Journal of Technology Law & Policy

Volume XIV – Spring 2014

ISSN 2164-800X (online)

DOI 10.5195/tlp.2014.146

http://tlp.law.pitt.edu

A Voluntary Cybersecurity Framework Is Unworkable—Government Must Crack the Whip

Robert Gyenes

A Voluntary Cybersecurity Framework Is Unworkable—Government Must Crack the Whip

Robert Gyenes*

INTRODUCTION

On Black Friday, parents line up at the door of their local department store hoping to grab that hot item ticket for their eager kids. Six months later, they apply for a car loan and find that their credit has been ruined.[1] Why? Because two months before Black Friday an employee at an air conditioning and refrigeration firm outside of Pittsburgh opened an email he shouldn't have.[2] The email contained malware that stole the authentication credentials of the air conditioning and refrigeration firm, which was one of Target's contractors.[3] As a direct result of the successful breach, 110 million credit card numbers, from some of the nation's largest retailers, were stolen during one of the busiest shopping seasons.[4]

Due to the economic loss doctrine, companies face little risk of liability for the injuries resulting from their failure to prevent cyber-intrusions.[5] Pure economic loss by a consumer without any physical injury is difficult to pursue in court.[6] This immunity from liability from economic loss due to cyber-intrusions provides no incentive for corporations to voluntarily take the costly measures necessary to prevent such a massive breach.[7] Consequently, the response to the Black Friday

* Robert Gyenes is a student at the University of Pittsburgh School of Law and J.D. Candidate, Class of 2015.

[1] Chris Isidore, *Target: Hacking hit up to 110 million customers*, CNN MONEY (Jan. 11, 2014, 6:20 PM), http://money.cnn.com/2014/01/10/news/companies/target-hacking/.

[2] Dan Goodin, *Epic Target hack reportedly began with malware-based phishing e-mail: Attack hit contractor two months before the compromise of 40 million payment cards*, ARS TECHNICA (Feb. 12, 2014, 4:00 PM), http://arstechnica.com/security/2014/02/epic-target-hack-reportedly-began-with-malware-based-phishing-e-mail/.

[3] *Id*.

[4] Isidore, *supra* note 1.

[5] Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1557 (2013).

[6] *Id*.

[7] *Id*. at 1555–57.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

breach was not massive private investment in prevention.[8] Instead, affected stores merely offered a year of free credit monitoring.[9]

For all the benefits and profit brought by the increasingly connected world, connectivity has unleashed countless troubles. Cybercrime has increased fantastically since the internet's humble beginning.[10] Cybercrime has become a bigger threat than terrorism.[11] We have even seen a "worm" scorch the world's computer systems and strand delegates to a cybersecurity summit in Luxembourg at the airport when it knocked out the airport's reservation desk.[12]

Governments often speak of protection against cyber threats as a national security issue, requiring inventive and comprehensive prevention measures.[13] The U.S. Government's approach has been to collaborate with private companies, who are significant targets of cyberattacks.[14] Recently, the Obama Administration proposed a cybersecurity framework for "critical" infrastructure enterprises that attempts to satisfy both the demands of these private businesses and the overarching goal of better defending our national security's vulnerability to cyberattack.[15]

This private-public partnership has cooled significantly due in large part to the NSA PRISM scandal that resulted from Edward Snowden's release of NSA documents on Wiki-leaks.[16] It is now harder for lawmakers to address serious

---

[8] Caroline Fairchild, *Target security breach likely to be 'highly sophisticated organized crime*,' CNN MONEY (Dec. 19, 2013, 3:43 PM), http://tech.fortune.cnn.com/2013/12/19/target-security-breach-likely-to-be-highly-sophisticated-organized-crime/.

[9] Dana Liebelson, *Target's "Second-Rate" Fix for Hacking Victims May Leave Customers Vulnerable*, MOTHER JONES (Feb. 11, 2014, 3:00 AM), http://www.motherjones.com/politics/2014/02/target-credit-hack-breach.

[10] Michael Coren, *Experts: Cyber-crime bigger threat than cyber-terror*, CNN (Jan. 24, 2005, 1:35 PM), http://www.cnn.com/2005/TECH/internet/01/18/cyber.security/index.html?section=cnn_mostpopular.

[11] *Id*.

[12] *Id*.

[13] *See* The White House, *The Comprehensive National Cybersecurity Initiative*, *available at* http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (last visited Mar. 6, 2014).

[14] Mark Rockwell, *Agencies pay for public distrust in post-Snowden era*, FCW (Jan. 28, 2014, 12:00 AM), http://fcw.com/articles/2014/01/28/privacy-concerns-agency-costs.aspx.

[15] Exec. Order No. 13,636, 78 Fed. Reg. 11739, 11739 (Feb. 19, 2013).

[16] *Id*.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

cybersecurity threats in a way that is acceptable to powerful industry players.[17] As a result of this and other concerns, the Obama Administration's current cybersecurity policy is not a viable option for actual advancement in private cyber protection.

One primary problem with the Obama Administration's cybersecurity plan is that it promotes an information-sharing program between the government and private industry, which is likely to be ineffective given the reluctance of the private sector to participate.[18] Additional problems with the President's policy include criticism that the policy may be confusing for private enterprise to implement and that executives may struggle with the possibility that voluntary guidelines will become mandatory as an industry standard benchmark.[19] The policy also creates a financial burden on the target "critical" infrastructure without providing a solution.[20]

A simpler plan could push "critical" industry to improve its cybersecurity without these pitfalls. For example, a scheme that focuses on financial support for improvement while imposing mandatory liability for security failures would produce results yet still allow some independence in how the results are achieved.

Part I of this Article outlines the characteristics of cyber-attacks that create difficulties for policymakers, and argues that any successful government policy must take account of the continuously changing tactics of cyber criminals. Part II examines the President's current strategy for improving cybersecurity of "critical" infrastructure and discusses the best possible outcome of the Executive Order-based strategy and subsequent agency implementation. Part III analyzes the Executive Order's "Information Sharing Program" and "Best Practices Framework" provisions. Part IV concludes by proposing an alternative plan focused on financial support and a mandatory liability regime.

---

[17] Gerry Smith, *"Snowden Effect" Threatens US Tech Industry's Global Ambitions*, THE WORLD POST (Jan. 28, 2014), http://yaleglobal.yale.edu/content/%E2%80%9Csnowden-effect%E2%80%9D-threatens-us-tech-industrys-global-ambitions (last visited Apr. 4, 2014).

[18] Jason Miller, *DHS finds classified cyber sharing program slow to take off*, FEDERAL NEWS RADIO (June 13, 2013, 6:44 AM) http://www.federalnewsradio.com/473/3356694/DHS-finds-classified-cyber-sharing-program-slow-to-take-off.

[19] James Stenger, *Companies Need To Take Notice of the Government's Cybersecurity Program*, TMT PERSPECTIVES (Sept. 26, 2013, 12:00 AM), http://www.tmtperspectives.com/2013/09/26/companies-need-to-take-notice-of-the-governments-cybersecurity-program/.

[20] Anthony M. Freed, *ISA Outlines Criteria to Evaluate NIST Cyber Security Framework*, TRIPWIRE (Feb. 6, 2014, 12:00 AM), http://www.tripwire.com/state-of-security/top-security-stories/isa-outlines-criteria-evaluate-nist-cyber-security-framework/.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

I. THE NATURE OF THE THREAT

On account of the massive scale and variety of targets of modern hackers, cybersecurity threats are often treated as a new front in an undeclared war.[21] It is tempting to force this relatively new threat into the terminology and framework we understand by comparing it to a new Cold War or Afghanistan, but there the comparisons stop; weapons for this "war" change every day and the "innovation" of the enemy is astounding.[22] In effect, there are attackers and defenses, but this war has no borders, no ideological lines, and no face.

A. Targets

Cybercrime targets change each day. Early on, criminal activity in cyberspace was aimed at governments and banks, because they were the few that possessed large computer networks.[23] The targets broadened when a wider range of firms collected useable data.[24] This meant information brokers, such as credit reporting agencies and data aggregators like ChoicePoint or LexisNexis, were ripe targets for cyber-crime because of their large stores of identity data.[25] But now that computers are found in most homes and almost every business, there has been an increase in the number and types of potential victims of cybercrimes.[26] With news of another massive cyber breach every day, one may wonder if such attacks are becoming white noise. Schools, department stores, and home computers are all targets.[27] Our refrigerators are even being hacked.[28] Several law firms in Pittsburgh have also become victims.[29] Headlines and ubiquitous commercials for credit-score

[21] Chris C. Demchak, *Hacking the Next War*, THE AMERICAN INTEREST (Aug. 10, 2012, 12:00 AM), http://www.the-american-interest.com/articles/2012/08/10/hacking-the-next-war/.

[22] *Id*.

[23] Charlotte Decker, *Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S. CAL. L. REV. 959, 961 (2008).

[24] Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201, 204 (2006).

[25] *Id*.

[26] Decker, *supra* note 23.

[27] Patrick Svitek & Nick Anderson, *U-Md. computer security attack exposes 300,000 records*, THE WASHINGTON POST (Feb. 19, 2014, 12:00 AM), http://www.washingtonpost.com/local/college-park-shady-grove-campuses-affected-by-university-of-maryland-security-breach2014/02/19ce438108-99bd-11e3-80ac-63a8ba7f7942_story.html.

[28] Silvana Ordonez, *Hackers can get into your refrigerator, too*, CNBC (Jan. 7, 2014, 12:00 AM), http://www.cnbc.com/id/101345760.

[29] U.S. Attorney's Office, *Pittsburgh Man Sentenced for Role in Law Firm Hack*, FBI, http://www.fbi.gov/pittsburgh/press-releases/2013/pittsburgh-man-sentenced-for-role-in-law-firm-hack.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

watchdogs are constant reminders that no company or web-user should feel completely safe from cyberattacks.

B. Actors

The actors behind each of these far-reaching cyber assaults are equally varied in purpose, demographics, and organization.[30] Initially, cyber-criminals were the computer whiz kids—the individuals with esoteric technical knowledge of computer languages and programing.[31] But as computers proliferated, so did those who tried to misuse them. There now exists a group of individuals known as "enablers" who are "persons who use their technical expertise to create and then sell data to non-technically savvy people to engage in cyber-crime."[32] Cybercrime has essentially become a business enterprise.[33] Although profit remains a significant incentive for cybercrime, it is not the sole motivation.[34] Businesses, and defense contractors as it seems lately, must worry about ex-employees using inside knowledge to strike back at their former employer.[35] Other cybercriminals are motivated by a self-proclaimed altruism and dub themselves "hacktivists."[36] The range of actors and motivations is incredible; from lone wolves, hacking clubs, ex-employees, to "unmentionable" government-backed cyberattacks from our trading partners, Russia and China.[37] It is therefore hard to conceive of a plan where everything is protected from everyone.

---

[30] Yang & Hoffstadt, *supra* note 24, at 205.

[31] *Id*.

[32] *Id*.

[33] *Id*.

[34] Debbi Wilgoren, *Edward Snowden fired by Booz Allen after admitting leak*, THE WASHINGTON POST, June 11, 2013, 12:00 AM, http:// articles.washingtonpost.com/2013-06-11/world/39886122_1_ systems-administrator-hotel-room-u-s-officials.

[35] *Id*.

[36] Brian B. Kelly, *Investing in A Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform*, 92 B.U. L. REV. 1663, 1676 (2012).

[37] David E. Sanger, Davide Barboza et al., *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 18, 2013, 12:00 AM, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all; *see also* Jim Finkle, *Russia hacked hundreds of Western, Asian companies: security firm*, REUTERS (Jan. 22, 2014, 12:00), http://www.reuters.com/article/2014/01/22/us-russia-cyberespionage-idUSBREA0L07Q20140122; Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals*, 16 VA. J.L. & TECH. 116 (2011).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

C. Methods

The myriad of methods that cybercriminals use, are so varied, that academics and politicians have spent considerable time simply trying to identify an appropriate definition for cybercrime.[38] The most general definition includes any crime "that is facilitated or committed using a computer, network, or hardware device."[39] But changes in technology and hacking methods means that any definition is a moving target and as new techniques emerge, lawmakers must struggle to amend statutes.[40] State and Federal governments have played catch-up, filling in the gaps of existing laws as cybercrimes evolve from Trojan horses, to password phishing, to increasingly sophisticated or opportunistic tactics.[41] For a national cyber-policy to be effective, it will need to take into account this amazing brevity of the *status quo*.

II. THE CURRENT EXECUTIVE ORDER PLAN TO FORTIFY CRITICAL BUSINESSES

Congress has been trying to tackle this wild, twisting cyber security problem for some time.[42] In the last 15 years, dozens of bills have been introduced.[43] Some proposed legislation, notably CISPA and SOPA, has even been criticized as a draconian threat to civil rights.[44] One of the main concerns with these recent cyber security bills has been their potential allowance of a government invasion of privacy rights due to the government's ability, under the proposed legislation, to request limitless data from ISPs that would not be anonymized.[45] These bills also

[38] Pinguelo & Muller, *supra* note 37.

[39] *Id*.

[40] Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 179 (2000).

[41] John D. Saba, *The Texas Legislature Goes Phishing*, 68 TEX. B.J. 706, 708 (2005); Jasmine E. McNealy, *Angling for Phishers: Legislative Responses to Deceptive E-Mail*, 13 COMM. L. & POLICY 275, 281 (2008).

[42] *See* Cyber Security Information Act, H.R. 2435, 107th Cong. (1st Sess. 2001); *see also* Cyber Security Enhancement Act of 2002, H.R. 3482, 107th Cong. (2d Sess. 2002); *see also* Cyber Security Information Act of 2000, H.R. 4246, 106th Cong. (2d Sess. 1999).

[43] *Id*.

[44] Jason Koebler, *ACLU: CISPA Is Dead (For Now)*, US NEWS (Apr. 25, 2013, 12:00 AM), http://www.usnews.com/news/articles/2013/04/25/aclu-cispa-is-dead-for-now.

[45] Jeff Nesbit, *CISPA Rolls Along*, US NEWS (May 6, 2013, 12:00 AM), http://www.usnews.com/news/blogs/at-the-edge/2013/05/06/cispa-rolls-along.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

contained provisions that went beyond cybersecurity.[46] For example, some of the bills' provisions allowed *ex parte* requests from copyright owners to block access to websites, ostensibly to protect against alleged infringement.[47] To say that American businesses were concerned is an understatement—major online entities like Wikipedia and Reddit "blacked-out" their websites in a massive coordinated protest.[48] As a result of these concerns, Congress lost support for their cyber protection plan and the bills ultimately died.[49]

Nevertheless, the problem still needs an answer. To this end, the Executive branch took up the cause where Congress fell short.[50] Through Executive Order, the Obama Administration has initiated a general framework for cybersecurity, which contains a more limited scope.[51] In February of 2013, the White House released Executive Order 13636: "Improving Critical Infrastructure Cybersecurity," which focuses only on improving the cybersecurity protection of what are deemed to be "critical infrastructure entities."[52] Critical Infrastructure Entities were chosen as a more focused demographic, because "the national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of [cyber] threats."[53] In doing so, the Executive Order's plan does not address other admittedly vulnerable private enterprises such as Target and Nieman Marcus.[54] While the term "critical" is expressed generally in the plan, the expectation is that the term includes industrial sectors such as banking,

[46] *Id*.

[47] *See id*.

[48] Derek E. Bambauer, *The New American Way of Censorship*, 49 ARIZ. ATT'Y 32, 36 (Mar. 2013).

[49] Koebler, *supra* note 44.

[50] 78 Fed. Reg. at 11739–40; Declan McCullagh, *Obama signs long-awaited cybersecurity executive order*, CNET (Feb. 12, 2013, 12:00 AM), http://news.cnet.com/8301-13578_3-57569092-38/obama-signs-long-awaited-cybersecurity-executive-order/.

[51] 78 Fed. Reg. at 11739.

[52] *Id*.

[53] *Id*.

[54] Matt Picht, *Report: Neiman Marcus missed 60,000 alerts about card hack*, ATLANTA JOURNAL CONSTITUTION (Feb. 23, 2014, 1:21 AM), http://www.ajc.com/news/news/national/report-neiman-marcus-missed-60000-alerts-about-car/ndYww/.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

communication, power, and transportation—sectors already heavily regulated because of their fundamental role in the smooth operation of society.[55]

Two of the primary components of the Executive framework are what the Executive Order describes as "Cybersecurity Information Sharing" and "Baseline Framework to Reduce Cyber Risk to Critical Infrastructure."[56]

A. The Information Sharing Provision

"Cybersecurity Information Sharing," the first of the two components, is a strategy to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.[57] To achieve this goal, the Department of Homeland Security ("DHS") has expanded existing programs for voluntary corporate-to-government and government-to-corporate information sharing.[58] Previously pilot programs or programs run by another government agency, the information sharing pools have been significantly boosted by the Executive Order.[59] What these programs aim to achieve is an effective information-sharing framework among the government, which includes Information Sharing and Analysis Centers, ISPs, and their respective critical infrastructure members and customers.[60] Currently, the system employs a series of "bulletins," which provide an initial threat alert, followed by subsequent analysis on the content of the actors, their strategy and seriousness, and general threat climate overviews.[61]

---

[55] Michelle Richardson, *President Obama Shows No CISPA-like Invasion of Privacy Needed to Defend Critical Infrastructure*, ACLU (Feb. 13, 2013, 12:00 AM), https://www.aclu.org/blog/national-security-technology-and-liberty/president-obama-shows-no-cispa-invasion-privacy-needed.

[56] 78 Fed. Reg. at 11739–41.

[57] *Id*. at 11739–40.

[58] Notably, the Enhanced Cybersecurity Services (ECS) program, the Cyber Information Sharing and Collaboration Program (CISCP) (formerly run by the Department of Defense), and the National Cybersecurity and Communications Integration Center (NCCIC); see Dep't of Homeland Sec., *CIKR Cyber Information Sharing and Collaboration Program (CISCP)* (June 2013), http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_menna_ciscp_one_pager.pdf.

[59] Written testimony of NPPD Office of Cybersecurity & Communications Acting Assistant Secretary Roberta Stempfley, and National Cybersecurity and Communications Integration Center Director Larry Zelvin for a House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies hearing titled *Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities* (May 16, 2013, 12:00 AM), *available at* https://www.dhs.gov/news/2013/05/16/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-hearing [hereinafter WT-NPPD].

[60] *Id*.

[61] Dep't of Homeland Sec., *supra* note 58.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

In the best case scenario, this information sharing program would witness government-corporate harmony through enough private "critical" companies voluntarily sharing information with the government to create a large pool of threat information.[62] Consequently, threats that target our nation's most vital private infrastructure would be thwarted by a rapid and actionable alert provided by the DHS.[63]

Advocates for the "Cybersecurity Information Sharing" program point to a number of improvements over previously proposed legislation.[64] For example, it avoids serious privacy concerns by being "privacy-neutral"—the data shared by "critical" corporations is still covered by state privacy laws.[65] The plan's focus on only "critical" corporations shows a prioritization that is likely to be more palatable as it will interfere less with online commerce.[66] Perhaps most importantly, the information-sharing program is *voluntary*.[67] CEOs can watch from the sidelines if they fear sharing information with the government.[68]

There is also some benefit to the fact that this new initiative isn't so new after all. Instead, the plan builds off existing departments and agencies, which have been running information sharing pilot programs for some time.[69] The main DHS-programs were sharing information well before the Executive Order expanded their task.[70] Companies can therefore have more confidence in participating with programs that have a track record (i.e. the Enhanced Cybersecurity Services ("ECS") program (established 2012), the Cyber Information Sharing and Collaboration Program ("CISCP") (2011), and the National Cybersecurity and Communications Integration Center ("NCCIC") (2009).[71] The DHS has pointed to the success of its 45-partipant, two-way CISCP program, which shared almost

---

[62] *See id*.

[63] *Id*.

[64] Richardson, *supra* note 55.

[65] *Id*.

[66] Andy Greenberg, *President Obama's Cybersecurity Executive Order Scores Much Better Than CISPA On Privacy*, FORBES (Feb. 12, 2013, 10:37 PM), http://www.forbes.com/sites/andygreenberg/2013/02/12/president-obamas-cybersecurity-executive-order-scores-much-better-than-cispa-on-privacy/.

[67] 78 Fed. Reg. at 11739; *see also Enhanced Cybersecurity Services*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/enhanced-cybersecurity-services (last visited Mar. 7, 2014).

[68] Greenberg, *supra* note 66.

[69] *See* WT-NPPD, *supra* note 59.

[70] *Id*.

[71] *Id*.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

20,000 indicators in the first year or so.[72] The DHS reports that of the information shared within the CISCP program, roughly 60 percent was provided to the government by the private sector.[73]

Thus, the two-way information sharing policy outlined by Executive Order has the potential at least to provide a large pool of useable threat information, which hopefully will prevent some of the cyberattacks hindering our national security.

B. The Best Practices Provision

The second major component of the Executive Order is the "Baseline Framework to Reduce Cyber Risk to Critical Infrastructure."[74] This component aims to create a roadmap of best practices "that align policy, business, and technological approaches to address cyber risks."[75] The philosophy tries to account for an ever-changing threat and economic viability.[76] The guidelines seek to be "technology neutral and enable critical infrastructure sectors to benefit from a competitive market."[77]

As required by the Executive Order, the National Institute of Standards and Technology ("NIST") released a "best practices" guideline based on this policy in February 2014 (the "Framework").[78] The Framework provides a blueprint for identifying potential threats, protecting against cyberattacks and, if an attack occurs, recovering from it.[79] The standards outlined are flexible, and generally contain no specific methodologies or mandatory procedures for private companies to take.[80] Instead, the Framework uses a system of "Tiers" of preparedness, which

---

[72] Miller, *supra* note 18.

[73] *Id*.

[74] 78 Fed. Reg. at 11739.

[75] *Id*. at 11740–41.

[76] *Id*.

[77] *Id*.

[78] *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS AND TECH. (NIST) (Feb. 12, 2014, 12:00 AM), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf [hereinafter NIST].

[79] Kathleen Hennessey & Chris O'Brien, *Cybersecurity guidelines for companies are unveiled by White House*, LA TIMES, Feb. 12, 2014, 12:00 AM, http://articles.latimes.com/2014/feb/12/business/la-fi-cyber-security-20140213.

[80] Antone Gonsalves, *NIST Cyber Security Framework proposal provides no 'measurable cybersecurity assurance,'* CSO ONLINE (Sept. 5, 2013, 12:00 AM), http://www.csoonline.com/article/739139/nist-cyber-security-framework-proposal-provides-no-measurable-cybersecurity-assurance-.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

are flexible enough to allow a company in any specific critical industry to adapt to its unique security situation.[81] This avoids a one-size-fits-all approach. Since the preparedness "targets" are couched in generalities, the idea is they will not force companies to adopt any technology or practices that the company finds inefficient or too costly.[82] As one commentator noted, "the cybersecurity framework doesn't tell companies what to do or what tools to buy . . . but it does standardize the questions all CEOs should ask about their companies' security practices. . . . and it shows them what the answers ought to look like."[83]

Since the Framework's standards are voluntary goals, "critical" infrastructure is spared the draconian imposition of previous legislation. The voluntary nature of the program shows "how sharply proponents of strong regulation have scaled back their ambitions—and even their language—in the face of industry opposition to government intervention."[84] The Framework lets organizations choose the level of cybersecurity they want to achieve; nothing in the guidelines is mandatory.[85] It is unlikely, therefore, to cause immediate financial or logistical burden on the profit-minded company.

Like the information sharing programs, the actual standards and methodologies are for the most part, the status quo. Companies will not be surprised by what amounts to little more than a compilation of established industry security practices.[86] Thus, the Framework has the possibility of raising the industry-as-a-whole, by outlining a path for cybersecurity improvement that does not place any undue burden on the "critical" infrastructure companies that seek to utilize it.

III. THE FAULTS OF THE CURRENT APPROACH

Despite any potential this Executive Plan has if executed perfectly, it is likely to do very little to protect this nation's critical infrastructure against cyberattacks.

[81] Hennessey, *supra* note 79.

[82] Cynthia Brumfield, *NIST framework released to widespread praise, but what happens next?*, CSO ONLINE (Feb. 13, 2014, 12:00 AM), http://www.csoonline.com/article/748216/nist-framework-released-to-widespread-praise-but-what-happens-next-.

[83] Wyatt Kash, *Why Businesses Can't Ignore US Cybersecurity Framework*, INFORMATIONWEEK (Feb. 14, 2014, 9:25 AM), http://www.informationweek.com/government/cybersecurity/why-businesses-cant-ignore-us-cybersecurity-framework/d/d-id/1113838.

[84] *Id.*

[85] Gonsalves, *supra* note 80.

[86] Kash, *supra* note 83.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

Even at its best, it fails to confront the business realities and certain unique characteristics of cyber threats, which are necessary to create an effective government-led cyber policy.

A. Problems With Information Sharing Program

An information-sharing scheme will likely see resistance no matter how much privacy protection is provided. Despite privacy and civil rights concerns, however, information sharing has remained a key concept in the new executive order-based cybersecurity plan.[87] Still, even if the policy achieves its goal of being "privacy-neutral" and avoids the controversial elements that killed CISPA and SOPA, information sharing in general is likely to create a considerable deal of hesitation and concern.[88] "The big consequence of Edward Snowden's NSA leaks will be that countries and companies will erect borders of sorts in cyberspace" and thus be extremely wary of anything that has the words "government" and "information sharing" so close together.[89] Companies like Microsoft and Google are openly trying to thwart the Government's possible acquisition of their data and similar resistance is likely to be found among privacy-minded "critical" companies.[90]

Experts have asked if information sharing programs can actually work.[91] Even the Government itself is aware that this is a murky area. Anne Neuberger, director of the NSA's Commercial Solutions Center, has said of information sharing programs: "on the one hand, they're cited as critical . . . on the other hand, they're frequently criticized as ineffective."[92] With the constantly morphing nature of cyber-threats, it is difficult to determine how effective advance information regarding the attacks would be or the extent to which countermeasures could be effectively deployed based on advance information. Most available information regarding threats thwarted by existing programs is unclear.[93] The 20,000 indicators shared by the DHS last year do not reveal how effective that information was.[94]

---

[87] 78 Fed. Reg. at 11739; McCullagh, *supra* note 50.

[88] Richardson, *supra* note 55.

[89] L.S. Davos, *The Snowden effect*, THE ECONOMIST (Jan. 24, 2014, 2:06 PM), http://www.economist.com/blogs/babbage/2014/01/internet-governance.

[90] *Id*.

[91] Michael O'Connell, *Threat information sharing builds better cyber standards, expert says*, FEDERAL NEWS RADIO (Oct. 3, 2013, 5:05 PM), http://www.federalnewsradio.com/1195/3470899/Threat-information-sharing-builds-better-cyber-standards-expert-says.

[92] *Id*.

[93] Miller, *supra* note 18.

[94] *Id*.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

How necessary or valuable was any of it? One may assume that such a quantity of information necessarily put a burden on the 45 companies based on sheer volume, but an accurate account of that burden does not appear to be available.

It seems true that information-sharing programs can be effective when targeted to highly specific information shared among a small group of related companies.[95] But the success of such programs, like the "Financial Services—Information Sharing and Analysis Center," is due to the very limited and interconnected nature of that industry.[96] At best, it is unclear whether such a model can be expanded to the varied sectors deemed "critical."

The Executive Order's information sharing program also fails to fix issues that have stymied such programs before.[97] In part because the government doesn't provide any funding, businesses have decided not to invest in new secure facilities and network upgrades to handle classified data.[98] Additionally, because the government seeks to share *classified* information, there will be added costs.[99] Not all companies have employees with the necessary clearance levels. This is noted in the Executive Order itself.[100] Yet the proposed solution of expedited clearance will still add costs that may dissuade corporate participation.[101] A cheaper alternative would still present problems. An independent research group suggests the government share classified threat information with "key decision makers" when a corporation otherwise lacks certified employees.[102] While this would improve the odds a threat warning is acted upon, it is likely to increase fears about leaked information.[103]

---

[95] O'Connell, *supra* note 91.

[96] *Id*.

[97] *See* Miller, *supra* note 18.

[98] Miller, *supra* note 18.

[99] Jacob B. Pankowski & Debra McGuire Mercer, *Executive Order on cybersecurity impacts Government contractors and other critical infrastructure entities*, LEXOLOGY (Mar. 4 2013, 12:00 AM), http://www.lexology.com/library/detail.aspx?g=8431e873-8d30-43fb-8aca-5f87ab068a5c.

[100] 78 Fed. Reg. at 11740.

[101] Pankowski, *supra* note 99.

[102] Bipartisan Policy Center, *Cyber Security Task Force: Public-Private Information Sharing*, 13 (2012), *available at* http://bipartisanpolicy.org/sites/default/files/PublicPrivate%20Information%20Sharing.pdf.

[103] *See* David Ingram, *Stephen Kim Pleading Guilty For Leaking Classified Information*, HUFFINGTON POST (Feb. 7, 2014, 12:00 AM), http://www.huffingtonpost.com/2014/02/07/stephen-kim-guilty_n_4746710.html.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

As a result of these unaddressed costs and mistrust, existing information sharing programs have witnessed feeble participation rates. For example, critics have cited very few have made the investment and joined the voluntary Enhanced Cybersecurity Services program.[104] In fact, "none of the 54 companies that showed initial interest since the executive order came out have moved into the program."[105]

Sharing programs could increase participation by sharing only unclassified information, but obviously the value of such information would be proportionately degraded.[106] Consequently, the Cyber Information Sharing and Collection Program ("CISCP"), which shares two-ways among 45 companies, has a higher participation rate, albeit only slightly.[107]

Beyond its failure to address the problems of existing programs, the Executive Order's plan creates confusion as to what companies are now required to do.[108] There is serious concern that the voluntary program may soon become mandatory.[109] This could happen in two ways. First, this program could become mandatory as agencies promulgate regulations.[110] According to the Executive Order, the federal agencies "shall propose prioritized, risk-based, efficient, and coordinated actions . . . to mitigate cyber risk."[111] One of the "actions" agencies could propose would be enforcement of the program using existing regulations, expanded interpretations of existing regulations, and adoption of new regulations.[112] Critics argue this directive "can only be read to open the door for federal agencies to enforce the Program."[113]

The voluntary information sharing programs also risk becoming mandatory through civil liability pressure.[114] "A company that receives cyber threat reports from the government will ignore those reports at their peril since regulatory agencies and private litigants could claim that the company was negligent . . . for

---

[104] Miller, *supra* note 18.

[105] *Id*.

[106] *See generally* Pankowski & Mercer, *supra* note 99.

[107] O'Connell, *supra* note 91.

[108] *See* Brumfield, *supra* note 82.

[109] Stenger, *supra* note 19.

[110] *Id*.

[111] *Id*.

[112] *Id*.

[113] *Id*.

[114] *Id*.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

ignoring the reports."[115] There will also be pressure to *share* information. A company in an information-sharing regime that fails to share appropriate cyber threat information is therefore in danger of litigation or regulatory action for failing to participate.[116] Private companies could therefore be pressured into sharing sensitive data to the government and other private companies participating in the ostensibly voluntary program.

An information-sharing scheme as proposed by the Executive Order is therefore unlikely to be as effective as planned. Its efficiency is limited by participation issues and cost concerns, as indicated by the inefficiency of current sharing programs.

B. Problems With Best Practices Policy

The Best Practices Policy of the Executive Order will also not be an effective improvement to the cybersecurity of "critical" infrastructure. The Framework's flexibility, voluntariness, and lack of both enforcement and incentive provisions are likely to create confusion and perhaps even stifle innovation. In an effort to create a program palatable to private enterprise, the net effect of conciliation will be very little progress.

The first problem with the NIST Framework is its creation of confusion regarding the duties of private enterprise.[117] Corporations will be left wondering if they have fulfilled their obligations.[118] "Most senior executives are likely to ask, 'have we adopted or are we in compliance with the Framework?'"[119] They will likely be told, "it's impossible to answer these questions clearly and that the goal is to simply 'use' the Framework."[120]

How will that framework then be "used?" Again, there is confusion. Critics have cited the outcome of a risk assessment can be stretched in any direction.[121]

---

[115] *Id*.

[116] *Id*.

[117] Joab Jackson, *How the NIST cybersecurity framework can help secure the enterprise*, PCWORLD (Feb. 14, 2014, 12:00 AM), http://www.pcworld.com/article/2098320/how-the-nist-cybersecurity-framework-can-help-secure-the-enterprise.html.

[118] *Id*.

[119] *Executive Summary Assessing President Obama's Executive Order on Cyber Security*, INTERNET SEC. ALLIANCE, *available at* http://isalliance.org/publications/Assessing%20Executive%20Order%20Success%20-%20ISA%20Criteria%20Paper%20-%20Final%202-6-14.pdf (last visited Mar. 17, 2014) [hereinafter INTERNET SEC. ALLIANCE].

[120] *Id*.

[121] Gonsalves, *supra* note 80.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

Executives are therefore able to ascribe to themselves a job well done. Allowing organizations to choose the level of cybersecurity they want to achieve means "an organization could choose a level of zero, and still be conformant with the guidelines."[122] The Framework allows any organization, no matter how effective they are regarding cybersecurity, to be guideline-conformant.[123] Instead of motivating corporations to spend large sums of money to improve their cyber protection, the Framework allows complacency and may even have a negative effect.[124] Therefore, in an effort to make everyone happy, "the guidelines have also made the hackers happy."[125]

There is also a significant fear that this Framework will become mandatory through the methods that apply to the information-sharing scheme.[126] "The guidelines are likely to become the *de facto* standard for litigators and regulators."[127] Commentators warn any company that manages critical infrastructure in the U.S. and disregards the Framework "does so at its own peril."[128] Critical infrastructure owners need to recognize, "if a company's cybersecurity practices are ever questioned during a regulatory investigation and litigation, the baseline for what's considered commercially reasonable is likely to become the NIST Cybersecurity Framework."[129] Courts have imposed liability on companies for failing to abide by industry standards, and because this publication carries so much weight, it is likely to set that standard.[130]

As executives struggle to address the possibility of civil liability, confusion will abound as to what level of adherence reduces that liability. Ostensibly the Framework binds companies to nothing.[131] Yet despite this technical lack of obligation, critics have also remarked that the Framework will create implicit

---

[122] *Id*.

[123] *Id*.

[124] *Id*.

[125] *Id*.

[126] Stenger, *supra* note 19; Gerald Ferguson, *NIST Cybersecurity Framework: Don't Underestimate It*, CSO ONLINE (Dec. 9, 2013, 12:00 AM), http://www.informationweek.com/government/cybersecurity/nist-cybersecurity-framework-dont-underestimate-it/d/d-id/1112978.

[127] Ferguson, *supra* note 127.

[128] *Id*.

[129] *Id*.

[130] *See* The T.J. Hooper, 60 F.2d 737 (2d Cir. 1932).

[131] Gonsalves, *supra* note 80.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

liability for "critical" corporations that fail to adopt the *highest* standard outlined.[132] "Critical infrastructure companies defending their cybersecurity practices in litigation or regulatory investigations should be prepared to show that the practices adhere to Tier 4, considered 'adaptive.'"[133] The "adaptive" level iHs obtained when a company is "regularly evaluating the threats it faces, testing its procedures, and modifying these procedures where appropriate to address new threats."[134] Tier 4 "adaptive" is the highest Tier, requiring the most diligence and the most financial and personnel resource to achieve.[135] Consequently, even though the Framework is promoted as a voluntary program of mere recommendations, it is actually likely to punish those companies that fall short of the most demanding mark.

A third problem with the guidelines is there is virtually nothing new in the framework.[136] As noted above, a lack of surprises is welcome news for "critical" infrastructure operators. However, this also makes the framework rather unnecessary. Many organizations essentially "adopted" the Framework elements long before the Framework itself was constructed.[137] Studies suggest 40-50% of private entities can be classified into this "best practices" group.[138] The Framework is therefore trying to achieve what the market can do on its own.

In this respect, the Framework may stall advancement and innovation. It may serve to fix the bar, but fix it low. "Policy makers need to understand that using the framework is not the same thing as assuring critical infrastructure security—much more is needed.[139] Such a misunderstanding could lead to misguided public policies."[140] Subjecting industry and technology corporations to Framework-based regulation may stifle innovation and ultimately result in increased costs to the federal government.[141] A scramble to protect from civil liability will promote

---

[132] Ferguson, *supra* note 126.

[133] *Id*.

[134] NIST, *supra* note 78, at 11.

[135] *Id*.

[136] INTERNET SEC. ALLIANCE, *supra* note 119; *see also* Ferguson, *supra* note 126.

[137] INTERNET SEC. ALLIANCE, *supra* note 119.

[138] *Id*.

[139] Freed, *supra* note 21.

[140] *Id*.

[141] Lee Vorthman, *IT Security: NIST's Cybersecurity Framework*, NETAPP (July 16, 2013, 12:00 AM), https://communities.netapp.com/community/netapp-blogs/government-gurus/blog/2013/07/16/it-security-nists-cybersecurity-framework.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

complacency and box ticking.[142] Given the nature of cyber threats today, this should be especially worrisome since "the bad guys are impressive innovators."[143]

The Framework has also been criticized for lacking focus on certain serious cyber threats.[144] For instance, there is no mention of cloud-based cyber threats.[145] Other threats aren't addressed by the very nature of the Framework's assessment system.[146] The traditional risk assessment structure of the Framework "doesn't address malicious intent . . . it's that simple."[147]

Other criticism of the Framework focuses on financials. "Although the President's Order requires the framework to be cost effective, there is almost no analysis of this critical issue in the framework documents. If the goal is to have industry adopt the framework on a voluntary basis, its cost effectiveness is an essential element."[148]

The Administration's plan of furthering cybersecurity through voluntary best practices is accordingly unlikely to achieve the desired results. Instead, it will create more confusion than innovation and subject "critical" companies to the threat of civil liability.

IV. AN ALTERNATE APPROACH SHOULD BE FOLLOWED

Rather than pursuing a program of information sharing and voluntary guidelines, the Administration should focus on financing improvements and creating a clear liability scheme, which forces the desired progress. This is the most efficient avenue toward better protecting our national security and would also take into consideration the business concerns of the target private enterprise.

"Most security officers already have a solid understanding of how their systems need to be secured . . . what they too often lack are the adequate

---

[142] Anthony M. Freed, *Cyber Security Framework Lacks Mitigating Controls and Cloud Security*, TRIPWIRE (Dec. 10, 2013, 12:00 AM), http://www.tripwire.com/state-of-security/regulatory-compliance/cyber-security-framework-murky-cloud-security-issues/.

[143] John Eggerton, *NIST Releases Cybersecurity Framework*, BROADCASTING & CABLE (Feb. 12, 2014, 12:00 AM), http://www.broadcastingcable.com/news/washington/nist-releases-cybersecurity-framework/129156.

[144] Freed, *supra* note 142.

[145] *Id*.

[146] *Id*.

[147] Gonsalves, *supra* note 80.

[148] Freed, *supra* note 142, at 21.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

resources."[149] Under the current Framework, companies are left to wonder how they will finance any voluntary cyber improvements without incentives.[150] Corporations failing to invest in cybersecurity often cite budget constraints as "the number one challenge to contributing to the [cybersecurity] levels the business expects."[151] Although the President's Order requires the framework to be cost effective, there is almost no analysis of this critical issue in the framework documents.[152] Therefore, if the goal is for industries to adopt the framework on a voluntary basis, its cost effectiveness is an essential element.[153]

Financing security improvements could be accomplished in two ways: (1) directly covering the costs of the necessary improvements or (2) creating financial incentives. The DHS is already directly funding airlines' security improvements and a similar approach could work for "critical" infrastructure.[154]

It seems, however, that incentives will likely be the preferred path in this situation, given its mention in the Executive Order.[155] But, any incentive has yet to be properly developed.[156] In theory, incentives would encompass a wide range of offerings or conditions that could include technical and public policy measures.[157] Training and education or critical software could be provided.[158] In such fashion, corporations would find it makes more financial sense to improve areas of neglect.

Financial incentives, however, are not enough. As a senior administration official has remarked, "government-based incentives are really important for us to pursue . . . but at the end of the day, it's the market that's got to drive the business

---

[149] Jackson, *supra* note 117.

[150] Gonsalves, *supra* note 80.

[151] Paul van Kessel & Ken Allen, *Under cyber attack: EY's Global Information Security Survey 2013*, at 7, EY (Oct. 2013), *available at* http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf.

[152] *Id*.

[153] *Id*.

[154] Office of the Press Sec'y, *Secretary Napolitano Announces $98 Million in Recovery Act Funding For Airport Security Technologies*, DEP'T OF HOMELAND SEC. (Sept. 17, 2010, 12:00 AM), http://www.dhs.gov/news/2010/09/17/secretary-napolitano-announces-98-million-recovery-act-funding-airport-security.

[155] 78 Fed. Reg. at 11742.

[156] Brumfield, *supra* note 82.

[157] Eric Chabrow, *Incentivizing the Cybersecurity Framework: Getting Industry to Adopt the Recommended Best Practices*, BANK INFO SEC. (Feb. 18, 2014, 12:00 AM), http://www.bankinfosecurity.com/incentivizing-security-framework-a-6510.

[158] Eggerton, *supra* note 143.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

case for the cybersecurity framework."[159] Surely the federal government is going to do its best to make the costs of using the Framework lower, and the benefits of the framework higher, "but it's the market that's going to ultimately make this work."[160] Corporate executives have noted the limitations of an incentive program.[161] The chairman of AT&T remarked, "the best incentive on cybersecurity is fear," he said, "it scares the living hell out of us."[162]

In addition to financial support, an effective cybersecurity policy requires a liability regime that is clear but not burdensome. Corporations should not have to weigh the risk of civil liability under a voluntary program with the cost of improvements. Instead, standards should be mandated, imposing liability on corporations' failures to improve their critical infrastructure. If done correctly, this could also allow for executives to implement a security protocol that is adapted to their unique corporate circumstance. For instance, assuming the Obama Administration wants serious results, a target similar to Tier 4 could be outlined with broad language. Making this goal mandatory removes the confusion by imposing actual liability on failure. Companies will immediately improve their cybersecurity infrastructure if liability for economic loss due to a breach is imposed. Due to the economic loss doctrine, companies presently face little risk of liability for the injuries that result from their failure to prevent cyber-intrusions.[163] Removing default immunity from liability would incentivize firms to harden their systems against intrusion.[164]

An imposed liability scheme is morally defensible. A higher standard and burden on private critical infrastructure entities is validated by their role in national security. As the President's Order itself states, "the national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats."[165] This varies slightly from the burden

[159] Chabrow, *supra* note 157.

[160] *Id*.

[161] Eggerton, *supra* note 143.

[162] *Id*.

[163] Sales, *supra* note 5, at 1557.

[164] *See* Christopher J. Coyne & Peter T. Leeson, *Who's to Protect Cyberspace?*, 1 J.L. ECON. & POL'Y 473, 492 (2005).

[165] 78 Fed. Reg. at 11739.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

placed on airlines.[166] No doubt any imposed liability scheme will face resistance, but given the small pool of companies targeted, this objection should be overruled.

It is a financially defensible scheme as well. Government imposed standards have been shown to be the most cost-effective in certain cybersecurity scenarios.[167] In a highly technical paper entitled "*Who Should Be Responsible for Software Security*," it was found that government imposed standards can be preferable to a system where the private company picks up the tab for either patching the problem or the cost of loss after a breach.[168]

Given possible resistance to an increased burden, a safe harbor provision may also be appropriate. For instance, firms that implement security standards developed in tandem with regulators, but nevertheless suffer cyber-attacks, could be offered immunity from lawsuits seeking redress for the resulting damages.[169] If such a carrot-stick tandem of liability and safe harbor were employed, companies would be encouraged to pursue the highest Tier of best practices without an undue burden for the inevitable intrusion. This would allow the individual businesses to choose the details of their particular security strategy, while still achieving broad industry-wide progress.[170]

CONCLUSION

The President's policy is a start in the right direction. It should be lauded for picking up a difficult subject after repeated Congressional failure. There is no doubt that a cyber weapon that can shut down nuclear reactors should become a priority in our overall national security strategy.[171] How to structure that government framework for cybersecurity will remain a subject of debate, but the President is correct for showing tremendous concern for industry input in the

[166] Alex Davies, *The Budget Deal Will Make Air Travel More Expensive*, BUSINESS INSIDER (Dec. 11, 2013, 12:00 AM), http://www.businessinsider.com/budget-deal-higher-air-fares-2013-12#ixzz2uBgSLW1.

[167] Terrence August & Tunay I. Tunca, *Who Should Be Responsible for Software Security?: A Comparative Analysis of Liability Policies in Network Environments*, 57(5) MGMT. SCI. 934 (May 2011), *available at* http://rady.ucsd.edu/faculty/directory/august/pub/docs/who-should-be-responsible.pdf.

[168] *Id*. at 934.

[169] Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SEC. L. & POL'Y 233, 235 (2010); Sales, *supra* note 156, at 1557–58.

[170] Eggerton, *supra* note 143.

[171] Charles Arthur, *Symantec discovers 2005 US computer virus attack on Iran nuclear plants*, THE GUARDIAN (Feb. 26, 2013, 12:00 AM), http://www.theguardian.com/technology/2013/feb/26/symantec-us-computer-virus-iran-nuclear.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu

process.[172] In light of Snowden's leaks and the SOPA and CISPA "blackouts," the battle is certainly going to be uphill. But letting corporations write the strategy is not going to produce results. The NIST Framework and the overall voluntary structure of the Presidential strategy acquiesce too much to public pressure.

If we are trying to protect something as vital as our national security, there is less room for compromise. We can achieve an increase in cybersecurity standards among private enterprise by imposing a liability regime that shows corporate executives that there will be real consequences for failing to properly protect their infrastructure. Proper incentives will then assuage some of the regulatory stress produced by such a plan. Putting money on the table is only part of the issue. We need to persuade private enterprise to use that incentive by providing consequences. Safe harbor will make the system more business-friendly.

It is important to remember that this Presidential policy is still only oriented toward "critical" infrastructure companies. That definition is flexible, but limited.[173] The benefit of a clear liability scheme that removes the currently enjoyed economic loss immunity is that it can be scaled up. When the time comes to shore up the security of Target or the air-condition repairman in Pennsylvania, this scheme can be easily applied across industry and operation scale.[174] With the threat of real financial liability, both critical industry and private retailers will have an appropriate incentive to better protect our national security and maybe produce a few less headlines.

---

[172] *NIST Issues Preliminary Cybersecurity Framework*, INFOSECURITY MAGAZINE (Oct. 23, 2013, 12:00 AM), http://www.infosecurity-magazine.com/view/35233/nist-issues-preliminary-cybersecurity-framework/.

[173] NIST, *supra* note 78, at 3.

[174] *See* Sales, *supra* note 5, at 1557.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.146 ● http://tlp.law.pitt.edu