protecting a simulated digital network linking phone systems, Social Security numbers, and power grids on which 10,000 fictitious citizens rely.[28]

The Center for Cyberspace Research at the Air Force Institute of Technology has been awarded a renewal grant in the amount of $2.1 million to continue its Scholarship for Service fellowship program that recruits and educates talented civilians to work for federal, state or local governments on cyber security issues. Those selected for this competitive fellowship attend AFIT all expenses paid for two years and earn a Master's degree in Cyber Operations. Students also receive a stipend of $25K a year for living expenses. After graduation, the student works as a civilian for a federal, state or local government agency for two years.[29]

The U.S. Cyber Challenge consists of three competitions: (1) the DC3 Digital Forensics Competition, a DOD competition that focuses on cyber investigation and forensics. The DOD is especially interested in this, and is offering a $1 million prize to people who can find solutions to digital forensics problems that currently can't be solved. (2) The CyberPatriot Defense Competition, a national high school cyber defense competition run by the Air Force Association. Now in its second year, it is being brought under the Cyber Challenge umbrella. (3) NetWars Capture the Flag Competition, a SANS Institute challenge, played across a network on a custom OS, and with the aim of penetrating the opponent's net security and controlling key files on a server.

These competitions and camps are designed to identify 10,000 young Americans with the interest and computer skills to become the next generation of cybersecurity professionals. The overall program is intended to nurture and develop their skills, give them access to advanced education and exercises, and enable them to be recognized by colleges and employers where their skills can be of the greatest value to the nation. Promising candidates will be invited to attend regional "cyber camps" at local colleges, with the chance for scholarships to study cyber defense. The cream of the crop may be offered placements in corporations and federal agencies that deal with cyber warfare.

Assuming these people can be recruited, how do we ensure their talents and training are compatible with the cybersecurity tasks they will be required to perform in their government jobs? A measure in the U.S. Senate, sponsored by Jay Rockefeller (D-W.Va.) and Olympia Snowe (R-Maine), would direct the Commerce Department to develop or coordinate and integrate a national licensing, certification and periodic recertification program for cybersecurity professionals. It would then become unlawful for a person lacking the proper license and certification to provide cybersecurity services to an agency or for an information system or network designated as critical infrastructure.[30]

However, there are questions about enforcement, legal liability, the value of certification versus licensing, and how federal requirements would affect states' rights and their traditional role in licensing various professions.[31]

The use of certification as a tool for hiring, placing and promoting employees is certainly nothing new. However, a mandatory licensing program would be unprecedented, and that proposal has proven particularly contentious. "A lot of people have problems with where do you draw the line: Who has to get a license, who doesn't, who would be the licensing authority, what would be the extra cost, what are the liability issues?" said Lynn McNulty, director

[28] U.S. is Striking Back in the Global Cyberwar; US News; Alex Kingsbury , Anna Mulrine; November 18, 2009; http://www.usnews.com/articles/news/2009/11/18/us-is-striking-back-in-the-global-cyberwar.html
[29] Center for Cyberspace Research awarded a $2.1 million grant; August 18, 2009; http://www.af.mil/news/story.asp?id=123163766
[30] New proposal would require cybersecurity workers be certified; Ben Bain; June 26, 2009; http://defensesystems.com/articles/2009/06/22/feat-cybersecurity-training.aspx
[31] New proposal would require cybersecurity workers be certified; Ben Bain; June 26, 2009; http://defensesystems.com/articles/2009/06/22/feat-cybersecurity-training.aspx

of government affairs at (ISC)² and a former federal information security program manager. (ISC)² is one of numerous organizations that constitute an expansive training and certification industry.[32]

During a roundtable discussion on certifications (ISC)² hosted in early June 2009, several participants said the licensing requirement would represent a departure from the state-based approach to validating the qualifications of professionals such as doctors and lawyers. Critics say another problem with licensure and its added layers of federal oversight is that the government's training and testing programs would not evolve as quickly as industry-driven certification programs.[33]

Establishing certification or licensing requirements would force the government to define skill sets and career paths for cybersecurity professionals. Such tracks are common for other government jobs but nonexistent for IT security.[34] Brenda Oldfield, director of cyber education and workforce development in the Homeland Security Department's National Cybersecurity Division, has been working for years to establish a common set of skills for information security professionals in the government. That effort has been folded into the education component of the Comprehensive National Cybersecurity Initiative, the multiyear, multibillion-dollar program launched by the Bush administration. Oldfield co-leads the education initiative for DHS in cooperation with DOD. "We have to be able to validate that cyber professionals have the skills needed, but we have to identify what those skills are uniformly," Oldfield said.[35]

The certification issue has sparked debate about its purpose and value. Although a good certification standard might be a measure of a baseline level of competence, it is not an indicator of job performance.[36] There are also concerns about certification becoming, in effect, a "license to practice" for cybersecurity professionals. As stated by Daniel Castro, a senior analyst at the Information Technology and Innovation Foundation, licenses are typically only required in professions in which the public is harmed by the absence of licensure. Castro goes on to say, "Therefore, the implicit assumption in arguing for a certification program for all federal cybersecurity professionals is that the public is being harmed because unqualified workers are filling those jobs -- not because of a lack of talent or insufficient training but because hiring managers cannot distinguish between competent and incompetent cybersecurity workers. That is the *only* problem that certification (in the form of a de facto license) could fix. However, no proponent of that approach has provided evidence to show that the problem exists, nor is the problem commonly cited in other studies as a factor contributing to cybersecurity risks."[37]

Castro also had this to say: "If certifications were effective, we would have solved the cybersecurity challenge many years ago. Certainly more workforce training, although not a panacea, can help teach workers how to respond to known cyberattacks. However, workforce training is not certification, and organizations, not Congress, are in the best position to determine the most appropriate and effective training for their workers.[38]

Given the rapidly-changing nature of both threats and capabilities in cyberspace, some experts question whether certifications can keep pace. One anonymous blogger, responding to Castro's *Federal Computer Week* opinion

---

[32] New proposal would require cybersecurity workers be certified; Ben Bain; June 26, 2009; http://defensesystems.com/articles/2009/06/22/feat-cybersecurity-training.aspx
[33] New proposal would require cybersecurity workers be certified; Ben Bain; June 26, 2009; http://defensesystems.com/articles/2009/06/22/feat-cybersecurity-training.aspx
[34] New proposal would require cybersecurity workers be certified; Ben Bain; June 26, 2009; http://defensesystems.com/articles/2009/06/22/feat-cybersecurity-training.aspx
[35] New proposal would require cybersecurity workers be certified; Ben Bain; June 26, 2009; http://defensesystems.com/articles/2009/06/22/feat-cybersecurity-training.aspx
[36] Certifications are not a panacea for cybersecurity woes; Federal Computer Weekly; Daniel Castro; December 01, 2009; http://fcw.com/articles/2009/12/01/comment-castro-certification.aspx
[37] Certifications are not a panacea for cybersecurity woes; Federal Computer Weekly; Daniel Castro; December 01, 2009; http://fcw.com/articles/2009/12/01/comment-castro-certification.aspx
[38] Certifications are not a panacea for cybersecurity woes; Federal Computer Weekly; Daniel Castro; December 01, 2009; http://fcw.com/articles/2009/12/01/comment-castro-certification.aspx

piece, expressed this sentiment well. Commenting on the inadequacy of standard certification exams in this environment, he wrote: "...We are narrowing knowledge, focusing energies in the wrong places, and stamping out diversification. You can count on future attacks against networks to be based on concepts outside what's tested on cert exams."

Another blogger who called himself "Army Civilian," had this to say: "What we need are classes detailing the security settings on firewalls, Internet security and acceleration servers, domain controllers, exchange servers, Unix, Apple, etc. These are all given by the vendors of the hardware/software we use. Security comes from technical expertise of the product one is familiar with, not a generic book full of security best practices for businesses… The CISSP certification gives the government a warm, fuzzy feeling but secures nothing."[39]

These arguments have extended beyond the certification and licensing of only professional cyber security personnel to include formal training and certification for all computer users. According to Dr. Russell Smith, a leading criminologist in Australia, "There's been some discussion in Europe about the use of what's called a computer drivers license - where you have a standard set of skills people should learn before they start using computers. At the moment we have drivers licences for cars, and cars are very dangerous machines. Computers are also quite dangerous in the way that they can make people vulnerable to fraud. In the future we might want to think about whether it's necessary there be some sort of compulsory education of people before they start using computers."[40]

DOD's current IT-related certification requirements cover a spectrum of management and technical information assurance roles for some 90,000 military, civilian and contract employees. Officials created the program in 2004 in response to departmental Directive 8570, released a manual of instructions in 2005 and updated that manual in 2008. Under the program, they identified commercially available, accredited certifications that information assurance employees and contractors need to have to work on DOD systems. [41] DOD officials decided to take advantage of existing commercial certifications rather than develop custom programs so that employees would have skills they could use in the private sector or at other agencies.[42] However, this approach has been met with some criticism. For example , Alan Paller, director of research at the SANS Institute, a cybersecurity training, certification and research organization, supports the idea of evaluating security professionals' skills in operational situations, as airplane pilots are tested. Paller said the way DOD developed its program by surveying commercial certifications was a huge error. He believes a certification program should measure specific skills that people use in specific jobs — something he said DOD's approach doesn't do. "My sense is if we care about this enough to make it a national law, we ought to make it much more technical and much more sophisticated," Paller commented.[43]

John Lainhart from IBM's Global Business Services disagrees. Lainhart said DOD's program, which is based on U.S. and internationally recognized certifications, is preferable. "Let's not reinvent the wheel," Lainhart said. "We'll achieve a global standard that way by using the certifications that are out there, and I think that's again consistent with [President Barack Obama's] cybersecurity policy review."[44]

---

[39] Army civilian; http://fcw.com/articles/2010/01/11/backtalk-security-certification.aspx
[40] Crime expert backs calls for 'licence to compute'; Ben Grubb; Aug 27, 2009; http://www.itnews.com.au/News/154129,crime-expert-backs-calls-for-licence-to-compute.aspx
[41] New proposal would require cybersecurity workers be certified; Ben Bain; June 26, 2009; http://defensesystems.com/articles/2009/06/22/feat-cybersecurity-training.aspx
[42] New proposal would require cybersecurity workers be certified; Ben Bain; June 26, 2009; http://defensesystems.com/articles/2009/06/22/feat-cybersecurity-training.aspx
[43] New proposal would require cybersecurity workers be certified; Ben Bain; June 26, 2009; http://defensesystems.com/articles/2009/06/22/feat-cybersecurity-training.aspx
[44] New proposal would require cybersecurity workers be certified; Ben Bain; June 26, 2009; http://defensesystems.com/articles/2009/06/22/feat-cybersecurity-training.aspx

Cyberspace Education and Training

Larry K. McKee, Jr., NSCI;
Jim Ed Crouch, NSCI
July 6, 2010

It is encouraging to see that incremental progress is being made and that there now exists in the United States a serious debate on how best to attack the challenges posed in defending cyberspace. However, much is left to be done.

Answers

Rather than continuing to debate on how to provide perfect cyber security, perhaps we should be taking decisive action to get started. As George Patton famously said, "A good plan violently executed now is better than a perfect plan next week." We know it won't be perfect, but we can certainly be flexible enough to make changes on the fly. Just as flexibility is the key to airpower, so too will it be key to cyber. The right answer today will not be the right answer next year; so let's get started and accept the fact that cyber education and training will continue to be a moving target for the foreseeable future.

A central issue for the federal government and private industry is hiring and retaining skilled cyber professionals. In addition to effective recruiting programs, organizations must implement systems that track qualifications and currencies to ensure the limited number of experts are assigned to the right positions. These individuals should also be active participants in identifying continuing education and experience needed to maintain the breadth and depth consistent with their responsibilities.

Personnel requirements must be more clearly delineated. Merely saying we need more "cyber professionals" is inadequate; organizations must understand the specific cyber skills that are unique to their missions, roles, and tasks. After determining the requirements, we must identify our gaps in expertise and numbers and develop/implement a plan to address those gaps. This will require a significant breadth of knowledge about available training and education programs – public, private, and academic – and a certain amount of trust/partnering between the disparate organizations involved.

Ramp up our recruiting efforts. Leverage intern programs, student temporary employment programs and student career experience programs to attract students with the hope that they will choose a career in cyberspace. Boost budgets for recruiting the best graduates in areas including computers, engineering, and mathematics. Merely sending "head hunters" to recruit top cyber talent may be insufficient. Organizations serious about top talent will ensure recruiters understand the position requirements and are able to accurately communicate benefits and career growth opportunities.

Money talks. Increase grant money available to attract young people to careers in science, technology, engineering and math (STEM), with an emphasis on computing. According to the Computer Research Association, computer science enrollment dropped 43 percent between 2003 and 2006. We must reverse that trend. Demonstrate as early as middle school the high-paying career possibilities that exist for science and math students, and the impact cyberspace will have on the future.

Provide career progression opportunities for IT specialists, including management and senior executive positions as end-game goals. Establish and/or endorse programs offering a concentration in the rapidly-growing field of computer forensics – gathering, preserving, and investigating evidence stored on digital devices.

Grow capability through cyber exercises and experiments. Give users hands-on experience and learning opportunities, preferably against "red force" adversaries. Also, incorporate tabletop exercises when resources are limited. Ensure scenarios require collaboration and information sharing with external organizations. From these exercises and experiments collect and share lessons learned and best practices. Create a culture of collaboration through the entire process – pre-event planning, to execution, to after-action reporting. Ensure scenarios include both public and private entities. Also, design exercises that require collaboration and information sharing between different levels of government – national, state, and local – and across departments within the government. Exercises and competitions such as Cyber Storm and Cyber Challenge have been very successful. We need more of these types of events, especially at the local and regional levels.

Cyberspace Education and Training

Larry K. McKee, Jr., NSCI;
Jim Ed Crouch, NSCI
July 6, 2010

Although we should never deemphasize the importance of people in cyber security, we must continue to aggressively pursue advanced technologies. Tools that can monitor, analyze, and alert can help relieve the requirement for personnel to perform tedious tasks. We also need tools to provide a Common Operational Picture as a Situational Awareness aid for commanders and other leaders. These technologies should be able to collect and correlate data from multiple sensors and multiple data feeds, generating alerts to users. Eventually, technology may provide intelligence to recommend specific priorities and/or actions.

When we acquire new technologies, we should ensure our people are thoroughly trained to employ all the capabilities resident in them. Training and technology should not be either/or resource choices for cyber leaders to make; they should be complementary and synergistic. In short, advanced technologies should be pursued to increase the effectiveness and efficiency of our cyber experts, not to replace them. We will always need trained cyber experts capable of leading and making decisions.

Hands-on training and certifications are a must. Establish metrics to measure training success. Treat cyber qualifications the same way we treat pilots by having them demonstrate their ability via "check rides." Periodic recertification should also be required. This could be done via a "cyber lab" or “range” that could also be used when hiring new employees to verify the required hands-on skills. Additionally, training should include information on the latest threats and technologies.

Educate policy makers, implementers, operators, and end users about cyber security and hold them accountable. Although not everyone can be security experts, they can be taught basic defense methods and how to spot and report suspicious activities. This will require top-down leadership and commitment. Cyber security is an executive responsibility as it significantly impacts nearly every aspect of an organization. Enforce company policy with training, including mock scenarios that include the potential consequences of poor practices. Training should also include operating in a degraded cyber environment to ensure personnel are able to work through a "cyber attack."

The importance of public awareness can't be understated. Beyond formal education, U.S. cybersecurity strategy must include a public awareness campaign that permeates the workplace, schools and homes. Some experts have pointed to the example of Smokey Bear in the fire prevention campaigns used since the mid-1940s.

Education of users could include classes or better user instructions to accompany the purchase of new products. These might include more detailed instructions – as opposed to "default" – on how to set security settings for firewalls and general computer hygiene information. Along with enhanced consumer education, should there be in place a few safeguards to protect those consumers from problems beyond their control?

Beyond public awareness, some security responsibility may have to be nationally mandated. For example, how much longer can we afford to allow "naked" computers on the net? When Internet Service Providers learn of viruses, worms, trojan horses, or other malware, shouldn't they be responsible for alerting consumers? How much product liability should be assumed by software developers when they release flawed code? Would some form of product liability that includes a recall of defective products – much as we do with automobiles – be appropriate?

Skills

With human skills being in short supply yet so important to cybersecurity, we offer a list of the ten top IT jobs for 2010 as compiled by *Network World*. An expanded discussion of these positions is available at http://www.networkworld.com/news/2010/020110-best-it-jobs.html

1. Security specialist/ethical hacker
2. Virtual systems manager
3. Capacity manager

4. Network engineer
5. Open source specialist
6. Service assurance manager
7. Electronic health records systems manager
8. Sourcing specialist
9. Service catalog manager
10. Business process engineer

In designing and implementing recruiting and training programs, government managers should consider "information to design, secure, assess, exploit, attack and defend seven types of networks -- telephony, Internet protocol, satellite, land mobile radio, industrial control systems, integrated air defense and tactical data link."[45]

A recent Information Security Today Career Trends survey revealed the below qualities at the top of the list for information security professionals in 2010[46]:

1. Data protection and classification from a business perspective
2. The effective integration of information security practices into key business and risk management efforts
3. The need for specialization and differentiation
4. Proficiency in fraud and forensics investigations
5. The need for grounded academic focus and educational program

In a recent interview with *Network World*, Tom Silver, senior vice president with Dice.com, provided an apt description of the marketability of well-trained and educated cyber professionals: "If you know how to keep your company's data secure, you were in demand yesterday, are in demand today, and will be in demand tomorrow."[47]

It is our view that executing cyber security starts with top down-directed recruitment, training, and education programs that produce knowledgeable, innovative thinkers, problem solvers, and professional cyber warriors. Backing these with sensible standards; private, public, and personal accountability; and laws with teeth to prosecute miscreants of all stripes could start us moving toward a more secure and safe cyber world.

[45] Training evolves to support cyber mission; 81st Training Wing Public Affairs; Susan Griggs, http://www.aetc.af.mil/news/story.asp?id=123157023
[46] The Future of the Information Security Profession; GovInfo Security; Upasana Gupta; December 11, 2009; http://www.govinfosecurity.com/articles.php?art_id=1997
[47] 10 best IT jobs right now; Network World; Denise Dubie; February 2, 2010; http://www.networkworld.com/news/2010/020110-best-it-jobs.html