THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

FEBRUARY 2015
CYBERSECURITY

VOLUME 14 NUMBER 5

EDITORIAL STAFF

EDITOR
Christie Jones
Tehreem Saifey
Dennis Pitman

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

This month, our authors discuss aspects of **Cybersecurity** as the NIST Cybersecurity Framework approaches its one year anniversary.

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

First, Mykhaylo Bulyk, Dr. William Horsthemke and Dr. Nathaniel Evans of the Argonne National Laboratory present an overview of offensive cybersecurity in the NIST Cybersecurity framework. George R. Cotter, a retired career cryptologist at the NSA, then discusses a case study on cybersecurity for critical infrastructure protection for the NIST Cybersecurity Framework. Next, Danilo D'Elia, a Ph.D candidate at the University of Paris VIII Saint-Denis and research associate at *Chaire Castex de Cyberstrategie* (Paris), examines the public-private partnership angle from the French experience on critical infrastructure protection.

Parham Eftekhari, Co-Founder and Sr. Fellow, Institute for Critical Infrastructure Technology (ICIT) and Marjorie V. Perry, Director, Cybersecurity Education and Training, Covenant Security Solutions, Inc. highlight the necessity to change the attitudes towards security awareness to protect critical national infrastructures. Finally, Dennis Pitman, Research Assistant at the Center for Infrastructure Protection and Homeland Security (CIP/HS), gives an overview of recent and potential upcoming cybersecurity initiatives from Congress and the White House.

In October's CIP Report, we provided an early overview of the Mason - IBM - NSF Cybersecurity Research Workshop that took place on July 11, 2014. I'm pleased to report that the workshop report "*Cybersecurity and Smart Grid Leadership*" from that very informative event is now available. You can access and download the conference report at this link: http://goo.gl/xuMmYb. Findings from all aspects of the projects will be unveiled and vetted at the Mason-IBM-NSF Cybersecurity Leadership and Smart Grid Conference on April 30, 2015 at Hyatt Fair Lakes in Fairfax, Virginia. The URL for the registration information for that conference is: http://goo.gl/v4zq97

We would like to take this opportunity to thank this month's contributors. We truly appreciate your valuable insight. We hope you find this issue of The CIP Report useful and informative. We are thankful for your support and the rich dialogue that follows each topic.

Best Regards,

Mark Troutman, PhD
Director, Center for Infrastructure Protection and Homeland Security (CIP/HS)

Offensive Cybersecurity in the NIST Cybersecurity Framework

by Mykhaylo Bulyk, Dr. William Horsthemke, and Dr. Nathaniel Evans*

Introduction

Government and corporate computer systems are *attacked*, networks are *penetrated* by hackers, and enterprises are protected by *demilitarized* zones.[1] Language that until recently was used to describe security and warfare in military settings has now become commonplace in cybersecurity discussions. The concepts of pre-emptive attack, counterattack, and offensive defense fit the linguistic cultural thread of security in cyberspace, at least in part due to the taxonomy adopted by cybersecurity as a discipline.

Military-style taxonomy[2] forces a narrative in the cybersecurity discipline that continues to be related to the topic of warfare. One such example is an increased use of the concept of offensive defense. Offensive defense refers to a call for corporations, small businesses, and government agencies to conduct offensive computer or network operations in response to, and preemptively against, the hackers who have attacked organizations' information technology assets.[3] In some cases, collective cyber-offense capability can yield results beneficial to many. For example, a public-private partnership between Microsoft, the Federal Bureau of Investigations (FBI), and European law enforcement limited the functionality of a botnet[4] composed of two million machines distributing malware. However, when viewed from the limited legal and technical capability of small- to medium-sized companies, neither the response of offensive operations nor tolerance for hacking back is likely to be encouraged or effective.

The viability of offensive techniques as tools in a cybersecurity toolbox is hotly debated across all sectors of the American economy exposed to hacking. Offensive capability as applied in the military warfare setting, where a powerful kinetic capability—a power in and of itself capable of changing tactical, operational, and strategic calculus for the enemy—proves itself as a deterrent is contrasted with application of a deterrent in cyberspace, where outcomes are less clear. In the United States military, several weapon systems are able to influence enemies without firing a shot: the F22 Raptor[5] air superiority fighter; the Aircraft Carrier Group[6] naval power projection capability; and Army and Marines full-force military exercises.[7] Unfortunately, a similarly powerful deterrent capability is not yet practical in cyberspace.

Although it is possible to turn off all active critical electronic devices by detonating a nuclear device and generating an electro-magnetic

(Continued on Page 3)

---

[1] "Identity Theft Resource Center Breach Report Hits Record High in 2014," *Identity Theft Resource Center* (January 12, 2015), accessed January 26, 2015, http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html.

[2] Eduard Hovy and David Klaper, "A Taxonomy and a Knowledge Portal for Cybersecurity," Paper presented at *dg.o '14 Proceedings of the 15th Annual International Conference on Digital Government Research*, June 18–21, 2014, accessed January 26, 2015, http://www.cs.cmu.edu/~hovy/papers/14dgo-cybersecurity-taxonomy.pdf.

[3] Michael Riley and Jordan Robertson, "FBI Investigating Whether Companies Are Engaged in Revenge Hacking," *Bloomberg Business* (December 30, 2014), accessed January 26, 2015, http://www.bloomberg.com/news/2014-12-30/fbi-probes-if-banks-hacked-back-as-firms-mull-offensives.html.

[4] Brian Donohue, "Microsoft and Friends Take Down ZeroAccess Botnet," *Threat Post* (December 6, 2013), accessed January 28, 2015, http://threatpost.com/microsoft-and-friends-take-down-zeroaccess-botnet/103122.

[5] Rebecca Grant, "Global Deterrence: The Role of the F-22," *Lexington Institute* (February 6, 2009), accessed January 26, 2015, http://www.lexingtoninstitute.org/global-deterrence-the-role-of-the-f-22/.

[6] "AIRCRAFT CARRIERS – CVN," *United States Navy Fact File* (October 16, 2014), accessed January 26, 2015, http://www.navy.mil/navydata/fact_display.asp?cid=4200&tid=200&ct=4.

(Continued from Page 2)

pulse,[8] nuclear capabilities are not part of a cybersecurity defense toolkit. Instead, all levels of organizations within the United States are left to find an attainable capability that can effectively and practically protect their intellectual property, sensitive business plans, and other critical operational and business information.

Cybersecurity Framework Description

Publication of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (the NIST Framework) offers a formal risk-based model for addressing cybersecurity. The NIST Framework is the result of collaboration between the government and private sectors. It standardizes the language used in managing cybersecurity risk and provides recommendations on best practices in improving the security and resilience of critical infrastructure.[9] The Framework provides a foundation that helps companies understand the tools, capabilities, processes, and procedures within the cybersecurity discipline.

Offensive defense discourse is at the forefront of the discussion within the cybersecurity community, mainly as a result of recent highly publicized hacking events including the Target breach,[10] Home Depot point-of-sale hacking,[11] JP Morgan Chase intrusion,[12] and Sony Pictures Entertainment hack.[13] As a consequence of these incidents, elevated media coverage has yielded an increased interest in cybersecurity. Fortunately, the NIST Framework is available to help organizations establish or improve their cybersecurity postures.

The NIST Framework provides an effective process designed to help companies develop a methodical approach for their cybersecurity capability through identifying, assessing, and responding to risk. Components of the Framework include the Framework Core, Framework Implementation Tiers, and Framework Profiles. The Framework Core consists of five concurrent functions: Identify, Protect, Detect, Respond, and Recover.[14] A short description of guidance presented by each function follows:

- Identify – business context, processes, critical assets
- Protect – logical and physical access, personnel, systems, data
- Detect – cybersecurity events, anomalies, processes, incidents
- Respond – critical assets, processes, personnel, data
- Recover – data, business function, trust

The functions provide a path for a given organization to develop and implement or improve its cybersecurity capability. To implement the Core Functions, the NIST Framework defines the Implementation Tiers presented as described below:

- Tier 1 (Partial) – limited awareness of cybersecurity risk

- Tier 2 (Risk Informed) – aware of cybersecurity risk
- Tier 3 (Repeatable) – active participation in collaborative risk management activities
- Tier 4 (Adaptive) – adaptive to the cybersecurity risks

The Framework Profile is informed

(Continued on Page 4)

---

[7] Michael S. Gerson, "Conventional Deterrence in the Second Nuclear Age," *Parameters 39* (Autumn 2009), accessed January 26, 2015, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/09autumn/gerson.pdf.

[8] Larry Bell, "The Ultimate North Korean Missile Threat to America: A Nuke Power Grid Attack," *Forbes* (April 14, 2013), accessed January 28, 2015, http://www.forbes.com/sites/larrybell/2013/04/14/the-ultimate-north-korean-missile-threat-to-america-a-nuke-power-grid-attack.

[9] National Institute of Standard and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity* ("Cybersecurity Framework"), (Washington, D.C.: NIST, 2014), accessed January 26, 2015, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[10] Rachel Abrams, "Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop," *The New York Times* (August 5, 2014), accessed January 26, 2015, http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=0.

[11] Shelly Banjo, "Home Depot Hackers Exposed 53 Million Email Addresses," *The Wall Street Journal* (November 6, 2014), accessed January 26, 2015, http://www.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282.

[12] Michael Corkery et al., "Neglected Server Provided Entry for JPMorgan Hackers," *The New York Times* (December 22, 2014), accessed January 26, 2015, http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified.

[13] "A Breakdown and Analysis of the December, 2014 Sony Hack," *Risk Based Security* (January 12, 2015), accessed January 26, 2015, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#celebritygossipandhackingback.

[14] NIST, *Cybersecurity Framework.*

(Continued from Page 3)

by the Implementation Tiers. For management awareness, an organization's profile can be compared to that of other organizations in similar economic sectors. An organization can also set its current profile as a baseline in an attempt to improve its cybersecurity posture in the future.

Offensive Defense

Applying a scenario across the NIST Framework is a useful way to understand how this framework would apply to a particular organization. Generally, a hypothetical cybersecurity incident is a good exercise to test the NIST Framework: assume a malicious actor was able to gain access to the organization's internal networks with the intent to find and exfiltrate valuable proprietary data. In this case, an incident may be identified by a system's user noticing the loss of data integrity or detected by a continuous incident monitoring solution on the network. The incident is passed on to the cybersecurity personnel for response and investigation. If the investigation reveals a serious and significant breach, the scope of the response is increased and recovery operations begin. While the investigation is continuing and recovery is ongoing, the personnel involved in triage may recommend an offensive response to stop an ongoing attack.

Given the context of the NIST Cybersecurity Framework, any organization with a Framework Profile informed by the Framework Implementation Tiers 1–3 would not be capable of properly detecting or identifying an incident. Moreover, accurate response and recovery are not likely to be expedient or conclusive. The high-profile hacking incidents mentioned earlier (e.g., the Target breach, the JP Morgan Chase intrusion, or the Sony Pictures Entertainment hack) all targeted corporations with active cybersecurity teams performing 24/7 monitoring. All of them are, arguably, Tier 4 organizations; however, investigations of the incidents took months to complete.

Offensive response to a hack should require considerable evidence and the investigative capacity to find conclusive evidence attributing the attack's origins. Because this is time-consuming and expensive, perhaps an alternative should be considered. Offensive cybersecurity capability should inform organization's defensive measures as an assessment capability for the organization's Core Functions. For example, cybersecurity assessment tools such as the Department of Homeland Security's Cyber Infrastructure Survey Tool or Cyber Resilience Review are designed to ask organizations a series of questions on protective and resilience measures to help evaluate the processes of the organization's cybersecurity risk management. In addition, an active penetration test can exercise the organization's Core Functions in the operational setting by performing an attack against the organization's physical and information technology systems. Together, the results of these tests can form a comprehensive offensive security assessment.

Penetration testing identifies vulnerabilities within a particular system or network that has security measures in place. As an offensive capability, penetration tests are conducted by trusted agents who emulate the techniques used by the malicious intruders[15] in an attempt to understand the vulnerabilities within a system. More broadly, however, penetration testing can expose limitations within an organization's cybersecurity program, especially when conducted as part of a comprehensive offensive security assessment. Placed in the context of the NIST Framework, offensive cybersecurity testing will inform an organization about (1) the level of its Implementation Tier; (2) effectiveness of the Core Functions; (3) in-place protective capability; (4) the detection and monitoring capability deployed on the networks; and (5) real-world response and recovery decisions and planning.

Finally, offensive security testing will result in increased resilience to malicious and incidental disruptions. By identifying critical cyber-systems in an organization's infrastructure, managers will be able to prioritize cybersecurity resources and reassess funding for a given cybersecurity infrastructure—if a system that is vital to the organization's business continuity is constantly tested, but is always found to be vulnerable, perhaps

(Continued on Page 5)

[15] Chan Tuck Wai, "Conducting a Penetration Test on an Organization," *SANS Institute InfoSec Reading Room* (2002), accessed January 26, 2015, http://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67.

(Continued from Page 4)

different defensive means should be introduced such as Moving Target Defense (MTD), network segmentation, two-factor authentication, and data-loss prevention.

Conclusion

The NIST Cybersecurity Framework recommends internal assessment measures such as testing the Protect and Detect Core Functions for relevancy and effectiveness.[16] However, this recommendation should also encompass other Core Functions (Identify, Respond, and Recover) as a measure of validation for the organizations adopting the Framework. Moreover, proper cybersecurity assessment requires a holistic and systemic approach, covering and identifying critical cyber-systems and cybersecurity assets while evaluating organization's risk management process; penetration testing is an inherent component of such assessments. Penetration testing as a component of offensive security exposes practical vulnerabilities in an organization's security infrastructure and helps prioritize management decisions by increasing the understanding of potential consequences to variety of cybersecurity events. Although it is very difficult for companies to mount a "hack-back" attack, it is easier and more effective for organizations to target their own systems using offensive techniques. This will allow them to benefit greatly in terms of a resilient and effective cybersecurity programs.

Acknowledgment

The work presented in this paper was partially supported by Argonne National Laboratory under U.S. Department of Energy (DOE) contract number DE-AC02-06CH11357. The submitted manuscript has been created by UChicago Argonne, LLC, operator of Argonne National Laboratory. Argonne, a DOE 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.

* *Mykhaylo Bulyk, Dr. William Horsthemke, and Dr. Nathaniel Evans work with the Risk and Science Infrastructure Center at Argonne National Laboratory.*❖

[16] NIST, Cybersecurity Framework.

A Case Study for the NIST Cybersecurity Framework – How Successful Has It Been in Broadly Underpinning Critical Infrastructure Protection Programs?

by George R. Cotter*

Background

Two years ago, the Administration, Congress, and critical industries were locked in a stalemate on cybersecurity for critical infrastructure protection. There was little agreement between the Administration and the Congress on the important actions that would significantly improve protection of the nation's most critical infrastructures, such as the electric grid. Critical industries could not adequately protect themselves but did not want mandatory regulation, only improved threat information from the federal government. The financial industry was under near-constant cyber-attack, which threat information would not adequately prevent. Instead of trying to block 100 percent of cyber-attacks, electric utilities had decided on a "resilience strategy" of recovering once attacks occurred; Hurricane Sandy showed that a parallel "resilience strategy" for extreme weather events was mostly a public relations strategy. Privacy advocates reflexively challenged almost all security initiatives.

The regulatory stalemate over cybersecurity left an overriding policy question unaddressed—the extent to which the private sector needs federal intervention or mandatory regulation. For the vitally important electric utility sector, lingering gaps in cybersecurity may not leave the nation with a second chance.

With little expectation that gridlock for cybersecurity legislation could be overcome, the President issued Executive Order (EO) 13636 in February 2013.[1] The EO tasked federal departments and agencies with initiatives that could be undertaken without legislation. A cornerstone of the EO was a directive to the National Institute of Standards and Technology (NIST) to develop, cooperatively with industry, a generalized cybersecurity Framework that could be voluntarily used by most organizations. Core requirements included consensus standards, industry best practices, prioritized cost-effective security measures, controls to manage risk, identification of cross-sector standards, and inclusion of methodologies to mitigate adverse effects on business confidentiality, individual privacy, and civil liberties.

Development of the Framework

NIST issued a call to industry for cooperative development of the Framework and hosted a series of workshops throughout 2013, completing a 41-page Framework on schedule, one year after the EO.[2] The Framework substantially complied with the EO tasking, supporting organizations wishing to increase their security posture. However, the Framework is not a "Roadmap" and is not a set of "Standards." Instead, the utility of the Framework lies in its contribution to voluntary development of a structured cybersecurity program.

The Framework has three major components; the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The top level of the Core is composed of five functions: Identify, Protect, Detect, Respond and Recover. These functions are further defined in terms of Categories and Sub-Categories. The Core is, in fact, an incidence response system; the framers basically acknowledged that a successful cybersecurity program must include the ability to recover from an attack. Framework Profiles flesh out the Core categories and subcategories, defining the set of baseline activities an organization is using (the Current Profile) and the desired capabilities the organization would like to achieve (the Target Profile). This permits, in theory, a gap analysis which

(Continued on Page 7)

[1] Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739 (Feb. 19, 2013).
[2] National Institute of Standard and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework")," February 12, (Washington, D.C.: NIST, 2014), accessed January 26, 2015, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

(Continued from Page 6)

could lead to a tiered implementation for cybersecurity protection.

The Framework acknowledges its generality and clearly articulates the importance of domain-specific analysis at each stage of implementation. Sound business decisions, risk management, and assessment of resources available are required. The Framework states:

> "To ensure extensibility and enable technical innovation, the Framework is technology neutral. The Framework relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience."

Good implementation of the Framework depends on organizational and domain processes to take the Framework beyond its skeleton form. Practitioners need to develop their own "Roadmap," with appropriate technical and architectural structure. Importantly, industries such as electric utilities would still need to develop cybersecurity "Standards" upon which compliance can be measured. Until these essential steps occur, the Framework is hardly more than "Cybersecurity 101."

Implementation of the Framework for Electric Utilities

The Administration initiated the Framework because private industry had failed to develop sufficient structured approaches to cybersecurity for critical infrastructure. The U.S. Government has categorized critical infrastructure into 16 sectors—for example, the energy sector which contains the electric grid. For the nation's electric grid there are not one, but two regulatory agencies—the Federal Energy Regulatory Commission (FERC) and the Nuclear Regulatory Commission (NRC). While FERC regulates interstate power transmission, both agencies regulate generation of power.

Another overlapping agency confuses lines of cybersecurity authority even more. A sector-specific organization—the U.S. Department of Energy (DOE)—is responsible under EO 13636 to work cooperatively (and voluntarily) with the electric utility industry. DOE is tasked with extending the Framework into implementation. Over the past several years, DOE has developed or identified a number of major tools to create what should be a highly cyber-secure national electric grid, specifically:

1. The Electricity Subsector Risk Management Process Guideline, 2012[3]
2. Guidelines for Smart Grid Cyber Security, IR 7628, 2010[4]
3. NERC's Critical Infrastructure Protection (CIP) Standards v3 (v5 by 2017)[5]
4. Cybersecurity Capability Maturity Model (C2M2) 2014[6]
5. Energy Sector Cybersecurity Framework Implementation Guidance, Jan. 2015[7]

How well is this voluntary industry-federal partnership working relative to the NIST Framework, given the Framework's intent of effective cybersecurity protection for critical infrastructure? The short answer is: not well at all.

(Continued on Page 8)

---

[3] U.S. Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process*, DOE/OE-0003 (Washington, D.C.: DOE, 2012), available at http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf.

[4] Smart Grid Interoperability Panel, *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security* (Washington, D.C.; National Institute of Standards and Technology, 2010), available at http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf.

[5] See (a) North American Electric Reliability Corporation (NERC), Cyber Security Reliability Standards CIP V5 Transition Guidance (Atlanta: NERC, 2014), available at http://www.nerc.com/pa/CI/Documents/V3-V5%20Transition%20Guidance%20FINAL.pdf; (b) NERC, *Implementation Plan for Version 5 Cyber Security Standards* (Atlanta: NERC, 2012), available at http://www.nerc.com/pa/Stand/CIP00251RD/Implementation_Plan_clean_4_(2012-1024-1352).pdf; and (c) pending CIP Revision 5 NERC filings, approved by the NERC Board of Trustees in Nov. 2014, to be filed with FERC, Feb. 2015, including updates of CIP-002, 003, 004, 007, 009, 010, and 011. See nerc.com for updates as issued.

[6] U.S. Department of Energy and U.S. Department of Homeland Security, Cybersecurity Capability Maturity Model (C2M2), Version 1.1 (Washington, D.C.; DOE/DHS, 2014), available at http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

[7] Department of Energy, *Energy Sector Cybersecurity Framework Implementation Guidance* (Washington, D.C.; DOE, 2015), available at http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

(Continued from Page 7)

The Problem is Not the Framework, It's the Builders' Failure to Use the Framework.

The electric grid is the lifeblood of the nation's civil, social, business, industrial, and national security systems. The grid cannot be allowed to fail. Our nation's adversaries see this vulnerability and have identified the grid as a high priority target. And adversaries take steps to operationalize their bad intent—in recent testimony before the House Permanent Select Committee for Intelligence, Admiral Mike Rogers, Director of the National Security Agency and, Commander of U.S. Cyber Command, confirmed that Chinese malware, and several other nations' malware, has been planted, at a minimum, in human-machine interfaces to control systems for the electric grid.

The electric utility industry persists in its self-deceptive fiction that the grid is resilient enough to survive cyberattack, even by the most capable adversary. As a result, major vulnerabilities are left unprotected. For example, communications between control centers and transformer substations are often left unencrypted and therefore unprotected. Exacerbating the vulnerability, electric utilities are increasingly using cheap internet communications for control purposes. But these same internet communications provide attack portals for cyber-adversaries.

Under the current regulatory structure, cybersecurity standard-setting for the electric grid has been delegated by FERC to a private self-regulatory organization, the North American Electric Reliability Corporation (NERC). NERC has successfully resisted technically-meaningful standards for protection. Instead, NERC standards depend on paperwork compliance rather than tangible technical protection.

Both FERC and NERC have failed to implement specific provisions of the Energy Policy Act of 2005. In an unusually specific provision, Congress required cybersecurity protection for "communications networks." FERC's technical staff and Commissioners understand the law's requirements but have failed, for over nine years, to require NERC to develop a compliant standard.

NERC's persistent refusal to secure grid communications is apparently motivated by the common money-saving practice of using commercial telecommunications, including the internet, that are not "owned" by grid operators. More responsible users of commercial networks execute contracts with carriers assuring reliability and security; for example, when the Department of Defense and intelligence community use commercial carriers, a number of security enhancements are added, including encryption of communication links.

Securing communication networks is the only practical solution to the inherent vulnerability of hundreds of thousands of industrial control systems (ICS) that control grid operations. Already, internet search engines find thousands of unsecured and vulnerable control systems. More sophisticated attacks being developed will exploit the myriad of internet-based portals used by the electric utility industry for business, management, and control. These attacks which will not be simple Distributed Denial of Service (DDOS) attacks but more subtle and complex operations that will destabilize the industry's unwise "resilience strategy."

For the electric utility industry and their captive standard-setting body, NERC, protection of the nation and the public are not foremost priorities. Instead, their priorities are cost containment, avoidance of financial liability, and minimizing regulatory oversight. With hundreds of utilities involved in the standard-setting process, the industry does not rationally protect itself and the public. Instead, decision-making devolves to the lowest common denominator—forestalling federal authorities from mandating effective cybersecurity protections. And in the event of a cyberattack, industry can always blame federal authorities for failure to give adequate warning or prevent attacks, or even to set mandatory cybersecurity standards in the first place.

Gaps in cybersecurity standards for the electric utility industry are characteristic of the overall standards development process at NERC, including standards for physical protection and solar storm protection. Standards rely on self-devised paper plans rather than concrete protection measures. Whole categories of critical facili-

(Continued on Page 9)

(Continued from Page 8)

ties are exempted. External review and approval of protective plans is minimized.

Let us return to actions at DOE, the coordinator for voluntary implementation of the NIST Framework for the electric utilities. Has all of this escaped the DOE's understanding of threats and vulnerabilities? Hardly. The tools and guidance documents preach motherhood; but in most cases, carefully circumscribe deep technical issues. DOE's recently issued C2M2 tool rigorously links to NIST's compendium of security control features. Yet DOE is well-aware that NERC has steadily refused to adopt the NIST standards. DOE is also well-aware that NERC has not adopted the Framework, makes no reference to it in its industry guidance, and places no value on it in the NERC cybersecurity standards agenda. Does the NIST Framework have real utility?

For companies and industries that are searching for a voluntary means to cybersecurity, the Framework clearly has utility in informing organizations on how to structure an effective cybersecurity program. But for industry sectors that put their business strategies ahead of the public interest, the Framework leaves glaring cybersecurity gaps. As this case study of the electric utility industry shows, the NIST Framework shows the way forward, but does not guarantee protection of the nation and the public from cyberattacks on critical infrastructure.

Acknowledgement

The author thanks W. R. Harris and T. S. Popik of the Foundation for Resilient Societies for editorial suggestions and click-through references.

**George Cotter is a career Cryptologist who retired from NSA in 2009 with over 60 years of service. He is a member of the National Academy of Engineering and has extensive experience on Cybersecurity technical issues. Since his retirement he has focused on Critical Infrastructure Protection, particularly the Energy field.* ❖

The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policy-makers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in information infrastructure protection. Following the success of the first eight conferences, the Ninth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection will again provide a forum for presenting original, unpublished research results and innovative ideas related to all aspects of critical infrastructure protection. The conference, which will be held at SRI International in Arlington, Virginia on March 16-18, 2015, will be limited to sixty participants to facilitate interactions among attendees and intense discussions of research and implementation issues. Information about the conference and IFIP Working Group 11.10 on Critical Infrastructure Protection and its activities is available at www.ifip1110.org.

Public-Private Partnership: The Missing Factor in the Resilience Equation - The French Experience on CIIP

by Danilo D'Elia*

Introduction

For many years, information security has been the exclusive domain of a closed community of people from military, academics and IT companies. The information revolution in the 90s radically changed the scale and the nature of the issue. With the massive penetration of digital information and communication technology (ICT) in all advanced economies, people and engineered machines are now part of the same global environment made of information: the *infosphere*. Moreover, due to the deregulation process of many public sectors in the 80s and the globalization of 90s, the private sector now owns the majority of critical infrastructures, including information networks, and is at the core of the ICT expertise. Therefore, this revolution brings the problem of Critical Information Infrastructure Protection (CIIP) beyond traditional national defense circles and the terms of the political debate around CIIP are now focusing on a main point: the cooperation between public authorities and the private sector is needed to enhance resilience, but its implementation is hard to achieve.

A Schizophrenic State No Longer at the Centre of the Security Realm

While cooperation is needed and obvious for both the public and private actors, determining how to organize the relationship presents a complex problem due to a conjunction of factors acting on several layers.

First of all, behind the oversimplified categories of public and private, various actors with conflicting representation and interests interface with each other. On the private side the players include infrastructure operators, maintenance firms, incident command system (ICS) providers and security companies. With the emergence of the CIIP issue, a main divergence appeared: the different culture between IT security (protection against intentional damages) and safety of operational technology, OT (protection against accidental events). Historically, confidentiality is not the main consideration in OT systems, and availability and integrity are by far the dominant concerns. On the other hand, OT systems frequently have little or no intrinsic security behavior. Although Stuxnet and recent events have encouraged ICS vendors to improve the security of their systems, some are only moving slowly, and many legacy systems will continue in service for many years with little or no built-in security due to the long life cycles of OT systems when compared to IT systems.

On the public side also, the presence of various players generates a fragmentation of the role of public sector: national intelligence, law enforcement, defense, emergency management, health services and first responders. Thus, four major challenge are undermining the implementation of PPP: unclear delineation of roles and responsibilities of players, lack of trust between partners, different languages (technological vs. bureaucratic), diverging interests (security vs. corporate benefits), and misplaced expectations (national security vs. multinational availability).[2]

Moreover, protecting against cyber threats has led to a contradictory practice and has revealed the schizophrenic conduct of national security authorities. In many countries,

(Continued on Page 11)

[1] This publication is a short version of the article presented at the CRITIS Conference 2014: the full-length article is forthcoming for Springer edition 2015.

[2] Myriam Dunn Cavelty and Manuel Suter, "The Art of CIIP Strategy, Taking Stock of Content and Processes," in *Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense*, ed. Javier Lopez, Roberto Setola, Stephen Wolthusen (New York: Springer, 2012), 15-38.

(Continued from Page 10)

intelligence services and defense agencies are developing offensive capabilities for security interests. To achieve that, they exploit vulnerabilities in current operating systems and hardware or contribute to new vulnerabilities in widespread encryption systems. This situation makes the risk assessment more complex: backdoors could be identified and exploited by malicious actors and thus reduce the resilience of the entire system.

Therefore the dialogue is inherently difficult. In accordance with the development of a comprehensive risk analysis, we argue time has come to define PPP through a new ethos. As do the technical security solutions and the insurance policies, PPP should be approached as a variable of the resilience equation and a risk mitigating factor.

The French Feedback Loop Process and Its Limits

In accordance with the objective to become a world power in cyber defense, France has launched numerous initiatives to ensure CIIP. Table 1 summarizes the main moves and highlights the global impact on cyber risk. If viewed broadly, these initiatives enable the move

FRENCH CYBER RESILIENCE EQUATION			
Domain	*Initiative*	*Description*	*Influencing*
Security standard	Working group on ICS security	Working group established by ANSSI (national authority on cyber security) and bringing together all the stakeholders involved in CIIP. Focusing on : security standard, risk management and trusted solutions.	Countermeasures Vulnerability Impacts
	Military Programme Act 2014-2019 article 22	Security Standards and legal measures to be imposed to CIs: mandatory cartography of the critical information systems; mandatory and regular audits of information systems and networks; mandatory declaration of cyber incidents; implementation of certified sensors.	Countermeasures Threats Impacts
Education & Training	French Centre of excellence for fight against cyber crime	The Centre is a PPP focusing on training and involving four companies (CEIS, Microsoft, Orange, Thales) three universities and the Gendarmerie.	Impacts Vulnerability
	Cyberdefence Cluster	Private company from telecom sector as well as from security and defense will jointly cooperate with the main research laboratories and MoD agencies in promoting innovation and training the future experts.	Countermeasures Vulnerability
	Chaire Thales Cyber defense	Research Program founded by private sector (Thales&Sogeti) in cooperation with the MoD. Focusing on cyber defense and developing courses and training for military.	Vulnerability
Awareness	Network of cyberdefence reservists	Network of reservist made up of about 100 citizens helping in raising awareness, debating and suggesting, organising and establishing events that contribute to making cyberdefence a national priority.	Vulnerability
	Awareness campaign led by DCRI	In 2012 the Central Directorate of Interior Intelligence (DCRI-Ministry of the Interior) lunched an awareness campaign on cyber risk targeting CIs employees and managers.	Vulnerability
	Chaire Airbus Cyber stategy	Research centre founded by Airbus Foundation in cooperation with and the Institute of Advanced Studies in National Defence . Focusing on geopolitics of cyber security and aiming to create a national community of researchers on cyber security issues.	Vulnerability
Trusted solutions	Industrial Cyber Plan	ANSSI is in charge to release a road map in order to boost the national cyber industrial base. The aim is to develop a sovereign industrial ecosystem and to develop a strategy in cooperation with the private sector.	Countermeasures
Information Sharing	Club des Directeurs de Sécurité des Entreprises	French Club of Security Managers is a non-profit organisation allowing CIOs, risk manager to meet, work and exchange information.	Threats
	CERT FR	French government CSIRT. As such, CERT-FR is the point of contact for all computer-related security incidents regarding France.	Vulnerability
Exercise	Piranet	Part of a series of national level crisis management exercises organised by the SGDSN. Tha aim is to test the crisis prevention and management plans. More than 500 public & private participants.	Impacts

(Continued on Page 12)

(Continued from Page 11)

from a supposed high-level of risk (A) to a low-level of risk (B) and thus reducing the severity. In France the CIIP is historically organized as a cross-ministerial issue and the operators, according to the legal umbrella called *SAIV Framework (Secteurs d'activité d'importance vitale)*, bear the financial and operational burden. Due to space constraints, a complete analysis of moves cannot be covered at much length, thus we selected a critical initiative on the field of the PPP: the SCADA working group.

Bridging the Gap between National Security and Operational Life of CIs

In 2009, a specialized agency in charge of the defense against cyber threat (French Network and Information Security Agency-ANSSI) was established and the strengthening of CIIP was defined as a major objective of cyber security strategy. Nevertheless, over the last years, several major attacks were disclosed and thus the 2013 White Paper on Defense and National Security defined cybersecurity as an element of national sovereignty and the government imposed additional constraints to CIs.[3]

The ongoing evolution of the SAIV framework shows that the traditional role of public authorities as rulemaker is still essential. On the other hand, the CIIP has to be thought as an adaptive process: standards are continually being established and updated, thus regulation needs to be reviewed over time to try to fit with new risks. However, due to the features of ICT environment, evolving much faster than the standard setting process, regulation could be only a stopgap and is not a silver bullet solution.

Here the PPPs play their crucial role: despite the enforcement of new standards, the public authorities defined the situation as unsatisfactory. Thus the second step of French strategy was the identification of the missing bricks in order to better mitigate the risk.

Particularly ICS security was identified as a main concern, thus ANSSI conducted a series of interviews in 2010 with CI operators, security suppliers and ICS vendors. The goal was to draw a shared understanding of the limits of the current security infrastructure, where best practices were to be found and the need of future requirements. In that way, the national authorities aim at establishing new standards and in parallel working with the industry to offer tailored solution for CIs.

However, the differences of language and culture emerged again.[4] In 2011, ANSSI was aware of that and created a department fully dedicated to foster cooperation with CIs. In addition, a permanent exchange platform (SCADA Working Group) was established with the main stakeholders from government (ANSSI and MoD) and industry (SCADA providers, national CIs and security suppliers) to establish best practices on supply chain risk management.

In parallel, a twofold initiative has been launched. The certification process, led by ANSSI, for the rating audit companies as independent evaluators states how well CIs have implemented the new framework. In addition, the standardization process refers also to trusted solutions and vendors. As showed by the Snowden affairs, a strong domestic ICT industrial base is a strategic advantage in cyber conflicts. The knowledge of software or hardware vulnerabilities could be exploited for both espionage and sabotage. ANSSI is promoting and leading the development of trusted suppliers by the accreditation process through the on-the-field expertise acquired through incident response and recovery.

These moves stress how cyber risk depends on so many variables that public and private players can impact only through a coordinated approach. The first important achievement is the mutual understanding of various interests and thus the convergence of opinions in adopting minimum security standards. In doing that, the SCADA WG reduces the gap between the

(Continued on Page 13)

[3] Military Programme Act 2014-2019 article 22, available at http://www.senat.fr/leg/pjl13-196.html. The measures include: mandatory cartography of the critical information systems, mandatory audits of information systems and networks by certified third parties; mandatory declaration of cyber incidents; implementation of certified sensors; more power to State authorities in order to take exceptional measures in case of a serious crisis.

[4] Stephane Meynet and Mathieu Feuillet, "SCADA/ICS Security ANSSI Working Group," Presentation made at the CESAR Conference 2013 (20 November 2013).

(Continued from Page 12)

government's lack of a technological path and the CIs' lack of a security path and contributes to better assess future needs for CIs. The outcomes of these initiatives could directly impact the risk factors, elaborating the secure design of new ICS leads to reduce the technical vulnerabilities. On the other hand, the implementation of trusted products, such as the detection sensors, generates more countermeasures and a broader view of frequency and gravity of cyber attacks.

In that sense, the process launched in 2010 is a first important step to organize the public-private dialogue. However, a more in-depth analysis reveals important tensions that might be potentially damaging the implementation of the dialogue. On the private side, increasing critics have been heard condemning the regulatory-based approach without taking the market drivers into account. The primary interest of CI operators is to employ solutions broadly adequate for multinational plants. For security suppliers their concern is more for developing solutions able to be sold on the international market. Here is where corporate interests clash with national security and highlight the need of more international cooperation. Since CIIP is defined as matter of national sovereignty, public powers are imposing new constraints to CIs and influencing the development of national technologies which should fulfill national standards. The consequences, such as limitation of foreign investment and increasing cost to implement a multitude of national standards, are relevant for the private sector.

In conclusion, these dynamics underscore the need to find the balance between national sovereignty and global business interests. That leads to the question of the right scale of international cooperation: how does one define a good partner? Is the European Union's the most appropriate level, or it would be more valuable to establish a trusted group of partners on the basis of mutual acceptance of national standards? The issue is complex, and the debate is still ongoing in Europe.

Gaming the Future: Public-Private Debate and 3PStrategy

The implementation of CIP is never going to be simple, but the French case outlines several important insights. Due to the complexity of the resilience issue, the State needs to make a preliminary capability assessment (which capabilities are needed to be jointly developed with the private sector?), then various and interdependent initiatives should be established with the private sector. PPP and regulation, thus, are complementary measures of infrastructure resilience. On the one hand, the government's responsibility is to build the appropriate and continuously-updated framework, both at national and international levels. On the other hand, PPPs operate to address the missing bricks that need a cooperative approach: training, situational awareness of attacks, technical solutions, etc. As demonstrated by the evolution undertaken by ANSSI in 2009-2013, dealing with CI resilience means being adaptive: being the policeman (conducting the inspection), the conventional rulemaker (helping CIs understand the measures to be implemented) or the facilitator (to develop the technical solution). Given that, the State takes on other important roles in enhancing the cyber resilience.

First of all, the debate on the balance between law enforcement, security and offensive capabilities must be open. Keeping secret vulnerabilities or cracking encryption standards means increasing technical vulnerabilities for everyone. In that way, the State schizophrenia (promoting and implementing defenses while actively attacking) is no longer sustainable with the concept of resilience. However, the schizophrenia is also on the citizen's side: we accept that the State needs pre-emptive intelligence in order to anticipate the major threats to CIs. This situation pushes States to openly explain their activities—without revealing security recipes—to the citizens.[5]

In addition, public power should establish a strategy of PPPs that will evolve as the risk evolves. The real question is not about what exactly the role of government and private sector is, but rather how the different pieces of public-private cooperation fit together in order to mitigate the risk. CIIP is neither a state nor a solution but a continuous process

(Continued on Page 14)

[5] David Omand, Securing the State, (London: Hurst, 2010); Bruce Schneier, "A Fraying of the Public/Private Surveillance Partnership," Schneier on Security, last modified November 2013, https://www.schneier.com/blog/archives/2013/11/a_fraying_of_th.html.

(Continued from Page 13)

based on dialogue and demanding different levels of intervention from public and private sector. Therefore, a large and trusted spectrum of PPPs can act directly as a mitigation tool able to improve the national resilience.

With this new ethos of PPP, the State and private sector can play an increasing role in reducing the overall impact of the cyber risk and improve the ability of organizations to defend themselves against cyber threats. At this stage more detailed studies should follow on specific cases, and since the CIIP topic includes transnational issues, further research on regional and international level of PPP should be encouraged.

Acknowledgements

This work is funded by *Airbus Defence and Space-CyberSecurity* and supported by the *Chaire Castex de Cyberstratégie*. Any opinions expressed in this publication are those of the author and do not necessarily reflect the views of Airbus Group.

**Danilo D'Elia is a Ph.D. candidate in Geopolitics at the University of Paris VIII Saint-Denis and research associate at Chaire Castex de Cyberstrategie (Paris). His research focuses on the dynamics of the implementation of the French strategy of cyber security.* ❖

CIP/HS is involved with a three year research study for the Department of Homeland Security looking at Improving the Effectiveness of Cybersecurity Incident Response Teams (CSIRTs). If you are a member of a CSIRT team or if you are involved in your organization's cybersecurity management or operations, we would like you to consider taking the attached survey. A link to the survey can be found here: https://www.surveymonkey.com/s/MHVXQTQ.

The survey should take 10 to 15 minutes to complete. The data collected in this study will be confidential and no individual or organization can be identified. A summary of the research results will be presented at future cybersecurity conferences and published in a future edition of the CIP Report.

Any questions on this survey or the DHS research study should be directed to me 703-993-4720 or via email at mtroutma@gmu.edu

Your Critical Infrastructure Security Program Will Fail Without a Security Awareness Program

by Parham Eftekhari and Marjorie V. Perry*

When developing critical infrastructure risk management programs, most strategies place emphasis on the implementation of cybersecurity technologies, policies, and governance models as "critical success factors" to securing an organization's assets. While these efforts are without doubt imperatives for securing digital assets and the physical world they impact, it is a mistake to overlook the importance of systematic programs of security awareness education among stakeholders in an organization. Until the centrality of security training is accepted and on par with investments in technology and processes, our critical infrastructure security efforts will fail to be fully effective. This essay will explore why investing in security awareness education is as important as the technology itself, how a cyber-aware culture can improve the financial health of your organization while reducing its security risk, and offer scenarios for various population segments that should be the focus of awareness efforts.

Traditionally, cybersecurity education and training has not been viewed as a priority due to budget constraints, a lack of understanding of the importance of security education, and an organizations' denial of the odds of a breach actually occurring. However, recent high profile breaches caused not by a lack of technology but a lack of education and awareness among the average employee have given organizations reason to take another look at how implementing an education and training program can benefit their business. Many of today's breaches are caused by simple human error or ignorance—clicking on the wrong link, opening the wrong email, incorrect password protection, not investing in readily available and affordable technologies like dual factor authentication—all of which can be prevented with better education.

As a result of our culture which devalues security education, security breaches are being reported daily at highly reputable organizations such as Sony, Target, Home Depot, and virtually every U.S. federal agency whereby cybercriminals gain access to highly sensitive information to the tune of billions of dollars a year and immeasurable damage to corporate reputations. The Sony hack, for example, has already cost the company $35 million dollars, has the company fighting several lawsuits, and has caused irreparable damage to the brand.

For security education to have a maximum societal impact, however, we must focus on more than just education among the "average employee" and middle-management classes who arguably get a disproportionate share of blame when it comes to some of the preventable causes mentioned above. Education is also desperately needed among the C-suite who is responsible for funding security investments and security training within organizations, as these executives often do not see the economic impact cybersecurity can have on their business and remain in denial that a breach can happen to them. From a policy perspective, advising is needed for federal and state legislators who, as politicians, cannot be expected to be subject matter experts in cybersecurity but are expected by the electorate to be educated on these issues before supporting and voting on security legislation.

When taken in this context, all of the money, technologies, risk frameworks, and governance models will be limited in their effect on our security unless we create cultures where everyone is cyber aware, and education is the only way that can happen.

The question now becomes how do you begin to develop a cyber-aware culture. When developing an educational/training program for non-technical security individuals, you must first define each segment you will be training, and then understand how the members of that segment are able to impact the security outcomes of your business based on their roles in your organization. Whether your program is designed to comply with federal requirements, better prepare your workforce to combat cyber threats,

(Continued on Page 16)

(Continued from Page 15)

or safeguard your reputation, due diligence best practice demands that business leaders are aware of resources available to support critical infrastructure cybersecurity through education and training initiatives. Below are some of the most important population segments currently underserved from a security education perspective as well as scenarios depicting how critical infrastructure security could be improved through improved security awareness among these segments:

- Legislators – Despite the tremendous increase in the amount of cyber and technology legislation being passed at the federal and state levels, there remains a lack of adequate education for policy makers to ensure that legislation will be effective and sustainable as technologies and threats evolve. Think Tanks like the Institute for Critical Infrastructure Technology (ICIT) provide valuable advising to the legislative community on technology issues and trends to ensure policymakers, who are not subject matter experts on technology, approach critical infrastructure legislation with as much information as possible.

Legislation has the potential to be one of the most powerful tools in our nation's cybersecurity arsenal. Today however, due in large part to a lack of adequately educated policy makers, cybersecurity laws fall short of their intended outcomes. Consider this scenario given to us by ICIT Fellow Ryan Kalember (Chief Product Officer, WatchDox): Destructive malware like what was used in the Shamoon, Dark Seoul, and Sony Pictures attacks exfiltrate local files from PCs, then destroy data on both local drives and mapped network drives before rendering the PC hard drive inoperable. Like what happened at Sony, the critical infrastructure provider is effectively shut down for weeks and operational processes move to paper, faxes, and personal smartphones. "If there was legislation in place requiring a CI provider to use a secure content gateway like WatchDox, rights management could have been applied to the stolen files, enabling the provider to revoke access to them even after the exfiltration," said Mr. Kalember. "In addition, the mapped network drives could have been protected from deletion and the local hard drive's files could have been synced to a secure server, enabling the CI provider to recover quickly from the attack"

The technology exists to make hacks like Sony and even the NSA "Snowden" incident much less impactful, but legislators need to be properly educated in order to pass meaningful legislation that will impact security outcomes.

- Executive Management - When developing training for the C-suite, always discuss security in terms of the impact to the financial stability to the organization as well as the damage a breach or incident will have on the reputation of the brand. Executives are less interested in the details of the technology, and more concerned about how the technology will work in the larger context of the business. From a risk management perspective, the biggest fear among this group is notifying clients their data has been compromised or, if they are large enough, being the lead story on the evening news.

ICIT Fellow Danyetta Magana (CEO, Covenant Security Solutions) shared her understanding of how implementing appropriate cybersecurity countermeasures can bring added value to the business' bottom line and how to communicate this to executives. "It is imperative that C-suite executives have information to make critical decisions around cybersecurity and its impact to their viability and profitability." Ms. Magana went on to explain that this can be realized through software that provides near real-time management insights into security incidents like Covenant's SOPHIA or other similar technologies.

- Employees – Perhaps the most important group that is underrepresented when it comes to security training is non-IT employees. A significant portion of breaches come from accidental data loss which cost companies billions of dollars a year and can be avoided though effective and sustained employee awareness and education campaigns. Organizations that build these initiatives into their budgets not only better protect their data and information systems, but protect the reputation of their business. CamPatch Webcam Covers reports that roughly 20% of its custom branded sales are used as part of internal awareness campaigns with messages such as "Think before you Click". As mentioned in this essay, support for employee education often starts by educating the C-suite and building an economic case behind making this investment.

(Continued on Page 17)

(Continued from Page 16)

• Consumers - As the Internet-of-Things grows and technology becomes increasingly engrained into our lives from the moment we wake up to the moment we go to sleep, the separation of critical infrastructure and one's personal space will continue to become increasingly blurred. Our collective hunger for technology and convenience is pushing innovation at unprecedented speeds, which has created an environment where security risk analysis, especially on the part of the consumer, is often an afterthought to instant gratification. To that end, consumers of technology—children, parents, adults, and the elderly—need to first understand the connection between technology and their personal safety. Then, when an emotional connection is made, we can start to engrain them with best practices to protect themselves and their assets.

There is no shortage of thought leadership coming out of the cybersecurity community regarding how to protect our critical infrastructures. Proven technologies like two-factor authentication, information security guidance such as the NIST 800-53 Risk Management Framework, and governance models exist. If implemented today, cybersecurity countermeasures of this nature would have an immediate effect on the security posture of most organizations. The lack of widespread adoption of cybersecurity countermeasures is not due to the unavailability of solutions, rather, a limited heightened awareness on the part of our society regarding what risks we face and how to effectively mitigate those risks.

Lack of exposure to resources many times is a factor in implementing cybersecurity education and training programs. In today's Cyber Age, organizations should seek readily available security countermeasures that can yield an immediate return on investment as they are easily incorporated in day-to-day business processes. The impact of continued education and training on cybersecurity cannot be understated and will be seen in many ways. The most obvious outcome is a more informed and aware set of consumers and decision makers, which will lead to better investments on the part of executives, better policies on the part of legislators and better decisions on the part of employees and consumers while using technologies.

A second less obvious but arguably more powerful impact will be a collective voice demanding change from service providers and the legislative community when it comes to securing digital services and assets. The vast majority of Americans have cars but are not car safety experts. Yet, we are confident when we get behind the wheel of our cars because we trust the governance set up by the industry, the safety features of our cars (seat belts, airbags, side impact guards, etc.), and the leadership governing our roads (speed limits, traffic lights, signs). The same needs to happen with our digital products and services. Yet until consumers demand this level of security, providers will not readily offer it as quickly as they can, and this demand will not happen until consumer are fully aware and educated.

One can empathize with how the technology industry—obsessed with speed, innovation and anything new—could dramatically undervalue the importance of education as part of its security imperatives. However, until we make a drastic change in our attitudes towards security awareness and follow it up with action, the efforts to protect our critical infrastructures will never outpace the attacks from our enemies.

**Parham Eftekhari is Co-Founder and Senior Fellow with the Institute for Critical Infrastructure Technology (ICIT). Marjorie V. Perry, CAP, CSSLP, CRISC, is Director of Cybersecurity Education and Training with Covenant Security Solutions, Inc."* ❖

The Legislative and Executive Agenda for Cybersecurity in 2015

by Dennis Pitman*

Despite substantial media coverage and vocal political calls to action, Congress failed to pass any of the several significant cybersecurity bills proposed in the previous legislative session. While no significant changes have been implemented, several small measures made their way to the President's desk before the 113th Congress adjourned in December, indicating that interest in cyber legislation has not faded. With a single party in the leadership of both chambers and added incentives from recent high-profile breaches against Sony and Anthem, officials and stakeholders have renewed hopes for significant legal reforms in the coming year. Looking at models from the previous session, bills already introduced this year, and the President's cybersecurity agenda, we can begin to see the outlines of cybersecurity initiatives that may become law in the coming months.

The Lame Duck Cybersecurity Laws

Congress enacted a flurry of new laws in the final days of the legislative session last year with several new provisions related to cybersecurity. Though none of these new laws provide the kind of far-reaching reforms industry was hoping for, they do provide for some incremental progress in federal agency activity in security partnership and information sharing. Aside from some directives for potential cooperation with the nations of Ukraine and Israel on cyber issues, four new laws provide for changes to cybersecurity policy within government agencies.

The Federal Information Security Modernization Act of 2014[1] calls for a number of new information security measures across the executive. Among other things, it provides operational authority to the Secretary of Homeland Security for implementation of information security policies across federal agencies. The Secretary's operational directives are required to be in harmony with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Along with this new authority for DHS, the law implements expanded reporting requirements for agencies, including the reporting of major incidents to Congress within seven days.

The Homeland Security Cybersecurity Workforce Assessment Act[2] directs the Secretary to take measures, along with the Office of Personnel Management, to identify, codify, and fill cybersecurity workforce positions within DHS.

The National Cybersecurity Protection Act of 2014[3] establishes a national cybersecurity and communications integration center in DHS to serve as a civilian interface for sharing cyber risks, incidents, analysis, and warnings across federal and non-federal entities. The new center comes with a number of new reporting requirements, as well as an explicit disclaimer against any authority on the part of DHS to regulate the private sector. All non-federal engagement with the center is to be through voluntary agreements and at the unreviewable discretion of the Under Secretary of the National Protection & Programs Directorate (NPPD).

The Cybersecurity Enhancement Act of 2014[4] calls for the development or continuation of a number of cybersecurity education and research initiatives. The most notable of these for our present purposes are the directives for NIST to produce new standards and procedures for addressing cyber risks on an ongoing basis through engagement with private-sector stakeholders as well as federal, state, and local security

(Continued on Page 19)

[1] Pub. L. No. 113-283, 128 Stat. 3073 (2014), available at https://www.govtrack.us/congress/bills/113/s2521.
[2] Pub. L. No. 113-277, §4, 128 Stat. 2995 (2014), available at https://www.govtrack.us/congress/bills/113/s1691.
[3] Pub. L. No. 113-282, 128 Stat. 3066 (2014), available at https://www.govtrack.us/congress/bills/113/s2519.
[4] Pub. L. 113-274, 128 Stat. 2971 (2014), available at https://www.govtrack.us/congress/bills/113/s1353.

(Continued from Page 18)

agencies. NIST is also given responsibility for coordinating federal agencies in the development of international technical standards for information security.

Stakeholder Concerns

Although these laws have some significance for federal security operations, they do little to address the concerns of many private stakeholders, including prominent legal issues like:

- Increased regulation and the availability of judicial review;
- Potential liability resulting from new standards and information sharing;
- Privacy concerns;
- Antitrust liability for collaboration in response to threats; and
- Loss of intellectual property and proprietary information.

These provide both the foundations and hurdles for legislative and regulatory action addressing current weaknesses in the nation's cybersecurity. No proposals put forth thus far have attempted to address all of these issues, and solutions are likely to be made piecemeal over the coming years. On January 14, the White House announced a legislative agenda proposal that will address certain information sharing, breach reporting, and law enforcement concerns. Congress is also currently considering a few bills with implications for these areas. Finally, in the absence of legislation, the President and the National Security Council have put forward executive measures for enhancing risk management and information sharing practices.

The President's Legislative Agenda

President Obama has put forward cybersecurity as an administration priority for years. In 2011, he put forward a legislative proposal for improving information sharing.[5] As we know, that legislation never became a reality as Congress became less productive in the years that followed. With the increasing frequency and severity of cyber breaches, the President has resurrected his legislative agenda with the announcement of a new proposal this January.[6]

The President's legislative proposal covers three areas: (1) increasing cybersecurity information sharing; (2) enhancing the authority of law enforcement agencies to combat cyber crime; and (3) implementing uniform national requirements for data breach reporting.

The core of the proposal's information sharing measures centers on targeted liability shields for companies who share threat information through the DHS National Cybersecurity and Communications Integration Center (NCCIC). The exact contours of these shields have not been announced as the administration attempts to navigate the competing interests at play. Excessive protection from liability would create a risk of moral hazard whereby the firms being protected under-invest in security or show insufficient regard for customer privacy with the knowledge that they will be safe from loss so long as they meet the minimum standards of the shield.

That said, under current law many of the companies that could provide useful threat information are deterred by the specter of potential liability to customers or the U.S. government for what would otherwise be an efficient process of threat disclosure. Without a liability shield, companies face the possibility that even voluntary standards will be used as the basis for a duty of care in civil claims for a future breach. In the case of massive breaches like those against Target and Anthem, companies found to have failed in compliance with such standards could face class plaintiffs numbering in the millions. Furthermore, some have argued that inadequate measures have been put in place to ensure that companies will not be accused of anticompetitive behavior for entering collaborative agreements for sharing threat data with other companies in the same market.[7]

(Continued on Page 20)

[5] Office of the Press Secretary, "FACT SHEET: Cybersecurity Legislative Proposal," The White House Website (May 12, 2011), available at http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

[6] Office of the Press Secretary, "SECURING CYBERSPACE: President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts," The White House Website (January 13, 2015), available at http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

[7] CONGRESSIONAL RESEARCH SERVICE, R42409, Cybersecurity: Selected Legal Issues (April 17, 2013), available at https://www.fas.org/sgp/crs/misc/R42409.pdf.

(Continued from Page 19)

Provisions for the increase in law enforcement authority include measures to allow prosecution for the sale of botnets, criminalize the sale of stolen financial data overseas, provide new authority to deter the sale of spyware, and enable courts to grant orders to shut down botnets. The proposal would also update the Computer Fraud and Abuse Act to prevent punishment of "insignificant" conduct while increasing enforcement against abuses by insiders, as well as the Racketeering Influenced and Corrupt Organizations Act (RICO) to bring organized cyber crimes legally into line with similar non-cyber crimes.[8]

The third prong of the legislative proposal would create a federal requirement for businesses to notify consumers following security breaches. Most states already have laws requiring some form of notification following a breach, but a federal law would place all businesses under a uniform mandate, theoretically easing compliance.

Opponents include both industry representatives and public interest groups. Some tech companies, including Google and Facebook, have stated reservations over any mandatory information sharing provisions due to ethical, legal, and public relations problems related to the recent controversy surrounding National Security Agency surveillance programs.[9] The Electronic Frontier Foundation (EFF) has criticized the new proposal as being a rehash of old ideas that failed to gain traction in 2011. They are concerned that the information sharing and law enforcement provisions threaten to increase already intrusive government surveillance programs, and despite general agreement with notification laws, EFF has expressed disappointment that the requirements from the 2011 proposal, which are likely to be the model for 2015, were more lenient than some existing state law requirements that would be preempted, namely those of California.[10]

Legislation Currently Introduced in Congress

Roughly one month into the legislative calendar of the 114th Congress, a handful of cybersecurity bills have already been introduced. The most extensive thus far is H.R. 234, the Cyber Intelligence Sharing and Protection Act.[11] As the name implies, this measure is primarily concerned with facilitating information sharing processes, especially in the intelligence community. It designates DHS and DOJ as the agencies primarily responsible for coordinating the sharing of cyber threat and cyber crime information, respectively. The bill also tasks the Secretaries of Defense and Homeland Security, as well as the Director of National Intelligence and Attorney General to develop policies and procedures for the collection, retention, and disclosure of cyber intelligence to other agencies and third parties with the goal of safeguarding privacy and civil liberties. In essence, these measures would encourage greater sharing of federal intelligence with the larger cyber community, but would do nothing to address the liability issues described above.

Aside from this measure, most other bills involving cybersecurity are fairly narrow in scope:

- H.R. 53, the Cyber Security Education and Federal Workforce Enhancement Act, is focused and educational and professional development resources, ranging from K-12 science and technology programs to DHS recruitment;[12]

- H.R. 54, the Frank Lautenberg Memorial Secure Chemical Facili-

(Continued on Page 21)

[8] Press Secretary, "SECURING CYBERSPACE."
[9] Justin Sink, "White House Brushes Off Tech CEO Snubs of Cybersecurity Summit," The Hill (February 13, 2015), available at http://thehill.com/blogs/blog-briefing-room/232742-white-house-unconcerned-by-tech-absences.
[10] Mark Jaycox and Lee Tien, "EFF Statement on President Obama's Cybersecurity Legislative Proposal," Electronic Frontier Foundation Blog (January 13, 2015), available at https://www.eff.org/deeplinks/2015/01/eff-statement-president-obamas-cybersecurity-legislative-proposal.
[11] Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. (2015, available at https://www.congress.gov/114/bills/hr234/BILLS-114hr234ih.pdf.
[12] Cyber Security Education and Federal Workforce Enhancement Act, H.R. 53, 114th Cong. (2015), available at https://www.congress.gov/114/bills/hr53/BILLS-114hr53ih.pdf.
[13] Frank Lautenberg Memorial Secure Chemical Facilities Act, H.R. 54, 114th Cong. (2015), available at https://www.congress.gov/114/bills/hr54/BILLS-114hr54ih.pdf.

(Continued from Page 20)

ties Act, calls for consideration of cyber threats in training materials and performance standard in chemical facilities;[13]

- H.R. 451, the Safe and Secure Federal Websites Act of 2015, would institute policies for federal websites that collect, store, or maintain personally identifiable information, including requirements for reporting breaches;[14] and

- S. 456, "a bill to codify mechanisms for enabling cybersecurity threat indicator sharing between private and government entities, as well as among private entities, to better protect information systems."[15]

With the possible exception of S. 456, these bills do not address the goals of the President's legislative agenda or reach very far beyond the domain of federal agency operations. While these measures certainly hold the potential to increase the resources of the cyber community by increasing access to government information and promoting a more proficient workforce, they do little to improve information sharing and breach disclosure law for those private entities that comprise the majority of the nation's cyber infrastructure.

Executive Initiatives

With progress in Congress likely to be slow, the President has announced a handful of executive actions and policies to press his cyber agenda to the extent available under current law.

Early in February, the National Security Council announced plans to tailor administration practices to incentivize private-sector adoption of the NIST Cybersecurity Framework. First, non-independent agencies with authority to regulate critical infrastructure will start the process of identifying and reforming regulations that are found to be "burdensome, conflicting, or ineffective."[16] Next, DHS will publish a report in the spring on research and development priorities for the next three to five years related to cybersecurity and risk management. Finally, based on the recommendations of the Department of Defense and General Services Administration, the administration will implement updated cyber risk management policies and requirements through federal procurement.

Even more recently, President Obama held the first Cybersecurity and Consumer Protection Summit at Stanford University. Leading up to this event, the President signed an advisory executive order[16] calling on public- and private-sector entities to take a larger role in building and utilizing Information Sharing and Analysis Organizations (ISAOs). Along with this call to action, the order announces the competitive process for the designation of an NGO to serve as the ISAO standards organization. It also designates the NCCIC as a critical infrastructure protection program with the authority to form voluntary agreements with ISAOs. Although Apple CEO Tim Cook attended the summit, many notable companies declined to participate, including Yahoo, Google, and Facebook.[18] Coincidentally, Facebook and Yahoo announced the creation of their own information sharing platform, ThreatExchange,[19] only days before the summit.[20]

(Continued on Page 22)

---

[13] Frank Lautenberg Memorial Secure Chemical Facilities Act, H.R. 54, 114th Cong. (2015), available at https://www.congress.gov/114/bills/hr54/BILLS-114hr54ih.pdf.

[14] Safe and Secure Federal Websites Act of 2015, H.R. 451, 114th Cong. (2015), available at https://www.congress.gov/114/bills/hr451/BILLS-114hr451ih.pdf.

[15] S. 456, 114th Cong. (2015). This bill was introduced on February 11, 2015. As of the writing of this article, the text for this bill has not been made available from the Government Printing Office.

[16] Michael Daniel, "Strengthening Cyber Risk Management," National Security Council (February 2, 2105), available at http://www.whitehouse.gov/blog/2015/02/02/strengthening-cyber-risk-management.

[17] Office of the Press Secretary, "Executive Order: Promoting Private Sector Cybersecurity Information Sharing," The White House Website (February 13, 2015), available at http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[18] Sink, The Hill.

[19] ThreatExchange, https://threatexchange.fb.com/.

[20] AFP, "Facebook, Partners Unveil Alliance on Cybersecurity," Security Week (February 11, 2015), available at http://www.securityweek.com/facebook-partners-unveil-alliance-cybersecurity.

(Continued from Page 21)

Conclusion

Recent attacks have reignited the conversation about cybersecurity both in media and in the Capitol. With the new congressional session starting and a new Republican majority in the Senate, the potential exists for greater movement on broad cybersecurity legislation in the coming year. While it is too early to know what the exact nature of the final legislation will be, the President's legislative proposal provides an outline of some initiatives likely to be atop the list of priorities. In the meantime, the President and private sector have both taken steps to increase adoption of the NIST Cybersecurity Framework and improve cyber threat information sharing. Despite these efforts, all such measures remain voluntary and carry the risks of potential liability until Congress acts to provide a more definite legal foundation.

**Dennis Pitman is a licensed attorney of the Commonwealth of Virginia and Research Assistant at the Center for Infrastructure Protection and Homeland Security at George Mason University. He is a 2013 graduate of the George Mason University School of Law.* ❖

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