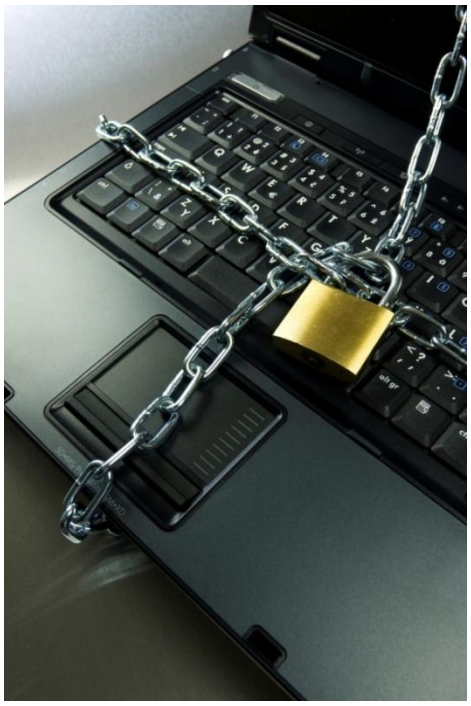
CyberPro

April 2009

Keeping Cyberspace Professionals Informed

ENABLING CYBER SECURITY IN A HOSTILE THREAT ENVIRONMENT

BY ANDREA BELMONT-GWILT & TRACY NITTI, ITT CYBERSECURITY ANALYSTS



As portions of the Comprehensive National Cyber Security Initiative (CNCI) are released in the media as well as the Center for Strategic and International Study's (CSIS) commission report on "Securing Cyberspace for the 44th Presidency," it is clear cybersecurity is vital to our economic strength and that the government is designating cybersecurity as a top priority. "America's power, status, and security in the world depend in good measure upon its economic strength; our lack of cybersecurity is steadily eroding this advantage."[1]

But with so much of the nation's infrastructure in the hands of the private sector, it is equally imperative to motivate and educate this sector on the financial (and perhaps physical) risks associated with cyber security threats; and to promote public/private collaboration in defensive efforts. If U.S. enemies were to launch a denial of service attack against key data centers that renders the Internet useless even for just one day – what would that mean to us? How much revenue would be lost? How many large corporations would lose millions as their stock prices plummet? An already troubled U.S. economy would crumble. Fear is "the great motivator" and with recent headlines, studies and statistics showing the increase in cyber attacks and revealing U.S. vulnerabilities, the private sector should be shaking in their collective shoes.

Steven Chabinksy, deputy director for the Joint Interagency Cyber Task Force, Office of the Director of National Intelligence, stated the former president's initiatives represented an integrated portfolio that was unique – "it's the first attempt to implement a totality approach" to improve the nation's cyber security posture.[2] In essence, a comprehensive approach includes awareness of insider and outsider threats; education and training in response to those threats; near and far technology portfolio for dynamic defense; and successful public, private and academic partnerships.

Already utilizing a comprehensive approach and nestled in the foothills of the Adirondacks is a center of excellence composed of a coalition of cyber experts fighting against those who seek to attack our infrastructure with the Information Age's most sophisticated tools. As cyber threats to

[1] "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies (CSIS), December 2008

[2] "Details Emerge about President's Cyber Plan," Government Computer News, 11/21/08 http://www.gcn.com/online/vol1_no1/47639-1.html

our nation have grown exponentially in the past years, the need for trained personnel to address these threats has also grown in significant proportions. In response to this need for a highly-qualified workforce, affiliates of the cyber coalition have played a supportive role to a program that is specifically designed to train and educate ROTC cadets in cyber defense. This program, initiated by the National Science Foundation and presently funded by the U.S. Air Force is known as the Advanced Course in Engineering (ACE), described in the Congressional Research Service's (CRS) report, "as an attempt to attract, train, and retain skilled information technology professionals,"[3] and further described by Brigadier General Mark Schissler as "building new cyber operators through their Cyber Boot Camp program bringing in the brightest of our ROTC cadets to learn advanced network operations and cyberspace operations techniques."[4]

Supported in conjunction with the ACE program but open to civilians is ITT's Embedded Intern Program, which provides a unique opportunity for high school, undergraduate and graduate students to gain hands-on experience in the field of cybersecurity at various law enforcement agencies nationwide. The foundation of this program is a joint venture between academia and the public and private sectors in an effort to expose students to a challenging experience in support of cybersecurity developments. Both emanate the innovative approach needed to address the education and training requirements outlined in the CNCI and the CSIS commission report and assist in developing a critical talent pool in information assurance and cyber defense.

Recruiting talented and skilled individuals is the task at hand but an increased investment in training and education for the practicing public sector will assist in the prosecution and adjudication of cybercrime as well. ITT's cybersecurity training vehicles include seminars, workshops, expos and webinars for first responders, investigators, forensic examiners, prosecutors, judges and corrections personnel – both domestic and international. Training and education on topics such as securing digital evidence, data hiding, phishing, technology exploitation, wired and wireless network security, and online fraud prevention and detection strengthen the public sector's capacity to combat cybercrime.

Another example of using an innovative approach to address the cyber threat involves a new twist on an old method. Throughout the Cold War, an era defined by the threat of nuclear annihilation, Western nations attempted to prepare civilian populations for atomic attack through staged drills, evacuations, field exercises and all things necessary to ensure survival of a physical war. Today's exercises now must address our 21st century fears that include our nation's survival of a cyber war. The solution involves the preparation and production of customized tabletop cyber exercises. The exercises are composed of mock incidents involving some type of cybersecurity breach or vulnerability; public and private stakeholders are tasked with solving the who, what, why and how of the incident. This method encourages the collaboration of law enforcement, government and those from the public and private sectors and it shows promise as one of the most effective ways of reaching and teaching stakeholders to prepare for such an event. The knowledge gained by

[3] "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues," Congressional Research Service (CRS) Report for Congress, Updated March 20, 2007
[4] "Questions and Answers with Brigadier General Mark Schissler, Director for Cyber Operations," CyberPro Special Edition 1, December 24, 2008, National Security Cyberspace Institute (NSCI)

participants throughout the exercise often propels them to leave with a central focus – secure their business infrastructure and develop an enterprise protection plan immediately.

As a result, tabletop exercises not only address incident response and enterprise security but promote the opportunity to make critical stakeholders aware of the tools and technologies that are available for transition. An effective technology transition agent will establish a practical, yet comprehensive, approach to this process, composed of the following steps: research, acquisition, testing and evaluation, deployment and transfer of feedback.[5] By transitioning technologies to those tasked with protecting critical infrastructure, the agent is able to provide operational feedback to technology developers, expose end-users to cutting-edge tools, and better match future investments from technology sponsors with cybersecurity requirements.[6]

Fostering the development of a highly-qualified workforce to meet the public and private sector needs of information assurance and cyber defense; creating awareness by educating and motivating key stakeholders; and transitioning technology to appropriate end-users within the cybersecurity industry are a direct result of effective collaboration. A center of excellence is defined "as a place where the highest standards of achievement are aimed for in a particular sphere of activity."[7] Upstate New York's center of excellence in cybersecurity is uniquely positioned and has the capability to bring subject matter experts, research and development, and cutting-edge technology to the forefront of our nation's cyber defense. ITT's cybersecurity initiatives and efforts can be directly correlated with the new U.S. administration's key areas of improvement. "Working with private industry, the research community and U.S. citizens, the government is aiming to 'lead an effort to build a trustworthy and accountable cyber infrastructure that is resilient, protects America's competitive advantage, and advances our national and homeland security'."[8]

[5] Salvatore C. Paladino and Jason E. Fingerman, "Cybersecurity Technology Transition: A Practical Approach," December 2008
[6] Ibid
[7] http://encarta.msn.com/dictionary_1861694214/center_of_excellence.html
[8] "Obama Outlines Key Security Tasks, is Barred from Facebook by White House Security Team," SC Magazine, January 27, 2009, http://www.scmagazineuk.com/Obama-outlines-key-security-tasks/article/126414/