THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 9 NUMBER 7

JANUARY 2011

CYBERSECURITY

Contact: dhardy1@gmu.edu
703.993.8591

Click **here** to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

This month's issue of *The CIP Report* highlights the efforts that have been undertaken by the public and private sectors, as well as academia, in the current and expanding field of cybersecurity.

First, the Institute for Infrastructure and Information Assurance (IIIA) at James Madison University (JMU) provides an overview of the events that shaped cybersecurity in 2010. The United States Cyber Command (USCYBERCOM), established in 2009, describes its mission and collaborative efforts to defend against cyber threats. The U.S. Department of Transportation's (DOT) Volpe National Transportation Systems Center discusses its support of the U.S. Department of Homeland Security's (DHS) National Cyber Security Division's Control Systems Security Program (CSSP) to conduct cyber security activities in all modes of transportation. Then, the Director of the National Security and Emergency Preparedness Department at the U.S. Chamber of Commerce elucidates upon the benefits of smart cybersecurity in business and household communities in the United States. Next, the Senior Advisor of Cyber Operations and Transformation and the Deputy Director of the Cyber and Information Operations Directorate at Headquarters U.S. Air Force (HQ USAF) illustrate the importance of the public and private sector collaboration framework. Finally, we announce two cyber workshops that will be co-hosted by the Center for Infrastructure Protection and Homeland Security (CIP/HS) and held on the George Mason University Arlington Campus in June 2011.

This month's *Legal Insights* examines the legal frameworks that are involved when cyber incidents threaten national and international security. We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Cybersecurity: Congressional Action, Public-Private Partnerships, and Education are Key to Mitigating Vulnerabilities

by Benjamin T. Delp, Associate Director of Research Development,
Sami Nuristani, Graduate Fellow, and
Blake Mitchell, Research Assistant,
Institute for Infrastructure and Information Assurance, James Madison University

Secure networks. Without them, business as usual in the United States ceases to exist. Take a moment to think about how much time a typical day depends on infrastructure linked with cyber networks: from heating up water for a shower, to flicking on the light switch when rolling out of bed, to powering on the coffee maker for a morning cup of Joe. These many routine conveniences of American life are often taken for granted. According to the Federal Bureau of Investigation (FBI) Deputy Assistant Director Steven Chabinsky, these same systems and networks, "... offer the chance of a lifetime to cheat, steal, and strike from afar with little money, covered tracks, and enormous real world impact for sophisticated criminals, terrorists, warmongers, and spies."[1]

Cybersecurity is expected to garner broad bipartisan support in the 112th U.S. Congress, as policy-makers recognize the importance of securing the networks and systems that support U.S. critical infrastructure and key resources, as defined by the National Infrastructure Protection Plan. However, instead of focusing on the outlook for 2011, this article will review how 2010 shaped the current cybersecurity landscape by examining legislative initiatives, threats, and recommendations with an emphasis on reports and events of the past year.

Congressional Action

In February 2010, the House passed the Cybersecurity Enhancement Act, which included provisions to:

- Help the Federal government develop a skilled cybersecurity workforce.
- Coordinate and prioritize Federal cybersecurity research and development.
- Improve the transfer of cybersecurity technologies to the marketplace.
- Promote cybersecurity education and awareness for the public.[2]

At a cost of $639 million from Fiscal Year (FY) 2010-2014 and $320 million thereafter, many would argue that this is a wise investment to ensure the safe, reliable functioning of the $14 trillion-plus U.S. economy. However, this piece of legislation has sat idly in committee since February.

At the time of this article, both the House and Senate included cybersecurity legislation in their chamber-specific versions of the National Defense Authorization Act.[3] On the House-side, cybersecurity provisions would, "… require government agencies to move to continuous IT security monitoring and the creation of a Senate-confirmed, White House cybersecurity director," while the Senate's version would "... require the Department of Defense (DoD) to report to Congress on cyberwarfare policy that includes a review of legal, strategy, and doctrinal issues; fund cybersecurity demonstration projects using commercial technology; develop a tailored acquisition process for cyberspace; and create a strategy to address software vulnerabilities and

(Continued on Page 3)

[1] Steven Chabinsky, "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line," *Journal of National Security Law and Policy*, 4 (2010), 27.
[2] Eric Chabrow, "House passes Cybersecurity Enhancement Act Measure, Approved by 422-5 Vote, Goes to the Senate (2010)." *GovInfoSecurity*, February 4. Accessed February 9, 2010, http://www.govinfosecurity.com/articles.php?art_id=2166.
[3] Ibid.

Year in Review *(Cont. from 2)*

supply-chain risk management strategies."[4] If these measures do not pass in the final version of the National Defense Authorization Act, it will be the responsibility of the incoming Congress to minimize threats by addressing the above essential components.

Threats and Vulnerabilities

As U.S. manufacturing heads overseas, one threat to cyber systems becomes real even before a computer is powered on. As one expert explains, "[s]traight out of the box, our computers (or the architecture they ride on) can be poisoned with dormant capabilities … our technology systems can come out of the factory in pristine condition, only to be manipulated by the delivery service, the wholesaler, the retailer, the installer, the repairman, or through the downloadable firmware update or patch."[5] The complex vulnerabilities existing within the supply chain of IT infrastructure will require an interdisciplinary approach by agencies and human resources.

In the 21st century threat environment, governments and companies assess risks not only outside their organizations, but also within. An incident involving disgruntled San Francisco IT engineer Terry Childs, who essentially shut down the government by locking San Francisco departments and agencies out of the city's wide area network in the summer of 2008, put the spotlight on insider access. Insider access "… provides a distinct perspective on a company's security weaknesses, including technical gaps, lapses in policy enforcement, knowledge of where the crown jewels are located, and even vacation schedules of security staff."[6] How do organizations address the threat of insider access? Is it through rigorous background checks and employee screening of IT staff with network-wide access? Is the answer robust education and awareness programs, along with information sharing strategies within the technology policies of an organization? This article addresses these questions.

Public-Private Partnerships

Focusing on a nation-state, the 2010 Report to Congress of the U.S.-China Economic and Security Review Commission identified a host of incidents and threats originating in China. One of the more high profile of these incidents culminated in a cyber attack targeting Google's operations in China. Lasting from December 2009 to January 2010, the attack, referred to as "Operation Aurora," resulted in Intellectual Property theft, specifically Google's invaluable source code.[7] As a direct response to the intrusion, *The Washington Post* reported an agreement between the National Security Agency (NSA) and Google, "… allow[ing] the two organizations to share critical information without violating Google's policies or laws that protect the privacy of Americans' online communications."[8] The focus of the initiative is less on cyber forensics (identifying the perpetrator), than on information assurance (managing the risks associated with the operation of Google's networks).

While details of partnerships like the above-mentioned are rarely released to the public, NSA and Google's public-private partnership may serve as a model for other U.S. companies, and some steps have already been taken in the right direction. One such example is Perfect Citizen, a program that enlists the expertise of NSA, "… to detect cyber assaults on private companies and government agencies running such critical infrastructure as the electricity grid and nuclear-power plants."[9] In particular, Perfect Citizen will focus on older networks that are

(Continued on Page 4)

[4] Ibid.
[5] Steven Chabinsky, "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line," *Journal of National Security Law and Policy*, 4 (2010), 32.
[6] Steven Chabinsky, "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line," *Journal of National Security Law and Policy*, 4 (2010), 34.
[7] U.S. Congress, U.S.-China Economic and Security Review Commission. *2010 Report to Congress*, 111th Congress 2nd session.
[8] Ellen Nakishima, "Google to Enlist NSA to help it ward off Cyberattacks," *The Washington Post* (2010), February 4. Accessed February 9, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html.
[9] Siobhan Gorman, "U.S. Plans Cyber Shield for Utilities, Companies." (2010), *Wall Street Journal*, July 6. Accessed December 4, 2010, http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html.

Year in Review *(Cont. from 3)*

susceptible to online threats. The Comprehensive National Cybersecurity Initiative, implemented by President George W. Bush's administration and continued under President Barack Obama, will provide funds for the program.[10]

Given that 85 percent of critical infrastructure is owned and operated by the private sector, the importance of public-private partnerships cannot be overstated. The U.S Department of Homeland Security (DHS) followed this line of thinking in preparation for Cyber Storm III, a tabletop exercise completed in October 2010. The purpose of the third, biannual war game was to test the National Cyber Incident Response Plan. The event included participation from 60 companies, 13 countries, 11 States, and seven Cabinet-level agencies. Focusing on information sharing and decision-making, "... the exercise had been designed to test how well and how quickly government agencies could declassify information so that it could be shared with private-sector companies that own and operate the infrastructure on which the Internet and other computer networks run."[11]

However, when government agencies, in particular Intelligence Community agencies, collaborate with private business, rigorous oversight is necessary to ensure a balance is struck between privacy and national security interests. This is especially important when considering the U.S. electrical grid, which has been described as the most complex, interconnected network on the planet. A report published last summer by the North American Electric Reliability Corporation, "High-Impact, Low-Frequency Risk to the North American Bulk Power System," named cyber attacks, pandemics, and electromagnetic disturbances as the three greatest threats to the power grid. According to the report, "[t]he threat of a coordinated cyber attack, which might be combined with a physical attack, is considered the first of the top three 'high-impact, low-frequency' threats to [the] North American electricity supply."[12] Additionally, similar to computers and computing software, many of the components of the grid are no longer manufactured in the United States.[13] This problem is highlighted in a 2010 study by the Idaho National Laboratory which references reports from earlier in the year, accusing Russia and China of embedding malicious software in the grid as early as 2006.[14] To put this in financial perspective, over the course of a year the grid is down, on average, 0.03 percent of the time, costing the U.S. economy $150 billion.[15] Providing the Department of Energy (DOE) with the necessary resources to protect the currently structured grid, and design the smart grid of the future with security in mind is a cost with perhaps no greater benefit than determining critical infrastructure protection strategies.

Education and Public Awareness

Cybersecurity vulnerabilities can be mitigated by supporting education, both to train those charged with protecting networks and to better inform the public. If passed, the Cybersecurity Enhancement Act would fund the Scholarship for Service program, providing colleges and universities with resources for students studying information assurance and computer security.[16] Such a program could complement the NSA's Centers of Academic Excellence in Information Assurance Education program. Accompanying educational efforts, the White House's strategy to

(Continued on Page 18)

[10] Ibid.

[11] Shaun Waterman, "Cyber Storm III Aims to Protect Against Real Thing." (2010), *The Washington Times*, September 28. Accessed December 1, 2010, http://www.washingtontimes.com/news/2010/sep/28/cyber-storm-iii-aims-protect-against-real-thing/.

[12] llen Messmer, "Cyberattacks: Top Threat to Zap U.S. Power Grid." (2010), *Network World*, June 2. Accessed June 3, 2010, http://www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html.

[13] Ibid.

[14] Siobhan Gorman, "U.S. Plans Cyber Shield for Utilities, Companies." (2010), *Wall Street Journal*, July 6. Accessed December 4, 2010, http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html.

[15] David Fessler, "America's Electric Grid: Three Companies Upgrading this Aging Infrastructure," (2010) *Investment U*, May 17. Accessed December 4, http://www.investmentu.com/2010/May/americas-electric-grid.html.

[16] Eric Chabrow, "House passes Cybersecurity Enhancement Act Measure, Approved by 422-5 Vote, Goes to the Senate (2010)." *GovInfoSecurity*, February 4. Accessed February 9, 2010, http://www.govinfosecurity.com/articles.php?art_id=2166.

United States Cyber Command

by CAPT Gina Cairns-McFeeters, U.S. Navy
Strategic Communication/U.S. Cyber Command

Background

In May 2009, President Obama stated that U.S. digital infrastructure is a strategic national asset and its protection is a national security priority. Reflecting the increasing importance of cyberspace regarding national defense, Secretary of Defense Robert Gates announced on June 23, 2009 the establishment of a Subordinate Unified Command under United States Strategic Command (USSTRATCOM) for Military Cyberspace Operations, United States Cyber Command (USCYBERCOM).

USCYBERCOM was formed by combining two USSTRATCOM entities, the Joint Functional Component Command for Network Warfare and the Joint Task Force for Global Network Operations. Initial operational capability was reached on May 21, 2010 and Deputy Secretary of Defense William Lynn declared full operational capability in a memorandum dated October 31, 2010. USCYBERCOM will be a focal point for DoD cyber-related issues and will synchronize planning efforts to direct the operation and defense of military information networks. Its current efforts include:

- Unifying efforts in military cyberspace operations
- Strengthening DoD cyberspace capabilities
- Sustaining network operations
- Integrating and bolstering DoD cyber expertise
- Enhancing mission effectiveness through partnerships with other agencies and governments

USCYBERCOM will be one of DoD's key organizations working as part of a whole-of-government approach that will deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks. Due to the magnitude of threats and the increased sophistication of cyber capabilities, a conscious decision was made to establish USCYBERCOM in order to defend DoD's information networks. In order to strengthen its capabilities in cyberspace, DoD has incorporated the following steps into the 2010 Quadrennial Defense Review:

- Develop a more comprehensive approach to DoD operations in cyberspace
- Develop greater cyberspace expertise and awareness
- Centralize command of cyberspace operations
- Enhance partnerships with other agencies and governments

USCYBERCOM Facts

Headquartered at Fort Meade, Maryland, under the command of GEN Keith Alexander (also Director of the National Security Agency), USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the DoD information networks. It is prepared to conduct full spectrum cyberspace operations (in accordance with all applicable laws, regulations, and Executive Orders governing military planning and operations) when directed to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries. The different Service Cyber Components consist of:[1]

- USA-Army Cyber Command

(Continued on Page 6)

[1] In addition, the United States Coast Guard, under the Department of Homeland Security, assists USCYBERCOM.

USCYBERCOM *(Cont. from 5)*

- USAF-24 Air Force/Air Force Cyber Command
- USN-Navy Fleet Cyber Command
- USMC-Marine Forces Cyber Command

DHS and DoD Partnership

USCYBERCOM is a key part of DoD's efforts to integrate its cyber missions in order to better share information and to more effectively support other stakeholders. Today's global society depends on cyberspace to facilitate commerce, trade, government services, communications, diplomatic exchanges, critical infrastructure support, as well as a multitude of other services. DHS will lead efforts in securing non-military networks and USCYBERCOM will provide support and technical assistance when, and as requested and directed.

In September 2010, Secretary of Defense Gates and DHS Secretary Janet Napolitano signed a Memorandum of Agreement to increase interdepartmental collaboration in strategic planning for the Nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities. A DHS - DoD Joint Coordination Element will be led by a senior DHS official at Fort Meade, Maryland. This official will serve concurrently as a senior liaison to USCYBERCOM and to the National Security Agency. In exchange, DoD will place a Cyber Support Element and a Cryptologic Services Group representative at DHS's National Cybersecurity and Communications Integration Center. These efforts will promote joint planning and provide enhanced support. This cybersecurity partnership was formalized in order to:

- Focus national cybersecurity efforts
- Increase the overall capacity and capability of both the DHS homeland defense and the DoD's national security missions
- Continue to provide integral protection for privacy, civil rights and liberties

The DHS and DoD cybersecurity agreement will further align and enhance America's capabilities to protect against threats to our critical civilian and military computer systems and networks.

Cyber Threat Environment

Malicious cyber activity results in billions of lost revenue, to include the corruption and possible disruption of sensitive data and intellectual property. It can also significantly impact and destroy some of the U.S. critical infrastructures that depend upon the Internet.

Not only is the U.S. civilian sector dependent upon cyberspace, DoD is increasingly dependent on cyberspace to support and conduct critical joint military operations. Cyberspace is unique because it is a man-made domain. This strategically and operationally critical domain, on par with sea, land, air and space, is being contested at an unprecedented rate. Due to the nature of the cyber domain, DoD must be able to quickly and effectively operate in cyberspace and defend against a growing array of threats that include, nation-state actors (or state sponsored actors) and non-nation state actors (terrorists, cyber criminal groups, and hackers) who seek to exploit, disrupt, or even destroy vital U.S. networks. These actors work tirelessly to degrade the security and stability of our networks. The low cost of sophisticated cyber capabilities means adversaries can more easily target and victimize millions of users and Internet service providers. These inexpensive cyber capabilities and methods expose our critical infrastructure to an unprecedented level of risk. Cyber threats are becoming more sophisticated, coordinated, and potentially damaging. The convergence of data in cyberspace also presents new challenges because more users of more services are on the same network. Vulnerability on one computer or network can lead to vulnerability on all. Cyber threats to DoD information networks are just as real and significant as physical threats — the challenge is immense. As stated in Deputy Secretary of Defense Lynn's September/October 2010 *Foreign Affairs* article, the department experienced an intrusion into its networks in 2008, which reinforced the cyber threat to the defense department and also marked a turning point in U.S. cyber defense. The DoD information networks

(Continued on Page 20)

DHS and The Volpe Center: Partnership for Cybersecurity in Transportation

by Michael Dinning, Rodney Cook, Kevin Harnett, and David Sawin,
Freight Logistics and Transportation Systems, Volpe National Transportation Systems Center

Cybersecurity is a growing concern to the transportation community, as E-enabled vehicles and net-centric systems are being introduced in nearly every mode of transportation. The national transportation system is becoming increasingly dependent on these information technologies, which may introduce new vulnerabilities to cyber attacks. The U.S. Department of Transportation's (DOT) Volpe National Transportation Systems Center is working with the DOT modal administrations, the Transportation Security Administration (TSA), DoD, DHS, and industry and academia to address these concerns.

The Volpe Center is supporting the DHS National Cyber Security Division's Control Systems Security Program (CSSP) to conduct cybersecurity activities in all modes of transportation. Anticipated activities include: identifying and assessing the vulnerabilities of major U.S. transportation control systems; preparing a Transportation Control System Cybersecurity Roadmap with information on how to enhance the security of these systems; creating a cyber laboratory for testing and validating cybersecurity measures; supporting development of transportation-based scenarios for use in national-level cyber exercises; providing outreach, awareness, and educational support, and enhanced professional capacity building focused on control systems; and expanding collaborative cybersecurity efforts with other U.S. and international members of the transportation community.

There is increasing concern over the potential cybersecurity vulnerabilities created by technologies such as open standard Internet communication protocols and commercial-off-the-shelf (COTS) equipment in new "E-enabled" aircraft. To assist in understanding and responding to this issue, the Federal Aviation Administration (FAA) and DoD asked the Volpe Center for assistance. In response, the Volpe Center developed the Airborne Network Security Simulator (ANSS) at Wichita State University (WSU) in Kansas. ANSS integrates commercial and military aeronautical simulators to provide a controlled test bed to identify security threats in airborne network environments. It is used to test, evaluate, and calibrate aviation systems and equipment; assess their potential weaknesses and vulnerabilities in a safe environment; and develop new and upgraded industry and regulatory policies and standards to address aviation security issues. The Volpe Center hosted the first ANSS Demonstration and Technical Workshop at WSU in Wichita, KS in June 2010. The demonstration was attended by over 70 participants from both the military and commercial aviation communities, including the Defense Information Systems Agency; the United Kingdom Communications Electronic Security Group; DHS; airlines; aircraft, engine and avionics manufacturers; IT companies; and universities. The Volpe Center/WSU demonstration included a security test of a Class 3 Electronic Flight Bag and the wireless connection used to distribute flight plan and performance information from an airline.

The Volpe Center is also working with TSA, DHS, and others to conduct outreach activities designed to increase the awareness of cybersecurity issues. The Volpe Center participated in the recent TSA Transportation Cyber Security Summit meeting, and will be involved in sessions focused on cybersecurity in the upcoming Transportation Research Board Annual Meeting. Additional communications, outreach, and professional capacity building activities are being planned. The Volpe Center advocates using an all hazards approach to maximize safety, security, and resilience in transportation. The Volpe Center's

(Continued on Page 18)

Smart Cybersecurity Is Good for Business and the Nation

by Matthew J. Eggers, Director
National Security and Emergency Preparedness Department, U.S. Chamber of Commerce

This article is adapted from the Chamber's Internet Security Essentials for Business *guidebook, which was released on October 26, 2010. The guidebook is available in PDF at www.uschamber.com/cybersecurity.*

Several U.S. presidents have said that protecting our Nation's digital infrastructure is a top economic and national security issue. While extensive public and private sector efforts have been underway for many years, in May 2009, President Obama articulated the need for wider public participation in protecting America's communication and IT infrastructure, or cyberspace. He called for a national public awareness and education initiative to promote Internet security. "It's the great irony of our Information Age — the very technologies that empower us to create and to build also empower those who would disrupt and destroy," the president said.[1]

The strength of our free enterprise system is directly linked to the prosperity and security of our interconnected world. According to U.S. Department of Commerce Secretary Gary Locke, the Internet is responsible for about $10 trillion in annual online transactions and is a bulwark of the global economy. This hefty figure is almost guaranteed to grow.[2] Businesses and households conduct an increasing amount of their daily activities — from paying bills to shopping to texting friends and communicating with colleagues — online. The new National Broadband Plan estimates that 97 percent of small businesses use e-mail and 74 percent have a company website.[3] Small businesses, which make up more than 99 percent of all businesses in the United States, play a critical role in enhancing our country's Internet security. They employ about half of all private sector workers and have been responsible for more than 60 percent of net new jobs over the past decade.[4]

Smart cybersecurity practices have positive implications for strong U.S. communities and national competitiveness. By managing their companies' cybersecurity, owners and managers not only help protect their crucial business and customer information but also help protect the Internet. Digital devices are so common in our daily lives that we often take them for granted, and yet sound day-to-day Internet security practices are much less ubiquitous.

However, there is some good news. A May 2010 poll conducted by the National Cyber Security Alliance and the Anti-Phishing Working Group, two leading Internet security education and awareness organizations, found that the vast majority of Americans are willing to practice good Internet safety and security habits given the right resources. Americans feel that doing their part to help keep the Internet safe benefits their homes and businesses as well as our national and economic security.[5]

(Continued on Page 9)

[1] President Barack Obama, "Remarks by the President in Securing Our Nation's Cyber Infrastructure," May 29, 2009, www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

[2] U.S. Department of Commerce Secretary Gary Locke, "Remarks at Cybersecurity Policy Review Meeting," July 14, 2010, at www.commerce.gov/news/secretary-speeches/2010/07/14/remarks-cybersecurity-policy-review-meeting; see International Telecommunication Union statistics at www.itu.int/ITU-D/ict/statistics/index.html.

[3] Federal Communications Commission, *Connecting America: The National Broadband Plan* (2010); see www.broadband.gov/plan/3-current-state-of-the-ecosystem, or http://download.broadband.gov/plan/national-broadband-plan-chapter-3-current-state-of-the-broadband-ecosystem.pdf.

[4] U.S. Small Business Administration, "Frequently Asked Questions," http://web.sba.gov/faqs/faqindex.cfm?areaID=24.

[5] See August 10, 2010, press release by the National Cyber Security Alliance and the Anti-Phishing Working Group. The release is available at http://staysafeonline.mediaroom.com/index.php?s=43&item=62. The poll was conducted as part of a public-private national messaging convention to promote cybersecurity awareness among members of the general public.

Smart Security *(Cont. from 8)*

Over the past two years, the U.S. Chamber of Commerce, in cooperation with DHS, has been visiting cities around the country to increase businesses' awareness about the need for greater cybersecurity and to educate them about tools that are readily available to manage online risks.

As many readers of *The CIP Report* are aware, research suggests that roughly 85 percent of security breaches are avoidable through simple and reasonable measures.[6] The U.S. Chamber recently released guidebook, *Internet Security Essentials for Business* (see Figure 1), with practical steps that small businesses can take to secure their information assets. The Chamber urges businesses to adopt Internet security fundamentals to reduce network weaknesses to make the price of success more difficult for cyber criminals and other virtual bad guys. The networked nature of our online systems means that defensive measures are only as good as their weakest link. So protection, therefore, is paramount.

The cybersecurity guide outlines a dozen recommendations and bundles them into three categories: workforce, policies and problems, and prevention and preparedness. Business owners and managers are urged to stress workforce education, such as pressing employees to use strong passwords for their digital devices and helping them spot e-mail scams. Businesses should also organize the information they keep, know where it is stored, and prioritize it by level of importance. In case of a cyber incident, businesses should have a plan in place to help speed recovery and prevent future incidents. *Internet Security Essentials for Businesses* emphasizes the following points:

- Businesses need to understand common online risks that may lead them to become victims of cybercrime. This guide is ultimately about business preparedness and resilience.

- Perfect online security is unattainable, even for large businesses. But there are inexpensive practices that can be implemented to improve the security of your information, computers, and networks.

- Businesses need to know how and to whom to report cyber incidents and online crime.

- Cybersecurity is a team sport. Taking the actions recommended in this guide will have positive consequences for the security of

(Continued on Page 10)

Internet Security Fundamentals

Workforce
- Educate your workforce
- Designate a person to handle security and preparedness
- Use strong passwords
- Control network access

Policies and Problems
- Indentify and prioritize your business' information
- Defend company computers
- Dispose of media safely and securely
- Have a plan to address cyber incidents

Prevention and Preparedness
- Defend your data on the go
- Encrypt business sensitive information
- Back up your data regularly
- Participate in National Cybersecurity Awareness Month

To download *Internet Security Essentials for Business* in PDF as well as additional online safety and security materials for free, go to www.uschamber.com/cybersecurity.

Figure 1.

[6] See, for example, Verizon Business RISK Team's 2008, 2009, and 2010 data breach investigation reports, which can be accessed, respectively, at www.verizonbusiness.com/resources/security/databreachreport.pdf, www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf, and www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf.

Smart Security *(Cont. from 9)*

businesses, communities, and the country. The interconnectedness of computers and networks in cyberspace means that the public and private sectors share responsibility in raising their game. U.S. competitiveness and security depend on it.

Cybercrime Is on the Rise

At a congressional hearing, a cybersecurity expert gave an account of a small wooden furniture company that had been successfully hacked, resulting in the loss of data containing its valued designs. The witness suggested that the alleged offender(s) was able to commandeer the company's intellectual property to rush new furniture to the market and at cheaper prices.

The thieves did not need to physically break into the company — that would be too risky and unnecessary. All they needed to do was steal the data with a few key strokes. How pervasive are cyber intrusions like this one, the witness asked rhetorically, if bad actors are hacking into the information system of a seemingly innocuous, small business for commercial gain?[7] The Obama administration's Cyberspace Policy Review suggests that losses from intellectual property theft were as high as $1 trillion in 2008, a staggering figure.[8]

A Snapshot of Cybercrime in America[10]

Year	Complaints Received	Dollar Loss (in millions)
2009	336,655	$559.7
2008	275,284	$264.6
2007	206,884	$239.1
2006	207,492	$198.4
2005	231,493	$183.1
2004	207,449	$68.1
2003	124,515	$125.6
2002	75,064	$54.0
2001	50,412	$17.8

Figure 2.

Cybercrime in the United States is growing rapidly in scope and sophistication. While it is difficult to get a complete picture of the entire problem, organizations such as the Internet Crime Complaint Center (IC3), a joint operation between the FBI and the National White Collar Crime Center, provides a window into a growing trend.

According to the IC3's 2009 Internet Crime Report, annual crime complaints reported to IC3 have increased nearly 668 percent when compared with data from its 2001 annual report. Complaint submissions for 2009 were 336,655, a 22 percent increase from 275,284 in 2008, and a 63 percent increase from 206,884 complaints in 2007. Yet research indicates that only one in seven incidents of fraud ever make its way to the attention of enforcement or regulatory agencies. The dollar loss from all cases of crime referred to law enforcement totaled $559.7 million, a 112 percent increase from $264.6 million in 2008 (see Figure 2).[9]

Anyone who uses the Internet is susceptible to offenses such as credit card fraud or the theft of intellectual

(Continued on Page 11)

[7] Example of the wood furniture company provided by Dr. James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies. See his testimony from a February 23, 2010, Senate hearing on cybersecurity and critical infrastructure, available at http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=a676548f-a2a7-40ff-a18d-889a7907801c&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=2&YearDisplay=2010. Also, in the September/October 2010 issue of *Foreign Affairs*, a top Pentagon official writes that while "the threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyberthreat that the United States will face over the long term" (p. 100); see also, www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

[8] See Cyberspace Policy Review, p. 2.

[9] Internet Crime Complaint Center (IC3), 2009 Internet Crime Report; see March 12, 2010, IC3 press release and report, respectively, at www.ic3.gov/media/2010/100312.aspx; www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

[10] Ibid.

Smart Security *(Cont. from 10)*

property. The cost of attack is relatively low for criminals, and the payoff is high. The goal for business owners and managers is to raise the sophistication of their cybersecurity practices to increase the price of success for their adversaries.

Critical Infrastructures Play Key Role

The Chamber's Internet security guide focuses on small businesses, which help drive the U.S. economy. For a complete picture, it is important to take a step back and look at the digital ecosystem from a national perspective, which involves larger businesses, entire sectors, and government players. Too often, the media focus on negative stories — the proverbial car crash during rush hour — to the exclusion of what is positive. Such stories form a significant part of raising public awareness. However, they can easily overlook much of the positive work that various sectors of the economy are undertaking to enhance the computer and network security of the Nation's critical infrastructure (See Figure 3).

In addition to its educational components, the guide includes brief highlights of initiatives being undertaken by the 18 critical sectors — the Banking and Financial Services, Chemical, Communications, Electric, and Information Technology Sectors

(Continued on Page 18)

Cyber Incident and Complaint Reporting Organizations

OnGuard Online (www.onguardonline.gov; www.alertaenlinea.gov in Spanish)
OnGuard Online offers practical tips on how to protect yourself against Internet fraud, secure your computers, and guard personal information. The site is sponsored by both government, with FTC in the lead, and private sector entities.

File a complaint with OnGuard Online at www.onguardonline.gov/file-complaint.aspx.

Internet Crime Complaint Center (IC3) (www.ic3.gov)
IC3 was established to receive Internet-related criminal complaints and to research, develop, and refer the criminal complaints to federal, state, local, international law enforcement, or regulatory agencies for further investigation. Since its inception, IC3, a partnership between the FBI and the National White Collar Crime Center (NW3C), has received complaints crossing the spectrum of cybercrime matters, including IP rights matters, computer intrusions (hacking), economic espionage (theft of trade secrets), online extortion, international money laundering, identity theft, and a growing list of Internet-facilitated crimes.

File a complaint with IC3 at www.ic3.gov/complaint/default.aspx.

United States Computer Emergency Readiness Team (US-CERT) (www.us-cert.gov)
US-CERT is the operational arm of the Department of Homeland Security's (DHS's) National Cyber Security Division (NCSD), which leads a public-private partnership to protect and defend the nation's cyber infrastructure. Partners include industry, academia, federal agencies, information sharing and analysis centers, state and local governments, and international organizations. NCSD was established by DHS to serve as the federal government's cornerstone for cybersecurity coordination and preparedness.

File an incident report with US-CERT at https://forms.us-cert.gov/report.

Figure 3.

The Public and Private Sector Collaboration Framework — A Policy-Neutral Solution to Cyber Security Challenges

by Riley Repko, Senior Advisor, Cyber Operations and Transformation, HQ USAF, and
John Toomer, Deputy Director, Cyber and Information Operations Directorate, HQ USAF

When operating in the cyber domain, the partnership between the government and the private sector is absolutely essential. The nature of this domain, that of being "man-made," has at its core a strong majority of the intellectual capital owned and residing "globally" with the private sector. Government, for all its efforts, has neither the capacity nor the resources to be the leader in cyberspace security development. There exists in government a strategic paralysis and persistent skepticism surrounding a military or any government role in cybersecurity. However, this argument is not where we need to invest more discussion. Yes, this is all about policy, but where government lacks the ability to act, the private sector can be tapped to lead our public and private sector defense of cyberspace. This requires a collaborative framework whereby private sector innovation can be easily brought to bear against the Nation's cybersecurity needs absent strong national policy. This framework is flexible and tailorable to entities large or small, classified or unclassified, and agile enough to meet the threat at network speed. What is needed now is a commitment to this collaborative framework to begin solving our Nation's cyber awareness and implementation challenges.

Collaboration between the U.S. government and the private sector is certainly nothing new. Melissa Hathaway, of President Obama's Cyber Commission, has documented 55 government-initiated cybersecurity partnerships; 30 of these partnerships emitted solely from DHS. This does not include the countless existing bi-lateral and informal relationships. This is just a small sample of the potential cyber solutions landscape. Large Defense Industrial Base (DIB) integrators have the majority of these partnerships with government. But these partnerships exclude 95 percent of the small innovative firms currently occupying the cyber ecosystem. If only small businesses could believe that they will receive adequate priority and attention from the government in terms of time and resources. Barriers that prevent small businesses from being a part of this partnership are many (e.g., too compliance intensive, time-consuming bureaucratic processes, and lack of government awareness). The critical "hard-nut," trust, however, cannot imply that businesses of all sizes will not take on additional costs and legal risks involved in collaborating with government.

The push for collaborating with the private sector within the cyber domain has created a new framework mechanism of awareness. The "what is out there" question amongst both the private and public sectors and how service delivery will be performed is of immediate importance, especially to the military operator. The framework connects the skill-sets and capability awareness found in the private sector to the cybersecurity requirements found within both the private and public sector. The value of engaging the private sector for mutual problem solving and partnerships, in advance, is a non-standard approach but paramount to success within the cyber domain, especially to counter or reduce the impacts of a very clever adversary. If we do not have the capabilities awareness and their capacity in some sort of dynamic catalog, then the next time an adversary is cleverly nipping at one's heels, flip through the yellow pages to find that solution, in real time (while the clock is ticking). We must focus our situational awareness to manage our risk and have clarity to where our gaps and seams are within this cyber domain and we need this information in advance. We must tap into resources and expertise previously unavailable to us, with a focus and realization that this cyber domain is about a shared vision, with shared risk/responsibility, and frankly shared success. In fact, careful

(Continued on Page 13)

Public-Private Collaboration *(Cont. from 12)*

consideration needs to also be given to a shared investment. A trusted partnership moving forward must include the incentives for small businesses, as an example, to realize their intellectual property will not be lost or stolen and that their solution will be applied if and when needed. The framework referred to can take into consideration these qualifiers because the collaboration framework is "neutral." It is a clearinghouse with no stake in the game except for administering and fairly brokering government requirements with the situational awareness to the capabilities and their current capacity found within the private sector, globally.

The lack of transparency is one of the greatest hindrances to better public and private sector collaboration; it is also an old excuse. So what would be the fair and equitable solution, one that addresses the "hard-nuts," the political and bureaucratic impediments and also the critical stakeholders? Having a neutral "nexus," a not-for-profit, clearinghouse organization (Figure 1) fulfill this engagement role with the critical communities of interest is a recommended first-step.

The U.S. government does recognize that the economic and social well-being, national security, and defense are often dependent upon systems that are owned and operated outside the government. This priority therefore recognizes that the public sector and the private sector must collaborate to provide more secure products and services. For example, it recognizes that Internet service providers (ISPs), in particular, occupy a unique position at the gateway to access to the Internet and therefore need to be a key partner in the U.S. government's efforts to maximize cybersecurity.

We also recognize those vulnerabilities in critical infrastructure and other systems of national interest. These represent a greater level of risk to our national security than systems supporting broader online commerce and that a more intensive level of engagement is required between government and the owners and operators of these systems of national interest. We must therefore cover initiatives that enable the government to develop greater situational awareness of potential vulnerabilities in critical private sector networks, while also providing mechanisms for the government to provide tailored information and targeted assistance to the owners and operators of these networks for dealing with sophisticated cyber threats.

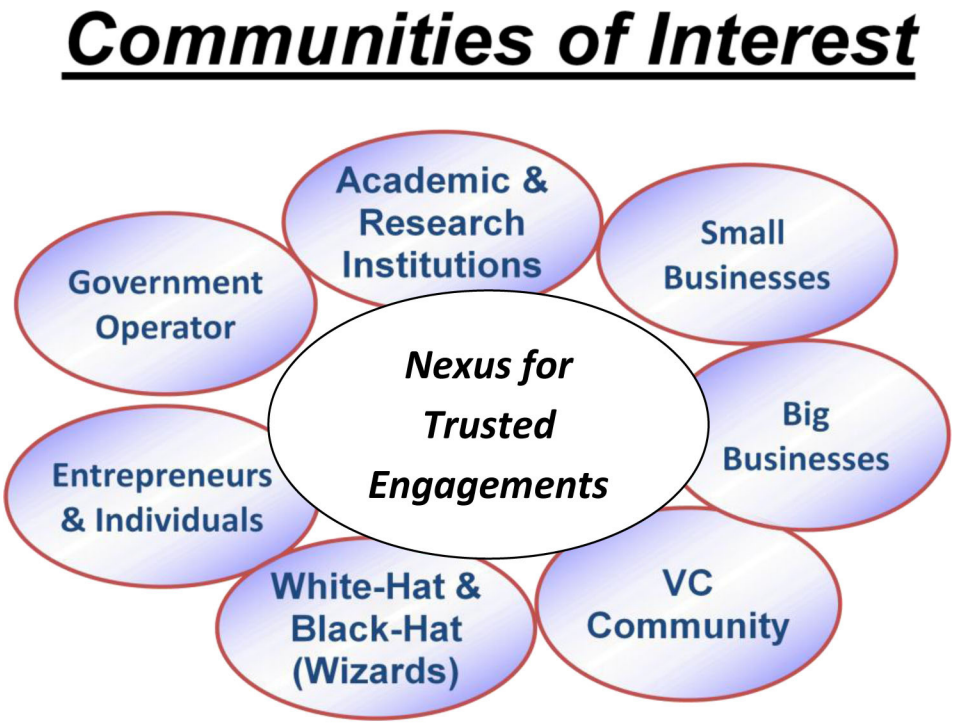

Figure 1

Summary

Everyone complains about the lack of awareness that exists (or not) in the cyber domain. It resides on both sides of the private-public sector transom. So, we should stop trying to take on this entire effort (boiling the ocean) and break-down the tasks required to develop such a collaboration framework into manageable tasks. The framework itself needs to be built. Then, the governance as well as the financial piece, which deserves solid consideration for being managed by the private sector through this new neutral organization, need to be

(Continued on Page 17)

CIP/HS to Host Cyber Economics Events in 2011

CIP/HS will host two workshops in the emerging field of cyber economics in June 2011. The Tenth Annual Workshop on Economics of Information Security (WEIS 2011) will be held from June 14 - 15. The first Annual Workshop on Cybersecurity Incentives (WoCI) will be held the following day on June 16. Both events will take place on George Mason University's Arlington Campus. WEIS will be co-hosted by the Interdisciplinary Center for Economics (ICES), led by Dr. Dan Houser, Chair of the Department of Economics at George Mason University. The Chair of the WEIS Program Committee is an internationally recognized security expert and author, Bruce Schneier. WoCI will be held in collaboration with Dan Arista of Syracuse Research Corporation (SRC).

Both events will focus on introducing interdisciplinary scholarship to the policy-makers, stakeholders, and decision-makers that will shape our cybersecurity policies and practices. Recent cyber incidents, such as the Stuxnet worm and the Wiki-leaks breach, demonstrate the challenge of cybersecurity across all levels of the Federal government and throughout the private sector. A consensus has emerged across the public and private sectors that existing approaches will not be able to keep pace with growing and evolving cyber threats, whether they are in the form of cyber conflict, espionage, vandalism, or crime.

To better secure cyberspace, it has long been noted that innovations in social, behavioral, and economic sciences will be just as critical as technical solutions. Such scholarship can better inform policy-makers seeking to craft new privacy rules and secure critical infrastructures. WEIS has been a leader in this area for a decade and CIP/HS is keen to host the annual workshop in close proximity to national policy-makers. WoCI represents an opportunity to leverage the work conducted at WEIS to more applied problems, including enterprise-level cybersecurity risk management. Each event targets a different stakeholder group. WEIS is primarily an academic conference in that it serves as a locus of the disparate disciplines with valuable insights into information security. WoCI will apply new and emerging concepts to real-world problems, addressing concerns of practitioners and stakeholders working in cyber fields.

WEIS is the leading forum for interdisciplinary scholarship on information security, combining and bringing to bare expertise from the fields of economics, social science, business, law, policy, and computer science. Prior workshops have explored the role of incentives between attackers and defenders, identified market failures dogging Internet security, and assessed investments in cyber-defense. This workshop will build on past efforts using empirical and analytic tools to not only understand threats, but also strengthen security through novel evaluations of available solutions. WEIS will bring together scholars in an attempt to answer the following questions:

- How should information risk be modeled given the constraints of rare incidence and high interdependence?
- How do individuals' and organizations' perceptions of privacy and security color their decision-making?
- How can we move towards a more secure information infrastructure and code base while accounting for the incentives of stakeholders?

WoCI, on the other hand, will discuss the past, present, and future of mechanisms and institutions to better incentivize behavior for security and explore cyber risk decision-making and the continuing competition between security and other priorities. Participants will present papers and engage in panel discussions in an attempt to determine best practices whether they currently apply in cyberspace or not. The agenda will focus on illustrating cyberspace as

(Continued on Page 17)

Legal Insights

When Cyber Incidents Threaten National or International Security: What is the Law?

by Maeve Dion, J.D.*

With society's ever-increasing reliance on the global information infrastructure, cybersecurity has become a significant aspect of national and international security. Governments, economies, and societies rely on the telecommunications and computer systems that make up this internationally-connected information infrastructure. Such dependence creates vulnerabilities when the information infrastructure becomes a target or field of conflict.

In the past several decades, governments have therefore broadened their traditional definitions of national security to incorporate protection of critical infrastructures, and particularly the computer systems of those critical infrastructures. However, given that telecommunications and information systems are connected globally, critical infrastructure protection may not be achieved from merely a national approach; it also requires international strategy and coordination.

The increasingly interconnected computer systems create the potential for a local event to cascade across geographical and sovereign borders. National security incidents in critical infrastructure computer systems may therefore have significant international components, requiring cooperation in efforts of prevention, mitigation, prosecution, reconstruction, and deterrence.

Most existing international legal frameworks, though, were established for incidents and crimes unrelated to the cyber context; they therefore may be inapplicable or inefficient to properly address and deter cyber incidents that threaten national or international security. For example, there is no explicit international law or structure that establishes minimum national cybersecurity and incident response efforts, or that mandates and coordinates global watch and warning capabilities.

However, some constructs in international law, which were not created for or written explicitly to include cyber incidents, may be applied in certain cyber contexts; applications of such law may help elucidate state obligations or expectations regarding cyber incidents that threaten national or international security.

One example is the concept in customary international law of the "duty of care," which roughly means that you should not use your property in a way that harms someone else. This concept has been upheld in international courts as binding on countries: a nation should not knowingly permit its territory to be used in a way that damages the rights of another country. Such an obligation may also imply a duty of prevention; this has been adopted in treaties and applied in disputes regarding environmental damage and state responsibilities.

Some other areas of law may also be applied to the international cyber security context, such as the law of armed conflict. However, there is still much debate on when and under what circumstances these existing laws may be applied, and just as much debate on the structure regarding "how" and "by whom" the laws may be enforced.

Of course, were counties to have explicit legal agreements regarding international cybersecurity, the obligations and expectations would be easier to understand and more commonly known. Perhaps the remedies and international enforcement structures would also be more clearly defined and accessible. Governments,

(Continued on Page 16)

Legal Insights *(Cont. from 15)*

individuals, and businesses alike may then be better able to predict the legal consequences of their actions.

Yet as history shows, it can be quite difficult — politically, socially, and legally — to reach international consensus broadly enough to write such explicit obligations and liabilities into documents such as treaties or multilateral agreements.

Nevertheless, the call for more clarity of international law in this field has been echoing around the world (see below).

An American Bar Association report noted that "the single greatest difficulty encountered thus far in the development of a legal response [to the national security cyber

(Continued on Page 19)

In mid-2008, the Organisation for Economic Co-Operation and Development (OECD) recommended that member countries conduct a systematic review of their laws and regulations relevant to critical information infrastructures; assess the need for updates, new laws, or new implementation and enforcement regimes; develop a national cyber security strategy that encompasses all the requisite government jurisdictions and private sector operations; and coordinate with other member states and non-OECD countries to take into account interdependency vulnerabilities of the global information infrastructure.

The European Commission in 2009 issued a new communication on Protecting Europe from Large Scale Cyber-Attacks and Disruptions, which emphasized the importance of international cooperation for cyber security, and included action items to help member states evolve from a purely national approach.

The United States' 2009 Cyberspace Policy Review identified multi-jurisdictional legal analyses and international cooperation as two of the most urgent policy action-items.

Along with the June 2009 update of its National Security Strategy, the United Kingdom released its first U.K. Cyber Security Strategy, for which one key priority was international coordination for the development of international law.

November 2009 saw the launch of Australia's first Cyber Security Strategy, which includes among its priorities: international engagement and effective legal and law enforcement frameworks.

In 2009 a Council of Europe ad hoc working group began activities to examine the responsibilities of countries regarding the management of critical Internet resources, and to "explore the feasibility" of establishing an international agreement to protect the cross-border flow of Internet traffic.

Cyber Workshops *(Cont. from 14)*

an ecosystem of actors and discuss their roles and responsibilities and the dynamics of their interaction and interconnectivity. WoCI will also ask participants to consider what is technologically possible and feasible in incorporating relevant characteristics into the design and change of cybersecurity systems. Ongoing debate and research in this area will be presented in practical terms allowing for participants to immediately realize implementable options for governing cybersecurity at the enterprise and national levels. The workshop will be composed of presentations and panel discussions covering legal, economic, and technological issues. ❖

For more information, please view the following websites:

WEIS: http://weis2011.econinfosec.org/

WoCI: http://bit.ly/WOCI-GMU

Contact Information:

For more information about WEIS, please contact Tim Clancy, Center for Infrastructure Protection and Homeland Security, at tclancy@gmu.edu.

For more information about WoCI, please contact Dan Arista, Syracuse Research Corporation, at darista@srcinc.com.

Public-Private Collaboration *(Cont. from 13)*

developed. These three elements alone will get us moving in the right direction, past what we all already know and feel comfortable discussing.

This is hard work. Our government has not taken an operational approach to solving these issues as a national enterprise. Collaboration between sectors's today appears so very stove-piped. Aside from the fact that most of these stove-pipes reside within select defense and intelligence partners, they are not broadly shared with the larger national community. The question of "where is our U.S. cyber policy?" gets more attention than where is the supporting concept of operation (CONOP)? Who has what lanes? Is this law enforcement or military operations? As stated earlier, policy will drive responsibilities, but awareness of and access to capability is policy-neutral. Establishing the collaborative framework can give the public and private sector the awareness and access it desires so as the hard policy decisions are made, the ability to reach out for cyber solutions is there for our national enterprise. ❖

Cyber and Transportation *(Cont. from 7)*

activities in transportation cybersecurity are being coordinated with related activities to assess the safety of cyber-physical systems in transportation. Ultimately, potential cyber vulnerabilities may be addressed as part of the safety certification process for new transportation systems. ❖

Smart Security *(Cont. from 11)*

were selected for mentioning — to guard businesses from interruption, prevent the loss of capital or intellectual property, and protect public safety.

Add Business Value Through Information Security

Unlike larger enterprises, which often have specialists, such as a chief information officer or a chief security officer, to manage an array of risks facing businesses, small businesses generally do not have the people and resources for a formal information security program. In today's challenging economy, small businesses are looking for creative ways to make ends meet. Still, regardless of size and resources, the obligation for dealing with threats to a business' information security rests with each person — from CEOs to frontline workers.

Business owners and managers can add value to their enterprises by implementing the suggestions highlighted in this guide, many of which are relatively easy and inexpensive to employ. It is far less expensive to invest in better Internet security than to lose trusted customers and business partners, get enmeshed in legal actions, or face the possible consequences of a security breach. ❖

Year in Review *(Cont. from 4)*

communicate cyber issues to the public requires improvement. Bob Dix, Vice President of U.S. Government and Critical Infrastructure Protection for Juniper Networks, citing the Nation-wide effort to inform people about the flu during the H1N1 pandemic in 2009, stated that the United States is in a cyber epidemic and asked, "[w]hy aren't we educating people?"[17] Former Representative Tom Davis, coauthor of the Federal Information Security Management Act and the E-Government Act, struck a similar tone in a comment last September regarding cybersecurity legislation stating, "[t]here's no immediate political value in pushing your green stamps on this because the public is pretty oblivious to this."[18]

In closing, one constant in the American tradition is that when challenges arise, the American citizenry wishes to have an active role in problem solving. A potential model illustrating this sentiment is the 2007 partnership between James Madison University and the Virginia Department of Education, which produced the Cyber Citizenship Guide, a resource organized around the way a middle-schooler uses the Internet, such as surfing for homework, connecting with friends through social networks and chats, gaming, email, and so on. Under Federal leadership with the private sector and higher education as equal partners, a cyber guide focusing on proactive protection recommendations could be produced and distributed at the State and local level. One possible road map is for the Federal government to coordinate a public awareness campaign, in time for National Cybersecurity Awareness month in October, to put the spotlight on cybersecurity, recognized by President Obama as the key to America's economic prosperity in the decades ahead. ❖

---

[17] Kevin McCaney, "Cyber 'Epidemic' Grows more Urgent," (2010) *Government Computing News*, October 26. Accessed October 28, 2010, http://gcn.com/articles/2010/10/26/elc-cybersecurity-collaboration.aspx.

[18] Eric Chabrow, "House passes Cybersecurity Enhancement Act Measure, Approved by 422-5 Vote, Goes to the Senate (2010)." *GovInfoSecurity*, February 4. Accessed February 9, 2010.

Legal Insights *(Cont. from 16)*

threat] lies in the transnational nature of cyberspace and the need to secure international agreement for broadly applicable laws controlling offenses in cyberspace."

In addition to political and legal commentary, technical and security experts such as International Telecommunications Union's (ITU) secretary-general and Bruce Schneier, have also been advocating an international framework for addressing such cybersecurity threats.

International organizations already at work in this area include ITU, the Organisation for Economic Co-Operation and Development (OECD), the North Atlantic Treaty Organization (NATO), the European Union (EU), and the Organization of American States (OAS). Many other groups have been equally busy with international efforts against cyber crime, fraud, terrorist financing, etc.; this *Legal Insights* article cannot attempt to be fully inclusive.

An example of one new initiative is the recent introduction of a Proposed EU Directive that calls for the establishment of "a new legislative framework aimed at combating (large scale) attacks against information systems." This proposed directive would introduce new crimes regarding "large-scale cyber attacks" and would also include new aggravating circumstances and higher criminal sanctions for such crimes. It would also create an explicit, legally-established, international system to record and trace cyber attacks. The proposal additionally attempts to improve cooperation between the judiciary and the police, to strengthen and modernize the European Network and Information Security Agency (creating a sort of European CERT of national CERTs), and imposes an obligation to make better use of the 24/7 network.

There are of course many challenges to establishing a workable, international legal framework regarding cyber incidents that threaten national and international security. Not the least of which include the wide variances in national perspectives of the cyber threat; in degrees of network resilience and technical or operational vulnerabilities; in societal, governmental, and commercial reliance on the Internet; and in national priorities to control or to open flows of information. Cooperative, international cybersecurity initiatives are at different stages of development; countries are at different phases in their cyber capabilities.

Many entities have recognized the importance of international activity on the cyber front. The consensus is forming that national cybersecurity challenges must be addressed at the international level. Given the activity around this priority in 2009 and 2010, it will be interesting to watch what 2011 will bring. ❖

**Maeve Dion is a former research faculty with CIP/HS. She is currently with Stockholm University, Sweden, lecturing in the Masters program in Law and IT, and pursuing her doctorate of law in national and international cyber security. Contact information and more research details may be found on her research pages of Stockholm Law Faculty website.*

USCYBERCOM *(Cont. from 6)*

are essential to military command and control, communications, intelligence, operations, and logistics — all potentially lucrative targets for a cyber adversary. There are over seven million DoD computing devices and more than 15,000 DoD networks being scanned and probed six million times per day. The high rate of change in operations will require enormous dedicated resources and modernized cyber processes — not just technology, but new military doctrine, organization, training and education, materiel, leadership, personnel, and facilities. Lastly, U.S. laws and policies also need to reflect the technological and cultural shifts occurring within our contemporary society.

Conclusion

Cyberspace demands a team approach because security is only as strong as its weakest link. Partnerships are necessary for successful cybersecurity. The U.S. government's efforts to secure its own interests in cyberspace would be greatly assisted if every American uses due diligence in securing their own systems and networks. Constant focus on cyber education and targeted discussions on effective means to secure cyberspace are necessary at every level of society. Our national security depends upon assured access to cyberspace and freedom of action in cyberspace. Cyberspace has become an effective and integrated part of our Nation's success; therefore, securing cyberspace will be an important step in increasing our efforts in homeland defense. ❖

References

1. President Barack Obama, *The National Security Strategy of the United States of America*, (Washington DC: The White House, May 2010, 27).

2. The Department of Defense, *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*, (Washington DC: Office of the Secretary of Defense, June 2009).

3. Secretary of Homeland Security and Secretary of Defense, *Memorandum of Agreement Between The Department of Homeland Security and the Department of Defense Regarding Cybersecurity*, (Washington DC: Office of the Secretary of Homeland Security and Office of the Secretary of Defense, released 13 October, 2010).

4. The Department of Defense, *Quadrennial Defense Review Report*, (Washington DC: Office of the Secretary of Defense, February 2010).

5. Foreign Affairs Article, *Defending a New Domain, the Pentagon's Cyberstrategy*, (Washington DC: Deputy Secretary of Defense William Lynn, III), September/October 2010, Volume 89, Number 5.

6. Small Wars Journal Article, *Winning the Ground Battles but Losing the Information War*, (http://www.smallwarsjournal.com: Gina Cairns-McFeeters, John Shapiro, Steve Nettleton, Sonya Finley and Daryk Zirkle). Posted by Small Wars Journal Editors 21 January, 2010.

The Center for Infrastructure Protection works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1