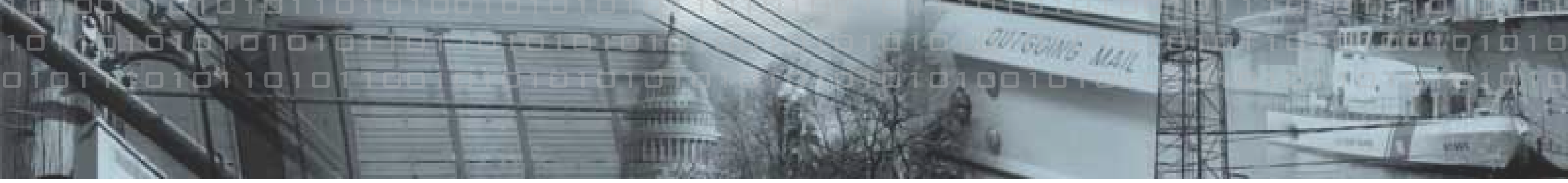

THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

OCTOBER 2014
CYBERSECURITY

EDITORIAL STAFF

EDITOR
Christie Jones
Daniel Miktus
Dennis Pitman
Tehreem Saifey

PUBLISHER
Melanie Gutmann

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

Follow us on Twitter here
Like us on Facebook here

VOLUME 13 NUMBER 3

This month's *The CIP Report* focuses on **Cybersecurity.**

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

First, Kristina Dorville, Deputy Branch Chief for the Cyber Education and Awareness Branch at the Department of Homeland Security, highlights National Cyber Security Awareness Month (NCSAM) and reviews the five weeks of NCSAM events that took place across the country. Next, a paper submitted by Andrea LeStarge, of Argonne National Laboratory, and Troy Campell, with the Kansas City Regional Terrorism Early Warning Group Inter-Agency Analysis Center, looks at leveraging national fusion centers' cyber intelligence capability to meet the growing and evolving cyber threat environment. Next, Christopher Topham, graduate assistant with the Center for Infrastructure Protection and Homeland Security (CIP/HS), discusses cybersecurity and current Congressional legislation; finally, Dr. Mark Troutman, Associate Director of CIP/HS and J.P. Auffret, Director of Executive Degree Programs with George Mason's School of Business, provide an overview of a cybersecurity research partnership between between George Mason University (GMU), the IBM Corporation (IBM), and the National Science Foundation (NSF).

We would like to take this opportunity to thank this month's contributors. 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

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

National Cyber Security Awareness Month Promotes Cyber Awareness and Secure IT Development

by Kristina Dorville*

For more than 10 years, the United States has recognized October as a month to reflect on the significance of cybersecurity and to engage the country about the importance of taking steps to be safe online. This year, the Department of Homeland Security (DHS) and its partners celebrated National Cyber Security Awareness Month (NCSAM) through five weeks of events across the country, virtual events such as Twitter chats, and the distribution of resources and materials.

- The Department's cyber awareness campaign, known as the Stop. Think.Connect.™ Campaign (the Campaign), gained six new partners in the first week alone, including the Department of Defense and the National Association of Women Business Owners, which means that six new organizations want to work with DHS to promote cyber awareness.
- Following The White House NCSAM Memo declaring October as National Cyber Security Awareness Month,[1] five Federal agencies reached out for more information, including the Department of Defense, U.S. Agency for International Development, Drug Enforcement Agency, Department of State, and the Peace Corps.
- In just the first two weeks of October, the Campaign gained nine new partners, which is 50 percent above the 2014 average monthly partner growth (six partners per month).
- NCSAM events and promotion continue to drive a significant spike in online conversation surrounding cybersecurity. The average weekly conversation in October is 228 percent higher than last month.

The campaign had a very successful month, with each week bringing about its own highlights.

Week 1: Promoting Online Safety with the Stop.Think.Connect.™ Campaign

The first week of NCSAM aimed to remind us that cybersecurity is a shared responsibility. Every person at every age should be educated and made aware of cybersecurity and the opportunities, as well as the threats, that accompany the Internet and technology. Week One also highlighted efforts that relate to Executive Order 13636,[2] which seeks to improve critical infrastructure cybersecurity across multiple sectors, such as our financial, electric, and communications systems. This year, the NCSAM 2014 Kickoff Event took place at the National Association of State Chief Information Officers (NASCIO) annual conference in Nashville, Tennessee, and was a resounding success! Over 400 people attended and even more watched via the live stream.

Week 2: Secure Development of IT Products

Security is an essential element of software design, development, testing, and maintenance, which is why NCSAM Week 2 focused on the secure development of IT products. The software we use every day on our phones, tablets, and computers may have vulnerabilities that can compromise our personal information and privacy. How we use our IT products and devices is important. Regardless of how secure our IT products are, individual users can and should take a few steps to improve their cybersecurity. During this week, Bloomberg Government hosted a panel to discuss the importance of secure development and current efforts within the private and public sectors to build safer products and services. Dr. Andy Oz-

(Continued on Page 3)

[1] The White House, Office of the Press Secretary, *Presidential Proclamation: Nation Cybersecurity Awareness Month, 2014* (Sept. 30, 2014), available at http://www.whitehouse.gov/the-press-office/2014/09/30/presidential-proclamation-national-cybersecurity-awareness-month-2014.

[2] The White House, *Executive Order 13636: Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013), available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

(Continued from Page 2)

ment, the Assistant Secretary of the Office of Cybersecurity and Communications (CS&C) within DHS, participated in the panel. Some simple tips offered include:

- Installing and maintaining vendor-distributed patches or updates;
- Ensuring employees use the latest operating systems on computers and mobile devices; and
- Being aware of vulnerabilities that may exist.

Week 3: Critical Infrastructure and the Internet of Things

The Internet underlies nearly every facet of our daily lives and is the foundation for much of the critical infrastructure that keeps our nation running. Week 3 focused on the security of the systems that support electricity, financial services, transportation, and communications. Just as those critical infrastructure items are essential to helping Americans live their everyday lives, a growing "Internet of Things" is changing the way we use technology and helping people live more efficiently. The Internet of Things (IoT) encompasses the devices that are embedded with computers and, through a combination of sensors, connectivity to the Internet, and human activity, work to connect our lives to the digital world. To promote this, a keystone event was held in downtown San Diego, California, where government, businesses, and consumers heard IT professionals in government and industry discuss issues currently revolving around critical infrastructure and IoT. A number of the speakers, including Jason Gates of DHS, Michele Robinson from the State of California, Chris Baker of Sempra Energy Utilities, and Nicole Dean of Raytheon, discussed how IoT provides us all with numerous opportunities in the ever increasing digital world in which we now live. However, with IoT products being brought to market quickly, strategies and important discussions amongst businesses must start to take place in order to protect systems from the potential risks and vulnerabilities associated with these products.

Consumers and businesses all play a large role in helping protect the 16 critical infrastructure sectors and the IoT. Some simple steps include:

- Learning how to enhance security and resilience within local businesses and communities so that individuals can be informed on how to handle various events and threats;
- Reporting suspicious activity to local law enforcement; and
- Exercising due diligence in what devices you choose to use within the IoT.

WEEK 4: Cybersecurity for Small and Medium-Sized Businesses and Entrepreneurs

Small and medium-sized businesses are the backbone of the Nation's economy. Aside from the wide range of services they offer, small and medium-sized businesses store significant amounts of sensitive data, from customer information to intellectual property. Entrepreneurs also face a unique cybersecurity threat as their data includes not only personnel data and financial spreadsheets, but valuable intellectual property that could be worth much more than they realize. NCSAM Week 4 aimed to emphasize the resources available to small and medium-sized businesses and entrepreneurs to be cyber-aware and safe. These entities are increasingly becoming targets for cyber criminals, who recognize that they may not have the awareness or resources to protect themselves. The assets required to protect small and medium-sized businesses from cyber risks are not as readily available as they are to their larger industry counterparts.

DHS has resources to help. It developed the Critical Infrastructure Cyber Community Voluntary Program, or the C^3 (pronounced "C Cubed") Voluntary Program. The C^3 Voluntary Program encourages businesses of all sizes to establish or improve their cyber risk management processes and to take advantage of resources made available by the U.S. Government. As part of that, DHS's Cyber Resilience Review (CRR) provides businesses a free, non-technical assessment of an organization's cybersecurity and resilience practices. A business can opt to do a self-assessment or a DHS professional will come on-site. For more information on the C^3 program, click here.

Week 5: Cyber Crime and Law Enforcement

Crimes such as credit card fraud, identity theft, and sexual harassment are not new. The Internet, however, has made these types of crimes more prevalent and easier to carry out. Criminals are not the only ones using technology for their benefit. Many law enforcement

(Continued on Page 4)

(Continued from Page 3)

agencies are taking advantage of technology to track down cyber criminals. NCSAM 2014 closed out the month focusing exclusively on law enforcement. This week served in part to remind everyone of simple things everyone can do to avoid falling victim to cybercrime, such as:

- Protecting any device that connects to the Internet;
- Checking the security of websites, especially those used for banking and shopping; and
- Avoiding suspicious emails or websites that do not look legitimate or request too much personal information up front.

National Cyber Security Awareness Month may solely be during the month of October, but NCSAM reminds us all that cybersecurity awareness should be discussed and taught throughout the year. The Stop.Think.Connect.™ Campaign works to build relationships with various businesses, government entities, and academia to promote cybersecurity and cyber awareness. As the world of technology continues to grow, DHS continues its mission to help build a nation of educated Americans and successful digital citizens.

For more information on National Cyber Security Awareness Month and the Stop.Think.Connect.™ Campaign, visit www.dhs.gov/stopthinkconnect. Additionally, for free resources tailored to various audiences and demographics, visit www.stcguide.com. PowerPoint presentations, blog posts, articles, posters, and videos are available at no cost and are readily available for download and distribution. ❖

**Kristina Dorville is the Deputy Branch Chief for the Cyber Education and Awareness Branch at the Department of Homeland Security. She has been at DHS since its inception in 2003. She is also an alumna of George Mason University.*

Leveraging the National Fusion Center Cyber Intelligence Capability

by Andrea LeStarge* and Troy Campbell**

Introduction

According to the U.S. Department of Homeland Security (DHS), "[o]ur nation faces an evolving threat environment, in which threats emanate not only from outside our borders but also from within our communities."[1] The phrase, "evolving threat environment" could not have been more prophetic. During the time this statement was written in 2010, cyber threats were not mentioned. Fast forward to March 2013, when a cadre of the Nation's top intelligence officials were testifying to the Senate (Select) I*ntelligence Committee on the Intelligence Community Worldwide Threat Assessment* and, for the first time since September 2001, began their comments by stating that cyber-attacks are the number one threat facing the United States.[2]

Cyber threats are pervasive and multiplying at an alarming rate. According to one global leader's analysis of data breaches, more than 200 million records were stolen between January and March 2014—that is approximately 93,000 records stolen every hour, which is an increase of 233 percent over the same time in the previous year (January through March 2013)[3]. State actors, sophisticated cyber-crime organizations, hackers, hacktivists, cyber jihadists, and State-sponsored or affiliated cyber armies are strengthening in techniques, tactics, and membership. As a result, vulnerabilities within networks ranging from those of the Federal government to State, local, tribal, and territorial (SLTT) governments and extending to networks within each of the 16 critical infrastructure sectors, or even to the smallest of businesses, are constantly being exploited.

In just SLTT entities alone, the potential size of the "attack surface" is vast: within the 50 States, there are just under 39,000 incorporated cities, towns, and jurisdictions.[4] Securing those communities at the ground level are 17,985 State and local law enforcement agencies—the majority with less than 24 officers.[5] Therefore, agencies with limited staffs are stressed with identifying, responding, reporting, and implementing the correct mitigation measures to thwart various cyber threats.

Information Sharing Partnerships: Fusion Centers and the Four Critical Operating Capabilities

The expanding reach of transnational organized crime syndicates across cyberspace, international borders, and jurisdictional boundaries within the United States highlights the continued need to build and sustain effective intelligence and information-sharing partnerships among the Federal government, SLTT governments, and the private sector.[6] Aiding in, and serving as a focal point within, those information-sharing partnerships are fusion centers. Fusion centers are uniquely situated to enhance current threat pictures at the tactical, operational, and strategic

(Continued on Page 6)

[1] U.S. Department of Homeland Security & U.S. Department of Justice, *State and Major Urban Area Fusion Centers* (July 2012), available at http://www.dhs.gov/sites/default/files/publications/Fusion%20Centers%20Handout.pdf.

[2] Office of the Director of National Intelligence, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community* (Jan. 29, 2014), available at http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf.

[3] Lavasoft, *Data Breaches Surge in 2014 with 200 Million Data Records Stolen*, (Apr. 30, 2014), available at http://lavasoft.com/mylavasoft/company/blog/data-breaches-surge-in-2014-with-200-million-data-records-stolen.

[4] U.S. Census Bureau, *Government Organization Summary Report: 2012: Government Division Briefs* (Sept. 26, 2013), available at http://www2.census.gov/govs/cog/g12_org.pdf.

[5] U.S. Department of Justice, *Bureau of Justice Statistics, Census of State and Local Law Enforcement Agencies*, 2008 (July 2011), available at http://www.bjs.gov/content/pub/pdf/csllea08.pdf.

[6] U.S. Department of Homeland Security, *2013 National Network of Fusion Centers: Final Report* (June 2014), available at http://www.dhs.gov/sites/default/files/publications/2013%20National%20Network%20of%20Fusion%20Centers%20Final%20Report.pdf.

(Continued from Page 5)

levels because of the breadth and depth of knowledge encompassed within the analyst cadre that work within these nodes. Although there are differences among centers on the basis of their geographical areas of responsibility, all centers have the common responsibility of executing the four critical operating capabilities (COCs):

1. **Receive**: Ability to receive classified and unclassified information from Federal partners.
2. **Analyze**: Ability to assess local implications of threat information through the use of a formal risk assessment process.
3. **Disseminate**: Ability to further disseminate threat information to other SLTT and private sector entities within the fusion center's area of responsibility.
4. **Gather**: Ability to gather locally generated information and then to aggregate, analyze, and share it with Federal partners, as appropriate.

In addition to these four COCs, fusion centers also provide critical information and subject matter expertise that allow the Intelligence Community (IC) to more effectively "connect the dots" to prevent and protect against threats to the homeland.[7] As a result of the evolving threat environment, many fusion centers now include cyber threats in their mission scope, in fact, exercising the four COCs through the lens of cyber. Nevertheless, there are so many agencies (including some commercial and not-for-profit organizations) trying to address cyber threats that the need for coordination with fusion centers is of paramount importance now more than ever before.

The Need: Outlining the Fusion Center Cyber Mission Space Based on the Complexity of Cyber Attacks

As stated in the *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity* (2014), the Nation benefits when State and Federal entities fully utilize their authorities and resources in cooperation.[8] However, because a cyber incident can constitute both a physical impact as well as a physical occurrence with cyber implications, the cyber mission space and the "lanes in the road" are not clearly painted or delineated for all partners responding to cyber events (whether threats, vulnerabilities, consequences, risk mitigation measures, or even the "high-occupancy vehicle [HOV] lane" that contains a coupling of these elements). Thus, this article suggests one possible option out of surely many that may help to provide a solution.

The pyramid presented in Figure 1 can be used as a generic visual to display the types of threats by the number of occurrences. Coincidentally, it also models the complexity of cyber threats and actors. At the apex of the pyramid is "APT," also known as Advanced Persistent Threat. It is easy to place espionage (corporate and State sponsored) as well as massive data breaches at this level. This threat is most effectively addressed by Federal entities such as the Federal Bureau of Investigation (FBI) or the National Security Administration (NSA), as well as Cyber Command groups found within the U.S. Department of Defense (DOD) because of the subject matter expertise among staff who are constantly working to detect, identify, and deter cyber threat actors.

Next, there are "Targeted" attacks, or exploits, in the middle slice of the pyramid. As its name implies, these attacks are specifically targeted at individuals or organizations, most often critical infrastructure owners and operators and/or companies with dependencies on these infrastructure elements. The agencies and organizations most likely to address these attacks are the U.S. Secret Service (USSS), U.S. Computer Emergency Readiness Team (US-CERT), and several entities housed within DHS. With similar knowledge and tools to those partners in the APT section, a given victim's characteristics drive the investigative procedures and response tactics encompassed within these agencies.

Finally, the base of the pyramid is where various cyber threats that are not targeted reside. These untargeted threats are conducted by actors with both intent and capabilities most appropriately detected by SLTT and private sector partners. As mentioned earlier, it

(Continued on Page 7)

[7] Ibid.

[8] National Governors Association, Council of Governors, *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity* (2014), available at http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1407CouncilofGovernorsCyberJointActionPlan.pdf.

(Continued from Page 6)

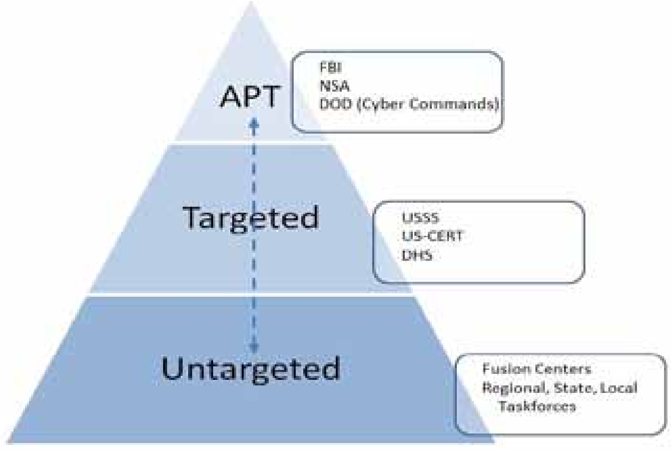

Figure 1 – Type of Threats by the Number of Occurrences

is within this component of the pyramid where fusion centers are appropriately stationed and uniquely situated. Here, analysts and fusion center liaisons constantly exchange information and exercise that information through the four COCs. The types of victims, investigative procedures, and response tactics are slightly different than those found in use among the previous partners. Furthermore, fusion centers within this level can also serve as a vetting entity supporting triage and burden to the other levels.

It is important to note that this pyramid's components are broad classifications and that both the agencies expected to be involved and the types of attacks in individual instances or events can be represented up and down the pyramid. Similarly, when the severity or complexity of an attack reaches a threshold, the event is transferred to the appropriate level in the pyramid (illustrated by the blue arrow). In sum, with the implementation of effective practices related to the receiving, gathering, analyzing, and disseminating of cyber-related information, movement within this pyramid could occur more frequently among all partners.

A Call to Action

Threat actors' techniques, tactics, and procedures continue to evolve, and the current efforts toward cybersecurity reveal the need for improved coordination and collaboration. While fusion centers continue to apply the four COCs to their mission-essential tasks, the need for operational organization still exists. Thus, at this point, it is critical that stakeholders involved in cyber defense efforts carry out the following:

1. Assist in defining the general outlines of the mission space of fusion centers regarding cyber threats.
2. Facilitate training in each of the four COCs regarding cyber so that fusion center analysts serve as an appropriate and accurate vetting mechanism.
3. Provide products, data, and analytical-assistive services within a timely manner while coordinating with fusion centers to help ensure their continued understanding and consistent messaging of the threat environment within their areas of responsibility.
4. Facilitate communication of cyber intelligence to and from the fusion centers at "net-speed" (e.g., fusion center to fusion center, fusion center to Federal partners, fusion center to SLTT, and fusion center to private sector partners).

With appropriate attention given to these four recommended areas of improvement, intelligence analysis activities and competencies within the cybersecurity realm will be effectively and efficiently executed.

Acknowledgment

The submitted manuscript has been created by UChicago Argonne, LLC, Operator of Argonne National Laboratory ("Argonne"). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government. The development of the tools presented in this paper has been funded by the U.S. Department of Homeland Security Protective Security Coordination Division under Contract No HSHXDC-13-X-00223. ❖

Andrea LeStarge is a Risk Analyst with the Risk and Infrastructure Sciences Center, Global Security Sciences Division, Argonne National Laboratory. Troy Campbell is a Cyber Threat Intelligence Program Architect with the Kansas City Regional Terrorism Early Warning Group Inter-Agency Analysis Center.

Cybersecurity and the Law: Moving Forward

by Christoper Topham*

Current State

In late July 2014, the U.S. House of Representatives passed a trio of bills aimed at improving various domains of cybersecurity and our national critical infrastructure. Of the three bills, H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act of 2014, has received significant attention as it captures two of the largest issues currently facing players in the cybersecurity market.

The first proposal in H.R. 3696 is aimed at solidifying formal partnerships between private industry and the federal government in cybersecurity. Expanding on the concerns that have previously been raised regarding gaps in the SAFETY Act,[1] this bill explicitly addresses privacy concerns regarding civil liberties while protecting Americans from cyber-attacks.

Second, the bill addresses a tremendous shortcoming in the Homeland Security Act in its current state, seeking to bring cybersecurity under the umbrella of antiterrorism technologies. The SAFETY Act creates partnerships and protections, including risk management and liability protection, for technologies and services that are deemed to have an antiterrorism function. These designations have yet to seep into the cyber sector, leaving a tremendous vulnerability in legal protection that impedes growth in the cybersecurity industry.

Should Congress pass H.R. 3696, it would constitute an amendment to the SAFETY Act, bringing cybersecurity technologies under the umbrella of "antiterrorism technologies" and providing all benefits currently available under the SAFETY Act to compliant cybersecurity technologies and services. Although these protections are necessary to foster the growth and development of affordable and effective cybersecurity technologies in the near future, the odds of this bill moving forward in its current state are slim in the present political climate.

Public-Private Information Sharing

The credit-card breach incident that occurred with national retailer Target Corp. last year[2] provides just one example of the chaos that can be caused by the successful exploitation of a large network. In that theft, malicious hackers stole over 40 million credit card numbers, even though alerts generated at the local level were present days before the attack and could have prevented the breach entirely.[3]

One of the major cybersecurity issues currently facing our nation is the lack of integration between private sector and public defense for cybersecurity. For unknown reasons, security personnel did not act upon the alarms triggered within Target's cyber and risk departments. An individual actor only has access to threat information that has been exhibited against him, whereas a federal cybersecurity network could consolidate information on numerous threats in one central location. If a formal pipeline existed, an isolated alarm at the local level would automatically be reported up the chain, and could receive closer scrutiny if it resembled known threats.

Presently, initiatives exist to create voluntary information sharing, but as numerous legal scholars have pointed out, encouraging voluntary action simply does not do enough

(Continued on Page 7)

[1] *See* The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act), Pub. L. 107-296, 107th Cong., subtitle G (2002), available at http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.

2 *See* Robin Sidel, et. al., *Target Hit by Credit-Card Breach*, The Wall Street Journal (Dec. 19, 2013), available at http://online.wsj.com/articles/SB10001424052702304773104579266743230242538.

[3] Michael Riley, et. al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Bloomberg Businessweek (Mar. 13, 2014), available at http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

(Continued from Page 8)

to create an effective response against a coordinated threat.[4] There are a number of reasons why a voluntary scheme of reporting and coordinating cyber defense has yet to bear real fruit, but the two most outstanding issues are privacy concerns and the lack of a clear national standard. The first of these issues highlights the challenge of the government's tenuously conflicting stance on cybersecurity—trying to encourage a trustworthy environment of information exchange while running programs like the NSA's PRISM platform in the background.[5] Companies are more hesitant than ever to hand over sensitive information about their systems that might contain information about their customers and client base, as this could have the twofold effect of eroding trust in that company and exposing them to civil liability.

The National Institute of Standards and Technology (NIST) has released a Framework for Improving Critical Infrastructure Cybersecurity (the Framework) that seeks to get more businesses on the same page of the cybersecurity playbook.[6] The Framework gives guidance to industry members on safeguarding against cyber-attacks and delineates certain "Tiers" of preparedness against attack. However well-developed the Framework may be, its generalized structure is insufficient on its own to provide for the privacy demands of many businesses. It does not provide incentives or benefits to companies that reach certain "Tiers" of preparedness, and has been criticized that it cannot be relied on to create an effective cybersecurity web.[7]

With the comment period for an updated NIST Framework now over, one can only hope that these major concerns will be addressed in the Framework's next iteration. While it does provide aid to a company initially creating a cybersecurity program, more work is required to create a uniform system that spans the entire economy.

Effective Liability Protection and Encouragement

However the Framework may evolve, an effective environment of sharing between the public and private sector will be useless if the technology is never created. While the concept of ethical hacking has been around for some time now, firms still face significant barriers to entry when contemplating development of cybersecurity technology and software. As it currently stands, a software developer could be held personally liable for shortcomings of their product or software. This prevents new developers from entering the market, because it is safer for a developer to create generalized software that can deal with a variety of broad threats without a guarantee against any specific threat.

Creating an effective cybersecurity and risk environment is like crafting a suit of armor; one layer of protection is simply insufficient protection. Cybersecurity planners must start at the bottom, with the most basic form of protection, and then work outward, layering and reinforcing in areas known as targets for the enemy.[8] For the consumer market, however, the current strategy with cybersecurity involves wholesale bandages over potential problem areas without a

(Continued on Page 10)

[4] Robert Gyenes, *A Voluntary Cybersecurity Framework Is Unworkable - Government Must Crack the Whip*, 14 U. Pitt. J. Tech. L. Pol'y 293, 303-306 (2014), available at http://tlp.law.pitt.edu/ojs/index.php/tlp/article/view/146/157; Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 Stan. J. Int'l L. 119, 148-151 (2014), available at http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2465923_code410303.pdf?abstractid=2446666&mirid=1.

[5] Gerry Smith, *"Snowden Effect" Threatens US Tech Industry's Global Ambitions*, YaleGlobal Online (Jan. 28, 2014),available at http://yaleglobal.yale.edu/content/%E2%80%9Csnowden-effect%E2%80%9D-threatens-us-tech-industrys-global-ambitions.

[6] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[7] Katie Dvorak, *NIST Cybersecurity Framework Needs More Guidance on Implementation*, FierceHealthIT (Oct. 20, 2014),available at http://www.fiercehealthit.com/story/nist-cybersecurity-framework-needs-more-guidance-implementation/2014-10-20; Antone Gonsalves, *NIST Cyber Security Framework Proposal Provides No "Measurable Cybersecurity Assurance,"* CSO Online (Sept. 5, 2013), available at http://www.csoonline.com/article/2133893/malware-cybercrime/nist-cyber-security-framework-proposal-provides-no--measurable-cybersecurity-assu.html.

[8] U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies* (Oct. 2009), available at https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf.

(Continued from Page 9)

large degree of specificity or innovation by the developer. This approach has the same effect as a medical doctor prescribing broad spectrum antibiotics to fight infections; they are affordable but do not have the precision of a finely tuned serum.

Another undesirable effect of such wholesale treatment of cybersecurity is that, like antibiotics, effectiveness diminishes with repeated use against general threats. Over time, vulnerabilities around the periphery are systematically identified and exploited by the smart and determined attacker. Without incentives and pathways for firms to build and extend proper layered defense systems, we will continue to see massive exploitations of private sector entities that have not evolved.

Market demand currently exists for more finely-tuned cybersecurity and risk resources that can help seal the critical gaps in a business's armor. The impetus is now with the government to step up and provide legal protections for those firms who are willing to develop software to protect against outside threats. To encourage growth in the cybersecurity industry, protections such as those proposed in the National Cybersecurity and Critical Infrastructure Protection Act must become a reality.

However, progress must not stop with the passage of one act of Congress. A comprehensive system must be created that provides incentives for developers to work on cyber-threat issues and for companies to feel safe sharing information regarding their cybersecurity. It is up to individual businesses and software developers to become aware of these issues, make their voices heard, and press for a resolution. Private industry must have a nuanced understanding of the challenges posed by cybersecurity; government regulation alone will not resolve these issues. Without a unified front against cyber-attacks, chinks in the armor in one sector or firm can have ripple effects through the entire industry. ❖

Christopher Topham is a Graduate Research Assistant with the Center for Infrastructure Protection and Homeland Security as well as a third year law student with the George Mason University School of Law.

The GMU/IBM/NSF Cybersecurity Research Workshop: An Early Overview[1]

by Mark Troutman*

The cyber threat to the nation's energy sector is a well-known and highly studied issue, yet we often fail to understand threats, vulnerabilities, and solutions because of the complex nature of the energy sector. Leaders and researchers pay great attention, with good cause, to malicious activity that impacts the generation, transmission, and distribution of power over the energy grid. The direct impact of electric power disruptions is evident. Natural and man-made operational impacts have made clear the vulnerability of the grid to disruption. Incident reporting from the U.S. Computer Emergency Readiness Team indicates that the grid is a popular target among adversaries, with 59 percent of the 256 critical infrastructure attacks in 2013 involving the energy sector, particularly electrical systems.[2] As Presidential Policy Directive 21 (PPD-21) and the 2013 National Infrastructure Protection Plan (NIPP) highlight, the cascading effects of disruptions across other sectors leads to equal or greater impact because of their dependence on the energy sector.

The threat manifest on the energy grid at the intersection of cyber networks and physical control systems is less well understood in the array of energy sector concerns. Vulnerabilities exist because the distributed system of grid control operates through a mix of interconnected and interdependent analog and digital systems. In short, we do not fully understand the implications of physical control systems, never designed for open network or wireless connections that operate in an increasingly interconnected world. Today we are in the midst of the automation of cyber-physical systems and the Internet of Things. These developing technological issues call for leaders with the critical thinking and interdisciplinary skills to understand this complex challenge and develop answers to secure the vital infrastructure of the energy grid.

A collaborative effort started this year between George Mason University and the IBM Corporation as part of IBM's Shared University Research Award program,[3] and the National Science Foundation continued an ongoing investigation of the technical, policy, and leadership challenges presented by the problem of legacy systems that operate on the energy grid as it continues to evolve into the "Grid of the Future." GMU participants include the School of Business, Volgenau School of Engineering, the School of Public Policy, and the Center for Infrastructure Protection and Homeland Security. IBM participants include researchers, energy and utility technologists, security strategists, and analytics specialists.

In a July 2014 mid-project workshop, the combined GMU/IBM/NSF research team hosted a group of over sixty scholars, business leaders, government leaders, and technical experts from the U.S., Europe, and the Asia-Pacific region to investigate the technological, policy, and leadership aspects of the cyber-physical dimension. The inquiry addressed best practices, open challenges, and the "Grid of the Future." The findings and highlights of the workshop are under review and report preparation is underway. *The CIP Report* will feature a future article reporting findings and highlights from the workshop. However, the way the team approached the major inquiries of this one-day workshop are significant and worthy of

(Continued on Page 12)

[1] This material is based upon work supported by the National Science Foundation under Grant No 1303299. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

[2] http://fcw.com/articles/2014/02/28/government-should-backstop-efforts-to-protect-grid.aspx

[3] https://newsdesk.gmu.edu/2014/02/mason-team-partner-ibm-research/

(Continued from Page 11)

dialogue in their own light, given the ongoing challenge of energy grid security.

The combined project began, as many such efforts do, with a set of technical challenges. As an indicator, author Jerry Forstater recently wrote that over 80 percent of critical access system components—one class of physical systems linked via internet architecture—are based on 1970s technology. As control systems designed and installed decades ago age, firms that generate repair capabilities and provide software fixes discontinue their support due to the costs associated with increasingly obsolete components. Technology continues to develop, and energy sector firms must modernize capacity without the luxury of taking systems offline for thorough upgrades. The result is an energy grid where state-of-the-art systems operate side by side with legacy architecture. In many cases, this grid is fragile and prone to failure. The vulnerabilities associated with the sheer complexity of this evolving control system are legion. Recent policy developments such as Executive Order 13636 and the subsequent development of the NIST Cybersecurity Framework, as well as focused work by the Department of Energy in collaboration with the energy sector, add urgency and partial solutions to the task of securing the energy grid. However, the leadership necessary to discern problems and formulate solutions remains a key element that requires inquiry.

The GMU/IBM/NSF inquiry in fact combines two efforts; the first is focused on the development of core Chief Information Security Officer (CISO) competencies with the goal of improving cybersecurity leadership and governance. A second effort seeks to develop management strategies and policies for securing industrial control systems for the future energy industry smart grid. The two efforts are complementary, as the workshop quickly showed. The GMU/IBM/NSF team is firmly convinced that a collaborative, multi-disciplinary inquiry with participation from government, business, and academic leaders offers the richest prospects for success in both efforts. Developing new connections and collaboration between government agencies and public-private partnerships will uncover commonalities, accelerate innovation, and help to abolish bureaucracy. The technical problem, daunting in its own dimension, is merely part of the challenge. Technical problems of infrastructure systems span the government – business space and require policy adjustments, rule changes and business plans to implement. Solutions also require board level leadership to develop strategies and business plans to create, implement, and resource effective solutions. The academic community is a partner in this picture, as it must research solutions and generate the human capabilities necessary to solve problems and implement them.

A series of keynote addresses opened the day-long event, followed by panels that addressed more specific areas. Speakers included:

- Bob Brese, CIO, Department of Energy;
- Mike Kuberski, CIO, PEPCo Holdings;
- Robert Coles, CISO, GlaxoSmithKline;
- Eddie Schwartz, Vice President, Global Consulting and Cyber Solutions, Verizon;
- Richard Guidorizzi, Program Manager, DARPA;
- Annabelle Lee, Senior Technical Executive, Electric Power Research Institute;
- Jeffrey Katz, CTO, IBM Energy and Utilities ;
- Richard Klimoski, Professorand Area Chair of Management, George Mason University School of Business
- and Kevin Kerr, CISO, Oak Ridge National Laboratory.

Topic-focused breakout sessions followed in the afternoon to generate dialogue and collect ideas. Topics of the keynotes included Characteristics of a Good Chief Information Security Officer, Cybersecurity Leadership and Governance Challenges, and The Role of the CISO in the Energy Sector from both US and international perspectives. Each keynote featured a senior executive leader in the government or private sector representing the energy and utilities, telecommunications, pharmaceutical, and government

(Continued on Page 13)

[4] Jerry "Dutch" Forstater, "System Shutdown," *Homeland Security Today* 10, no. 10 (December 2013/January 2014): 18-23, available at http://www.nxtbook.com/nxtbooks/kmd/hst_201312/#/20.

(Continued from Page 12)

industries.

Supplementing the day were panel sessions and breakouts of interactive presentations and group participation. The panels allowed the group to synthesize speaker messages and probe more deeply into specific topics and included perspectives from regulators, standards bodies, national labs, information technology companies, and more.

The first panel investigated the dynamics and challenges of Chief Information Security Officer (CISO) leadership. Panel speakers and participants highlighted the human element of cyber security leadership and the unique role of C-Suite leaders in creating a culture of security within organizations. A prominent aspect of the second panel addressed the role of boards in providing governance to ensure that leaders put in place processes to protect against threats and mitigate the effects of cyber disruptions. The panel also addressed the essential role of academic institutions in providing research and a workforce with the technical capability and strategic leadership acumen to drive improvements in the cyber domain.

The second panel and breakout focused on the technology challenges of supervisory control and data acquisition (SCADA) and legacy systems operating on an increasingly interconnected grid. Led by a representative from the private sector and moderated by faculty from GMU's School of Business, the participants also explored these technical challenges in the context of a grid that must support continuous operations. In a challenge common to many infrastructure systems, power generation and transmission systems have a limited ability to "go offline" to retrofit new capabilities. Moreover, upgrades occur in stages over time, leading to cases in which upgraded control systems rely on decades old industrial control systems for mechanical monitoring and coordination. The technical workshop addressed thought processes to realize technology solutions and opened the door to business and regulatory challenges that require solution.

The final discussion addressed topics of leadership at executive levels in the cyber domain. An international partner led this panel, with a moderator from the GMU Center for Infrastructure Protection and Homeland Security. This panel extended the inquiry of senior leadership and addressed the intersection between leadership in the private sector and government at all levels. The tightly regulated nature of the energy grid presents unique problems in the area of metrics, information sharing, and policy development. In particular, there is a natural reluctance of private firms to share vulnerability information with industry regulators. The role of industry associations, sector coordination councils, and information sharing and analysis centers (ISACs) each became topics of discussion for the roles they play in sharing information about threats, vulnerabilities, and solutions. Recent initiatives to share classified information in a timely and relevant form with the private sector also received in-depth discussion. The group addressed practical approaches to sharing information and the role of leaders in creating the trust necessary for information exchange. As with the CISO leadership panel, this forum addressed the essential role of the academic sector to provide workforce members and leaders at all levels with the skills and competence essential to improve security in the cyber domain.

The day's events yielded a trove of information presently undergoing refinement and synthesis. The goal of the GMU/IBM/NSF effort is to complete a comprehensive report early next year and conduct a follow-up conference in April 2015 to discuss findings. Definitive findings are in development, but a few broad themes are already evident from this unique forum.

First, there is clearly an essential human element to cybersecurity leadership, especially in complex systems that touch broad populations and impact other infrastructure sectors. Threats are dynamic, and complex systems abound in the energy sector. Critical thinking and innovative solutions, while always important, are even more vital attributes in the pursuit of cybersecurity and critical infrastructure resilience.

Second, distributed control architecture and the imperative to upgrade systems in place while in near-continuous operation bring special technical and leadership challenges. While some

(Continued on Page 14)

(Continued from Page 13)

of these challenges are specific to the energy sector, there are common approaches that apply to other complex and distributed infrastructure systems. Solutions that evolve over time, adaptive capacity, and resilience built from the point of design are important considerations. Lifelong learning, always a vital leadership attribute, is more important in an environment of constantly evolving threats and technological change.

Finally, there is a need for broad competence combined with sector-specific expertise to solve the complex security and operational challenges manifest in interconnected infrastructure systems. The requirement for professionals with the ability to understand technical challenges and grasp the interdisciplinary, international, and industry-government perspectives of threats and vulnerabilities is essential. These leadership competencies will grow in importance as systems become more complex.

The GMU/IBM/NSF Cybersecurity Research Workshop is an example of the practical, solutions-based inquiry that a public- private partnership of experts can conduct through collaboration. For the complex challenges of interdependent systems, a collaborative and multidisciplinary approach offers rich promise to find solutions and develop essential leadership capabilities. Nowhere is the need for collaboration greater than in the intersection between cyber and physical infrastructure systems found in the energy sector. *The CIP Report* will feature a follow-up article in a future volume that will provide a full report of findings. There is further need for the technical-, policy-, and leadership focused research to solve the complex problems of an interdependent world. For more information, please contact Jean-Pierre Auffret, Angelos Stavrou, and Mark Troutman at GMU or Jane Snowdon at IBM. ❖

**Dr. Mark Troutman is the Associate Director of the Center for Infrastructure Protection and Homeland Security. Jean-Pierre Auffret is the Director of Executive Degree Programs for George Mason University's School of Business.*

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University 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