Silicon Flatirons

A Center for Law, Technology, and Entrepreneurship at the University of Colorado

Summit Series*

Cybersecurity: Towards A Strategy for Securing Critical Infrastructure from Cyberattacks

Therese Kerfoot, *Rapporteur***

May 2012

* The *Cybersecurity* event is part of the Silicon Flatirons Summit Series. The reports from other summit discussions can be found at http://www.siliconflatirons.org/publications.php?id=report. Special thanks to Kenneth Bradtke, Kevin Brown, and Bryan Berman for their research assistance.

** Research Fellow, Silicon Flatirons Center.

COLORADO LAW

Executive Summary

Former Secretary of Homeland Security Michael Chertoff and former Secretary of Defense William Perry recently stated that the "present cyber risk is shocking and unacceptable. Control system vulnerabilities threaten power plants and the critical infrastructure they support, from dams to hospitals. . . . [and the] threat is only going to get worse. Inaction is not an acceptable option."[1] The National Security Agency warned that "[computer] hackers could have the ability to take down the entire U.S. electrical grid within the next two years[.]"[2] This concern echoes across industry sectors including energy,[3] telecommunications,[4] financial services,[5] and health care.[6]

These calls to action are supported by numerous examples of vulnerabilities and attacks on the Internet and information technology in the general commercial sectors (i.e., theft of private data).[7] The financial and competitive implications of cyberattacks cause many to consider them the most important threat to the future of the United States. The Federal Bureau of Investigation called the threat the "No. 1 concern as foreign hackers . . . penetrate American firms' computers and steal huge amounts of valuable data and intellectual property."[8] Although difficult to quantify or identify and easy to downplay,[9] it is fair to say that the threat is real and growing.

Evidence of commercial sector harms and existing risks in critical infrastructure sectors underscores the fragility of United States defenses to cyberattack. For example:

---

[1] Letter to Harry Reid and Mitch McConnell, Senate Majority and Minority Leaders (Jan. 19, 2011), *available at* http://pdfserver.amlaw.com/cc/120119_cyber_letter.pdf.

[2] Graham Smith, *Hacking Group Anonymous Could Shut Down the Entire U.S., Head of National Security Warns*, DailyMail Online, Feb. 22, 2012, http://www.dailymail.co.uk/news/article-2104832/Hacking-group-Anonymous-shut-entire-U-S-power-grid-head-national-security-warns.html.

[3] North Am. Electric Reliability Corp., 2009 Long Term Reliability Assessment: 2009-2018 6 (2009), http://www.nerc.com/files/2009_LTRA.pdf.

[4] *Tech Topic 20: Cyber Security and Communications*, FCC.gov, http://transition.fcc.gov/pshs/techtopics/techtopics20.html (last visited Apr. 25, 2012).

[5] Mark Rockwell, *Cyber Attacks Against Financial Services Firms Skyrocket, Study Says*, Govn't Sec. News, Apr. 13, 2012, http://www.gsnmagazine.com/node/26106.

[6] Brian Wingfield, *Power-Grid Cyber Attack Seen Leaving Millions in the Dark for Months*, Bloomberg, Jan. 21, 2012, http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html.

[7] For a list of 2011 attacks, see Matt Leibowitz, *Cybercrime Blotter: High Profile Attacks of 2011*, Security News Daily, Feb. 24, 2011, http://www.securitynewsdaily.com/455-websites-hacked-government-commercial-cybercrime-2011.html; *see also* U.S. Government Accountability Office, Multiple Efforts to Secure Control Systems Are Under Way, But Challenges Remain 13-17 (2007) [hereinafter Multiple Efforts]. Sean Lawson, *U.S. Cybersecurity Debate Risks Leaving Critical Infrastructure in the Dark*, Forbes, Feb. 11, 2012, http://www.forbes.com/sites/seanlawson/2012/02/11/u-s-cybersecurity-debate-risks-leaving-critical-infrastructure-in-the-dark/.

[8] Richard A. Clarke, *How China Steals Our Secrets*, N.Y. Times, Apr. 3, 2012, at A27.

[9] *See e.g.,* Timothy B. Lee, *Activists Fight Cyber Security Bill That Would Give NSA More Data*, ArsTechnica, Apr. 6, 2012, http://arstechnica.com/tech-policy/news/2012/04/activists-fight-cyber-security-bill-that-would-give-nsa-more-data.ars.

- The critical infrastructure of foreign nations has been attacked;[10]Spies from China and Russia reportedly made efforts to map out U.S. critical infrastructure; and,[11]

- Remote access and disruption of United States SCADA and other critical infrastructure control systems has been demonstrated.[12]

On Friday, February 10, 2012, the Silicon Flatirons Center at the University of Colorado Law School convened leaders from government, industry, and academia to discuss the cybersecurity challenges to United States critical infrastructure. After discussing the current market incentive structure, participants considered governance solutions to improving security. Echoing the diverse views on the national stage, the participants disagreed on many issues. They did, however, agree that the threat is real and substantial. Although some industries voluntarily adopt protective measures, several security professionals present during the discussion provided numerous examples of ones that have not.

Despite the threat, significant disagreement surrounded the appropriate level of government involvement. A majority of participants concluded that immediate government action can increase critical infrastructure security, while a few strongly argued that private firms can do a better job without government action. Still others argued that government action will be counterproductive.

In an effort to enrich the cybersecurity debate by articulating and evaluating these and other relevant public policy issues, this paper analyzes the key areas of contention and recommends workable solutions.[13] In particular, the paper concludes that:

- **The United States should adopt an overarching national cybersecurity policy**. It is important for the United States to adopt a critical infrastructure cybersecurity policy setting forth national goals and the means to achieve them.[14] *The appropriate policy goal should be to eliminate all reasonably avoidable risk based on best practices that balance both the relevant benefits of cybersecurity investment and the relevant harms of failing to invest*. Such a policy promises to guide federal agencies and the private sector in their security efforts. In so doing, it will allow them to prioritize the threats, determine business rationales for security solutions, and focus on accountability, prevention, and risk-management.

---

[10] Kim Zetter, *Report: Critical Infrastructure Under Cyberattack Globally*, Wired, Jan. 28, 2010, http://www.wired.com/threatlevel/2010/01/csis-report-on-cybersecurity/.

[11] Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, Wall St. J., Apr. 8, 2009, http://online.wsj.com/article/SB123914805204099085.html.

[12] Jeanne Meserve, *Mouse Click Could Plunge City Into Darkness, Experts Say*, CNN.com, Sept. 27, 2007, www.cnn.com/2007/US/09/27/power.at.risk/index.html; Billy Rios, *The Siemens SIMATIC Remote Authentication Bypass (That Doesn't Exist)*, Billy (BK) Rios (Dec. 22, 2011), http://xs-sniper.com/blog/2011/12/20/the-siemens-simatic-remote-authentication-bypass-that-doesnt-exist/.

[13] Cybersecurity Act of 2012, S. 2105, 112th Cong.(2011-2012); SECURE IT, S. 2151, 112th Cong. (2011-2012); Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong.(2011-2012); PRECISE Act of 2011, H.R. 3674, 112th Cong. (2011-2012); Cybersecurity Enhancement Act of 2011, S. 1152, 112th Cong.(2011-2012); Cyber Crime Protection Security Act, S. 2111, 112th Cong.(2011-2012); SECURE IT Act of 2012, H.R. 4263, 112th Cong.(2011-2012); Cybersecurity Enhancement Act of 2011, H.R. 2096, 112th Cong.(2011-2012).

[14] Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, 140 J. of Am. Academy of Arts & Sci. 70, 70-71 (2011).

- **Private firms, absent government oversight, are unlikely to adopt reasonably necessary measures in some sectors**. Summit participants agreed that market incentives work in some critical infrastructure sectors. At the same time, other sectors, such as "utilities, oil and gas, transport, telecommunications, chemical, emergency services, and postal and shipping industries[,]" remain vulnerable to attack, indicating the failure of free market incentives in those sectors.[15] Without effective incentives, these sectors are unlikely to take necessary security measures.

- **Defining legal duties will increase accountability and clearly identify responsibilities**. Most participants agreed that accountability is necessary to incentivize action where market forces fail to do so. Carefully defining legal duties for critical infrastructure managers and their supply chains will increase accountability. Once duties are well defined, **limiting liabilities** created by those duties (i.e., providing immunity from liability, limitations on non-economic damages, caps on actual damages, safe harbor protections, or eliminating punitive damages) may effectively incentivize adoption of best practices. However, regulators must guard against unintended consequences. Consider, for example, that incorrectly structured legal duties could drive players from the market or impede innovation. Further, if limitations on liabilities are not clearly defined, cost-effective, and tied to outcome-based standards, they may counteract the intended goal.

- **Effective economic incentives will increase the cost of failing to adopt security measures.** In many sectors, the business case for increased security is nonexistent. The cost of security is expensive and the impact of an attack difficult to quantify. For example, it is estimated that a secure energy grid today would cost nearly $3.7 billion.16 Despite the likelihood of attack, uncertainty as to the timing and extent of the harm makes defensive measures difficult to justify. Economic incentives that quantify failure to secure systems will help market players develop metrics to understand the financial implications of their actions. Effective economic incentives could include:

    - **Mandatory Disclosure Requirements**- Many states adopted data breach disclosure laws hoping to force companies to internalize the costs of such breaches. Public disclosure of a breach is expensive because it often drives away customers, decreases public perception, and increases the potential for lawsuits. These costs arguably incentivize security adoption in the commercial context. Similar mandatory disclosure of vulnerabilities and attacks by critical infrastructure could have the same effect. Yet in a world where cyberattacks are almost commonplace, many summit participants voiced skepticism at the benefits of disclosure requirements.
    - **Insurance markets**- Government facilitation of robust critical infrastructure cyberinsurance markets can increase both security and transparency. Cyberinsurance

[15] Fran Howarth, *Critical Infrastructure Under Attack*, ComputerWeekly.com Blog (Feb. 10, 2011, 6:11 PM), http://www.computerweekly.com/blogs/Bloor-on-IT-security/2011/02/critical-infrastructure-under-attack.html.

[16] MIT Energy Initiative, The Future of the Electric Grid 210 (2011).

allows critical infrastructure managers to share the risk of an attack. To limit their own expenses, insurers will increase security by requiring adoption of effective measures. Transparency will also improve as infrastructure managers are required to disclose attacks and vulnerabilities.

- **Direct expenditures**- Direct expenditures, which must be carefully tailored, can be effectively structured in a targeted and dynamic manner. For example, the Electronic Health Records Incentive Program on meaningful use, as created by the American Recovery and Reinvestment Act of 2009 (ARRA), uses direct expenditures to incentivize increased adoption and implementation of electronic health records over time. These types of direct expenditures can incentivize broad and long-term developments in critical infrastructure cybersecurity.
- **Government Procurement Process**- The government could require private sector contractors to adopt security standards as a prerequisite to enter the contracting process. This requirement might make the process more difficult for contractors, but it would likely raise the baseline level of security in many sectors.

- **A coordinated leadership effort could help avoid jurisdictional and authoritative confusion (and the inevitable delay it causes).** Although no consensus existed as to which entity or entities should lead the coordinated national effort, a majority of participants agreed that the Department of Homeland Security's current regulatory authority, institutional knowledge, and cybersecurity expertise makes it the best suited entity today.

- **Leadership must be backed by sufficient authority and resources**. Regardless of the entity or entities leading the national effort, summit participants strongly agreed that Congress must allocate sufficient authority and resources to get the job done.

- **Public-private partnerships must be empowered and their structures formalized**. Current public-private partnerships have not corrected the market failures that exist because they are under-empowered and frequently informal. Government should incentivize and empower such relationships. Roles, responsibilities, and authority of partnership members must be well-defined to avoid confusion and delay. The relationships between various partnership members must be based on maintained trust and balanced control. Industry groups should take the lead on partnership tasks. In empowering such efforts, it is important that industry leaders be sufficiently interested in the outcome, the amount of participants be sized appropriately, and the effort be organized to properly represent the constituency. In some cases, the potential role of government oversight—and its ability to certify best practice—will be important in catalyzing action by private sector organizations.

- **Digestible, complete, and timely information sharing about vulnerabilities and attacks on critical infrastructure is necessary.** Critical infrastructure will not be secure without effective and timely information-sharing. Summit participants agreed that such information is necessary to understand the risk and eliminate vulnerabilities. Yet concerns about privacy, data security, and innovation stymie information exchanges. Participants disagreed over the best exchange structure to eliminate these concerns. Some argued that smaller, industry specific exchanges were necessary to promote trust and real-time information, but others saw the distinct benefit of cross-sector exchanges. These broader exchanges would distribute information to industries not immediately affected and allow them to take proactive measures.

- **Outcome-based standards and best practices should be updated and enforced.** Overwhelming and confusing information on standards and best practices exist,[17] leaving critical infrastructure managers uncertain about the most effective security measures. Much can be done to identify the best standards and best practices for critical infrastructure managers. And, as technology constantly changes, much can be done to update and enforce outcome-based standards and best practices (either through government oversight or incentives for self-regulation).

- **Enforcement of liability schemes and identified standards and best practices is a key element of the cybersecurity picture.** Without effective enforcement regimes, critical infrastructure will remain vulnerable. Summit participants identified attribution and compliance as distinct barriers to effective enforcement. Joint and several liability regimes alleviate the need for attribution, while the use of third party auditors can evaluate compliance. Yet neither of these solutions is complete. Focusing on prevention, mitigation, and recovery can create a culture of security to support regulatory enforcement mechanisms.

- **Educated information technology professionals are necessary to the development of effective standards and best practices.** Strong consensus existed among summit participants that information technology professionals are fundamental to long-term security and must be directly involved in the development and implementation of standards and best practices. To ensure availability and quality of these professionals, educational programs must be incentivized and developed through increased federal funding.

[17] A December 2011 report by the Government Accountability Office noted that regulatory efforts have not been sufficiently effective. *See generally*, Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can be Done to Promote Its Use, U.S. Gov't Accountability Office (2011) [hereinafter *C*ritical Infrastructure Protection].

Contents

I. Introduction

On December 20, 2011, an American security researcher described in detail on his blog how to bypass authentication requirements for Siemens SIMATIC systems to achieve access to control systems and United States critical infrastructure.[18] It is clear from the comments on the blog that users successfully attempted the authentication bypass.[19] The researcher did not intend to induce an attack, but merely to expose Siemens's failure to fix the flaw disclosed six months earlier.[20] Although Siemens subsequently repaired the bug,[21] this example highlights the underlying cybersecurity problem the United States faces today: the market has failed to incentivize security managers and providers to comprehensively protect critical infrastructure. As critical infrastructure (i.e., energy supply, transportation systems, financial systems, water supply, and much more)[22] increasingly uses the Internet and networked information technology (often using Internet technology, but not necessarily the public Internet[23]), cyber vulnerabilities escalate in parallel.[24]

The opportunities and benefits of our modern Internet and networked information technologies are tremendous, but the associated public safety and economic risks are also significant. This is particularly true with respect to the greatly increased vulnerability to cyberattacks on critical infrastructure capabilities. Unlike loss of financial assets and private information, which is personally

18 Rios, *supra* note 12.

19 *Id.*

20 George V. Hulme, *More SCADA Security Flaws Surface,*CSOnline.com, http://www.csoonline.com/article/697013/more-scada-security-flaws-surface?page=2.

21 In an international example, Siemens addressed the Stuxnet worm, discovered in 2010, which was largely considered to be the most sophisticated and prolific attack on critical infrastructure by targeting and shutting down many of Iran's uranium enrichment centrifuges. The worm used the Microsoft Windows operating system to target vulnerabilities in Siemens's industrial control software. Nicolas Falliere, *Stuxnet Infection of Step 7 Projects, Symantech, Sept. 26 2010, http://www.symantec.com/connect/blogs/stuxnet-infection-step-7-projects.*

22 In this paper we will discuss critical infrastructure that relies upon both the Internet and networked information technology. Critical infrastructure has not been well defined and is likely to be narrowly defined in cybersecurity legislation. However, The Department of Homeland Security identified a total of 18 sectors representing the nation's critical infrastructure, including electricity and transportation, defense, financial systems, water, telecommunications, and many more. Rosenzweig, 3.
The Internet is a network of networks, but includes the hardware and software that allow information to move across the network including routers, switches, and servers, and the "protocols (e.g., TCP, IP, DNS, BGP) used to encode and transmit data." Kevin Alderson & David Soo Hoo, *The Role of Economic Incentives in Security Cyberspace,* Ctr. for Int'l Sec. & Coop. 6 (2004).
Networked information technology is the "end-to-end services that provide basic functionality to users of the network." *Id*.

23 For example, systems that us private networks that do not connect directly to the Internet without an IP address translator. These networks are still vulnerable, however, and the Stuxnet worm spread through interconnected private networks. Liam O. Murchu, *Stuxnet P2P Component*, Symantec Blog (Sept. 17, 2010), http://www.symantec.com/connect/blogs/stuxnet-p2p-component.

24 The Department of Homeland Security identified a total of 18 sectors representing the nation's critical infrastructure, including electricity and transportation, defense, financial systems, water, telecommunications, and many more. *Critical Infrastructure Resource Center*, Dept. of Homeland Sec., http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/sectorOverview.htm (last visited Apr. 25, 2012).

damaging,[25] harm to United States critical infrastructure can threaten national competitiveness,[26] physical well-being, and national security.[27] By standardizing management processes and increasing "connectivity of control systems to other computer networks and the Internet, insecure connections, and the widespread availability of technical information about control systems,"[28] critical infrastructure attackers can use these interconnected systems to take direct control of our infrastructure. For example, three-fourths of supervisory control and data acquisition (SCADA) systems are connected to the Internet or information technology networks.[29] Although they provide great value through remote maintenance and constant system supervision, they are difficult to update and require an average 331 days to implement system patches.[30] "If control systems are not properly secured, individuals and organizations may eavesdrop on or interfere with . . . operations from remote locations."[31]

In the event of such an attack, no "individual or organization, either in the private or public sector, [will be] immune."[32] If electricity systems are attacked, for example, the impact on individuals and businesses is likely to ripple through the economy beyond those Americans directly affected by the loss of electricity. Consider how the 2003 blackouts on the eastern coast of the United States (although not caused by a cyberattack) caused 11 deaths and cost an estimated $6.4 billion in lost employment and investment income, additional government spending, and lost or spoiled commodities.[33]

To combat and manage these cybersecurity threats, Congress must craft an appropriate

---

[25] Consumer privacy incidents are on the rise. In particular, vulnerabilities at nearly every level, including retail and sales, financial accounts and activity, sensitive healthcare information, and other personally sensitive information, are being taken advantage of with increasing frequency and damage to the economy. Although stories of stolen identities or credit card theft are prolific and frightening, consumer information is so widely available that its black market resale value has declined. Where credit card numbers could once be sold for $5 to $10, the current resale rate is no more than $1.50. In fact, in 2010, the incidence of electronically stolen data surpassed that of physical theft for the first time. *Information Theft at Companies Surpasses All Other Forms of Fraud for the First Time*, SecurityWeek.com (Oct. 18, 2010), http://www.securityweek.com/information-theft-companies-surpasses-all-other-forms-fraud-first-time; Nick Bilton, *Card Data is Stolen and Sold*, Bits Blog (May 3, 2011, 3:30 PM), http://bits.blogs.nytimes.com/2011/05/03/card-data-is-stolen-and-sold/.

[26] Economic espionage (i.e., theft of intellectual property, business processes, other proprietary technology), although nearly impossible to value, significantly impacts the U.S. competitive advantage through lost opportunities, reputational harm, loss of business confidence, an eroded research and development base, additional capital-intensive research and development, and legal fees. The reputational damage to a company, for example, generally lasts a year and can cost between $184 million to over $330 million for a company with a brand value of $1.5 billion. *Ponemon Institute Finds that Data Breaches can Cause Lasting and Costly Damage to the Reputation of Affected Organizations*, MissionCriticalMagazine.com (Oct. 27, 2011), http://www.missioncriticalmagazine.com/articles/84472-ponemon-institute-survey-finds-that-data-breaches-can-cause-lasting-and-costly-damage-to-the-reputation-of-affected-organizations.

[27] *See e.g.*, Richard Brust, *Cyberattacks: Computer Warfare Looms as Next Big Conflict*, A.B.A. J., May 1, 2012, http://www.abajournal.com/magazine/article/cyberattacks_computer_warfare_looms_as_next_big_conflict/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email.

[28] Multiple Efforts, *supra* note 7, at 14.

[29] SCADA systems are control systems that automatically regulate various infrastructural components of critical infrastructure, such as water treatment plants, gas pipelines, or power generation systems. *SCADA Systems*, http://www.scadasystems.net/ (last visited Apr. 25, 2012).

[30] Andy Greenberg, *Electric Oil Companies Take Almost a Year to Fix Known Security Flaws*, Forbes (July 28, 2010, 1:43 PM), http://www.forbes.com/sites/firewall/2010/07/28/electric-oil-companies-take-almost-a-year-to-fix-known-security-flaws/.

[31] Multiple Efforts, *supra* note 7, at 14.

[32] National Cybersecurity Research and Development Challenges, Inst. for Info. Infrastructure Protection 2 (2009).

[33] J.R. Minkel, *The 2003 Northeast Blackout -- Five Years Later*, ScientificAmerican.com, Aug. 13, 2011, http://www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later; Elec. Consumers Res. Council, The Economic Impacts of the August 2003 Blackouts 1 (2004).

oversight framework that identifies risks, goals, and best practices. This paper—supported by the summit discussion and independent research—is an attempt to influence the growing legislative discussion by providing a broad roadmap for understanding and addressing the cybersecurity policy issues now facing the United States. A broad understanding of cybersecurity issues prepares a framework for the industry- and sector-specific discussions that must take place to truly evolve critical infrastructure security. Although individualized considerations are beyond the scope of this paper, relevant cybersecurity issues are addresses broadly as follows: Part II provides the basic background information and context for the domestic policy challenges today. Part III addresses the persistence of market failures that exist under the current economic incentive structure and concludes that some measure of governmental oversight could help address those failures. In an effort to evaluate proposals for addressing market failures, Part IV expands on suggested economic incentives to promote private sector compliance. Part V discusses what an effective overarching cybersecurity governance structure could look like, describing the value of an empowered and expert agency positioned to oversee cybersecurity issues and possess clear authority to do so. That agency's role *vis a vis* the private sector, as Part VI explains, must be cooperative, with public-private partnerships to create overarching national principles, timely information exchanges, outcome-based standards and best practices, effective enforcement measures, and educational training programs for security professionals. Finally, Part VII summarizes the recommendations of this paper.

II. Background

Although the security problems we face today vary greatly from past experiences, much can be learned from historical comparison. The policy and structural development of the national highway system—its economic and security implications—illustrates the value that a standardized top-down nationwide initiative can provide. By learning from the past, our leaders can effectively coordinate the public and private sector to develop a long-lasting and more secure critical infrastructure.

A. The Information Highway

In 1954, Dwight D. Eisenhower began efforts to upgrade the highway system from a network of two-lane highways running through the main streets of America to a superhighway system.[34] Although automobile technology increased mobility, an inconsistent and dangerous road system constrained it. Few wanted to drive far when "[interstate] travel was a torturous ordeal, marked by rickety bridges and long stretches of mud or gravel between intermittent paved sections."[35]

Eisenhower knew that the existing system was insufficient to facilitate a national defense in the event of another war. Most pressingly, he knew transcontinental mobility was necessary to avoid a second Depression, and a superior highway system would give thousands of military veterans access to jobs nationwide. But building a national highway system that provided safe, secure, and swift intercontinental travel could not be accomplished without national standards for road quality,

[34] *Address of Vice President Richard Nixon to the Governor's Conference*, U.S. Dept. of Transp., http://www.fhwa.dot.gov/infrastructure/rw96m.cfm (last visited Apr. 25, 2012).

[35] T.R. Reid, The Healing of America 13 (2009).

highway identification, and vehicle safety. Adopting effective design standards meant a top-down national approach implemented at the state and local level. This system, formally named the Dwight D. Eisenhower System of Interstate and Defense Highways, facilitated economic growth through a dependable and efficient transfer of goods and services, as well as lower transportation costs and increased productivity.[36] As one observer summarized, the national highway system forever changed American life to include "the suburb, the motel, the chain store, the recreational vehicle, the automotive seat belt, the spring-break trek to Florida, [and] the thirty-mile commute to work."[37]

Like the highway system, the Internet and associated network technology developed unsystematically. The Internet was originally intended for communication only—its developers focused on the twin goals of interoperability and efficiency. Little thought was given to security. Indeed, one early Internet pioneer remarked that "[the] Internet was built in a university research atmosphere where the problems of creating a working system took priority. As the Internet grew, developers had neither time nor energy to address security."[38] As another commenter put it, "We've taken an open system based on anonymity and meant for a small, trusted community of government officials and university scientists, and we've turned it into the backbone of our national commerce and much of our national and military communications."[39] As this history shows, no one expected or prepared for the Internet to become the fundamentally important system it is today.

With so much of our economy and resources dependent on the Internet and information technology, those systems must be secure. President Obama explained in 2009 that the nation's virtual infrastructure is "the backbone that underpins a prosperous economy and a strong military and an open and efficient government."[40] He also explained that the risks to cyberspace are very real:

> [It is] clear that we're not as prepared as we should be as a government or as a country. . . Just as we failed in the past to invest in our physical infrastructure – our roads, our bridges and rails – we've failed to invest in the security of our digital infrastructure[.][41]

Although some entities have implemented proper security measures, those failing to do so lack mechanisms to educate them on cybersecurity standards and practices, norms to follow them, or incentives to take the issue seriously. And when portions of critical infrastructure are left insecure, the entire system is jeopardized.[42]

In discussing how best to incentivize complete security across all critical infrastructure systems, Phil Weiser, Dean of the University of Colorado Law School and Executive Director of Silicon

---

[36] Thomas F. Kaene, *The Economic Importance of the National Highway System*, Pub. Roads, 1996, http://www.fhwa.dot.gov/publications/publicroads/96spring/p96sp16.cfm.

[37] Reid, *supra* note 35, at 15.

[38] David Farber, *Balancing Security and Liberty*, Edge.org (Oct. 30, 2001), http://www.edge.org/documents/whatnow/whatnow_farber1.html.

[39] Joel Brenner, America the Vulnerable 33 (2011).

[40] Barack Obama, President, United States of America, Remarks Introducing a New Cyber Security Initative (May 29, 2009), *available at* http://projects.washingtonpost.com/obama-speeches/speech/317/.

[41] *Id.*

[42] Kim Zetter, *supra* note 10.

Flatirons Center, summarized three possible responses identified by summit participants: (1) realize that there is a threat but avoid understanding it, (2) understand the threat but consider it too complicated to address, or (3) try to understand the threat and take action to resolve it. Intentional ignorance is never the solution, and failure to act is almost as bad. This is especially true if current market failures risking critical infrastructure security can be diminished. Many companies fail to practice basic cyber hygiene and to the extent regulatory oversight can nudge them to increase their security, the public will benefit. In fact, one study concluded that a vast majority of cyberattacks—"between 80 and 90%—could be prevented or successfully mitigated simply by adopting best practices and standards that already exist."[43] Whether or not this account overstates the matter, as Dave Campbell, Founder and principal consultant at Electric Alchemy suggested at the summit, most participants believed that additional security measures can increase baseline protections. Participants also generally agreed that government, in association with the private sector, can increase cybersecurity by developing effective pathways for institutional coordination, norms for greater accountability and concern, and incentives for responsible behavior.[44] Like the national highway system, if the United States can improve critical infrastructure security, innovation and economic growth will flourish.

III. Market Failures and the Role for Government Oversight

One reason for insufficient cybersecurity is that cybersecurity, like public health or national defense, possesses many qualities of a public good (as explained below). Public goods are often underprovided by industries that do not see a financial benefit in offering the good. This section will explain why this is true and how, by avoiding the unintended consequences of legislative efforts and understanding the economic incentives causing market failures, government intervention can improve the state of critical infrastructure cybersecurity.

A. Government Oversight

Despite the risks caused by insufficient critical infrastructure security, summit participants did not agree that government intervention is imperative. After all, government efforts are not guaranteed to resolve market failures or completely eliminate cybersecurity risks, which all participants agreed will be ever-present. However, because critical infrastructure cybersecurity possesses many elements of a public good and is often underprovided by the market, it is clear that government oversight can help.

Public goods are particularly vulnerable to market failures and underproduction due to two distinct characteristics: non-excludability and non-rivalry. If it is physically impossible or prohibitively expensive to prevent individuals from consuming a good, that good is considered non-excludable.[45] No private company can gain from providing an unrestricted good. Likewise, private markets do not

---

[43] *Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Protection, and Sec. Techs. of the H. Comm. on Homeland Sec.*, 112th Cong. 3 (2011) (statement of Larry Clinton, President & CEO, Internet Security Alliance).

[44] Today "DDOS attacks are technically easier to detect and tamp down [than in the past], and most Internet Service Providers (ISPs) offer such mitigation to their clients—for a price." If no price is paid, ISPs may sit there and "watch [a DDOS attack] go by." Stewart Baker, Shaun Waterman & George Ivanov, In the Crossfire: Critical Infrastructure in the Age of Cyber War, McAfee 5 (2009).

[45] Niva Elkin-Koren & Eli M. Salzberger, Law, Economics and Cyberspace 49-50 (2004).

offer a sufficient amount of non-rivalrous goods because such goods are consistently available to any and every individual interested consuming it.[46]

Public health (preventing disease and promoting wellness) for example, is both non-excludable and non-rivalrous. It is non-excludable because all Americans can access and benefit from health research and public education that limits diseases and promote personal well-being.[47] Every American can also benefit equally from public health, with no additional individual diminishing its availability—the definition of a non-rivalrous good.[48] No profit-seeking company would offer these goods because it cannot financially benefit from a good that is not scarce. If a good is not scarce, no individual consumer will pay for it and no market will provide it. Therefore, if government does not alleviate relevant market failures, public goods (like public health) would not be provided.

Professor Deirdre Mulligan, Assistant Professor at the University of California Berkeley School of Information, opened the summit by analogizing critical infrastructure cybersecurity to the public health challenge. To flesh out the analogy, participants then discussed how much security is actually provided by the private sector. Adam Golodner, Director of Global Security and Technology Policy at Cisco Systems, Inc., voiced his belief that market forces are in fact sufficient to incentivize security measures and additional government intervention is unnecessary. Most summit participants agreed that many sectors of the economy are protecting their infrastructure. "Sophisticated actors," said Weiser, "take the threat seriously." Kevin Gronberg, Senior Counsel to the Committee on Homeland Security, illustrated this point in describing grassroots efforts to address security threats in communities like Colorado Springs, Colorado. When businesses increase cybersecurity measures, they decrease the likelihood of attack on their infrastructure. In so doing, they receive a direct benefit and can justify a business case for cybersecurity measures.[49]

Despite these good actors, summit participants agreed that the development of and commitment to maintaining best practices is followed inconsistently and intermittently across critical infrastructure sectors. This is often because security efforts have spillover effects that benefit others connected to or relying upon the secure system. The firms who have failed to adopt sufficient security measures can free ride (intentionally or not) on the investment of others or expect (to the extent they are conscious of the issue) that any consequences of cybersecurity failings will be dispersed and they will not be blamed or unduly harmed.

This free-rider dynamic is one cause of underinvestment in security. Other causes include a lack of marketplace transparency, few market players, and high provider switching costs. For example, when consumers cannot evaluate the effectiveness of security measures, they cannot influence corporate decisions by calling for better or more security. In some sectors, (i.e., regulated energy industry) security is not likely to be a market differentiator because few market players give consumers limited provider options. In other sectors (i.e., water, telecommunications, etc.), switching costs may

---

[46] *Id.*

[47] Mulligan & Schneider, *supra* note 14, at 75.

[48] *Id.*

[49] *Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal: Hearing Before the Subcomm. on Crime and Terrorism in the United States of the S. Comm. on the Judiciary*, 112th Cong. 2-3 (2011) (statement of the Financial Services Roundtable).

be high enough to dissuade consumers from electing a more secure provider. In instances like these (where consumers do not demand increased security and providers are not otherwise incentivized to provide it) infrastructure managers cannot support a business case for increased security.

Whether private returns make investment in security measures worthwhile is a key factor in determining how much security will be adopted, added Howard Shelanski, professor at Georgetown University Law Center. Like public health, unless the private benefits or costs of underproduction incentivize critical infrastructure security, the marketplace is unlikely to produce a sufficient level of investment in cybersecurity on its own. Therefore, without government intervention aligning business and public interests, firms will continue to underprovide cybersecurity.[50]

B. Unintended Consequences of Government Oversight

As with any type of government intervention, unintended consequences can produce significant challenges. Congressional rent seeking and overreach that burdens innovation, violates civil liberties, and wastes resources, can be avoided through conscious intent. Other unintended consequences can be avoided if policymakers understand marketplace dynamics. With these challenges in mind, lawmakers can enact legislation addressing the market forces that underprovide cybersecurity while avoiding harmful implications.

Legislative rent seeking and overreach present relevant concern in any Congressional efforts. According to public choice theory, special interests can influence government actors to choose policies that advance their interests at the expense of the public good.[51] Congress could, for example, mandate technical standards in favor of a specific technology when a more technology-neutral choice might be wiser. Government overreach in areas like cybersecurity presents especially acute concerns in light of recent behavior. Consider, for example, the increase in corporate governance oversight in the wake of the scandals at Enron and WorldCom. Although inappropriate activities by corporate leaders strongly suggested a need for government intervention, many commenters believe that Sarbanes-Oxley went far beyond the specific abuses highlighted in those cases by imposing unnecessarily onerous and poorly designed regulations.[52] One participant described its effect as forcing resources to corporate compliance functions that were needed elsewhere. Although overreach and rent seeking may be difficult to avoid, relevant instances of failure can provide a check on harmful unintended consequences.

Summit participants also discussed potential unintended consequences of government action specific to critical infrastructure cybersecurity. Professional security hackers Chris Roberts, Founder of One World Labs, and Dave Campbell discussed how technological vulnerabilities and strategies to exploit them are evolving much, much more rapidly than any conceivable government framework. And the complex incentives for various critical infrastructure players make broad policies seemingly unhelpful or even harmful. Regulation that fails to address these complexities and technological

[50] Benjamin Powell, *Is Cybersecurity a Public Good? Evidence from the Financial Services Industry*, 4 (Independent Institute Working Paper No. 57) (2001), *available at* http://heartland.org/sites/all/modules/custom/heartland_migration/files/pdfs/28830.pdf.

[51] *See e.g.,* Pierre Lemieux, *The Public Choice Revolution*, 27 Reg. 22 (2004).

[52] *Darned SOX*, Economist, Sept. 14, 2006, http://www.economist.com/node/7914930; *see also, e.g.*, James M. Crowe, *The Unintended Consequences of Sarbanes-Oxley*, Silicon Flatirons Ctr. (2007).

developments will lead to a "check the box" mentality that produces outdated and insufficient security measures.

Golodner also argued that current market incentives may in fact be appropriate, just not yet realized. If that is true, prescriptive measures could set the wrong baseline for security standards, and best practices. Once enacted, legislation is difficult to modify quickly, a problem particularly ill-suited to the ever-changing cybersecurity landscape. Establishing a process-oriented standards framework could also drive the technical experts away from the discussion altogether, an effect all participants agreed would be detrimental.

In light of these and other unintended consequence, Pierre de Vries, Senior Fellow at the Silicon Flatirons Center, commented that those advocating legislation should bear the burden of proving it is necessary. He argued that any type of government action may be more harmful than helpful and should therefore be avoided.[53] In response, Weiser cautioned that it is important to consider the implications of government's failure to act. In doing so, we must identify realistic benchmarks for assessing how government action or non-action affects the marketplace. The following discussion of the current market failures informs the analysis of government inaction by describing the status quo.

C. Market Failures

As will be discussed below, asymmetric information, poorly aligned incentives, inter-temporal choice, and bounded rationality affect decisions made by critical infrastructure market players by favoring minimal security measures. In understanding the incentives that lead to these market failures, government can take legislative steps to correct them while avoiding unintended consequences.

1. Asymmetric Information

Asymmetric information is a lack of equally distributed information between parties to a transaction. When complete and relevant information is unavailable, it becomes impossible to determine exactly how much of a good must be supplied.[54] Therefore, the good is likely to be over- or under-produced.[55] In the security marketplace, the intangible, sometimes unintentional, covert, and dynamic nature of cyberattacks means insufficient information about the threat is available. The quality of security software is also nearly impossible to evaluate at all times. If infrastructure managers do not have sufficient information to correctly analyze the risk of attack or effectiveness of security measures, they will not understand the need for or benefit of cybersecurity investments. As a result, security will be underprovided.

Both the public and private sectors have distinct disincentives to releasing information. The government, for example, often fails to disclose classified information about attempted attacks due

---

[53] Pierre de Vries, *Placebo Legislation Doing Good by Doing Nothing*, Deep Freeze 9 Blog (Feb. 14, 2012 3:18 PM), http://deepfreeze9.blogspot.com/2012/02/placebo-legislation-doing-good-by-doing.html.

[54] Tyler Moore, *The Economics of Cybersecurity: Principles and Policy Options*, 3 Int'l J. of Critical Infrastructure Prot. 103, 108-09 (2010).

[55] *Id.*

to perceived national security benefits.[56] Arguably this happened in Brazil in 2007. After media, including 60 Minutes, reported that the country suffered from power outages due to attacks, the Brazilian government denied the reports and attributed them to "soot-covered" insulators.[57] This type of information about critical infrastructure vulnerabilities could jeopardize public networks to those looking to attack. However, causes of such an attack are important to connected critical infrastructure entities that would likely increase security measures if made aware of the risk. [58] Therefore, a core public policy challenge is facilitating the free flow of information in a way that protects the interests of all parties without increasing security risks.

In the private sector, software developers (i.e., developers of security software, operating systems, database software, etc.) and critical infrastructure managers are incentivized to underreport vulnerabilities and attacks. Software developers are often unlikely to publicly disclose software quality problems.[59] Evidence indicates that public notice of software weaknesses by the vendor, competitor, or client reduces the vendor's stock price by 0.6% or approximately $0.86 billion in average market cap per vulnerability announced.[60] If firms avoid public disclosure, parties relying on their software may not know that additional security is necessary.[61]

There are also reasons to believe critical infrastructure managers routinely underreport what they know about potential breaches absent a legal requirement to do so.[62] Like software developers, publicly releasing hacking information may harm their market share, reputation, and customer base (in markets in which consumers have provider choices).[63] Notice of an attack or vulnerability may also incite increased regulatory attention, which can increase the cost of doing business for both the company and the industry as a whole.[64] Finally, by publicly disclosing vulnerabilities, a company may increase the likelihood of future attack by signaling its weaknesses to potential hackers.

2. Misaligned Incentives

In the cybersecurity market, incentive structures also favor infrastructure managers and software vendors at the expense of the public. Industry players are increasingly incentivized to move their infrastructure online and rely on information technologies that create efficiencies and allow for innovation, but which also create greater vulnerability. For infrastructure managers, moving control

---

56 Eric Goetz, Critical Infrastructure Protection 37 (2008).

57 Zetter, *supra* note 10.

58 *Id.*

59 Rahul Telang & Sunil Wattal, *Impact of Software Vulnerability Announcements on the Market Value of Software Vendors-an Empirical Investigation*, 33 IEEE Transactions on Software Eng'g 8, 8 (2007).

60 *Id.*

61 This is true to the extent it is not financially beneficial to disclose the vulnerability (i.e., the vendor believes a third party will disclose and believes a defensive disclosure will soften the impact on its stock). *Id.* at 11.

62 Joel Brenner, America the Vulnerable 107 (2011).

63 Matt Egan, *Disclosure Debate When Should Companies Reveal Cyber Attacks*, FOX Business, Oct. 28, 2011, http://www.foxbusiness.com/technology/2011/10/28/disclosure-debate-when-should-companies-reveal-cyber-attacks/.

64 *See, e.g.,* Roland L. Trope & Sarah Jane Hughes, *The SEC's Staff "Cybersecurity Disclosure" Guidance: Will it Help Investors or Cyber-Thieves More?*, A.B.A., Dec. 19, 2011, http://apps.americanbar.org/buslaw/blt/content/2011/12/article-3-trope-hughes.shtml (The SEC now requires disclosure on cyberattacks, but the regulations are uncertain as of yet and may have unintended consequences).

systems online and allowing them to run concurrently with other information technology networks on one system produces economies of scale, consolidates resources, and allows remote access and control. However, as "power grids, telecommunications networks, banks, [and] transportation[systems become] interdependent[,]"[65] the number of access points by which a hacker can reach the united system grows, as does the potential breadth of an attack. A breach that once was limited to a local bank or power supply before it moved its controls online can now reach all connected systems with little additional effort by the hacker.

The interconnected network, which extends far beyond any individual company, means the traditional cost-benefit analysis does not apply to critical infrastructure cybersecurity. The transaction costs of contacting and influencing the security of every party connected to the infrastructure network (including software vendors and consumers) are too high. Yet without every element secure, the entire system is vulnerable. This reality keeps the likelihood of a successful attack high. If the risk remains high regardless of security measures, infrastructure managers will likely rely on the security provided by those to whom they are connected, if it is available, or they will provide no security at all because no business case justifies the cost. Supporting this view at the summit, Roberts and Campbell described personal experiences with businesses that made conscious efforts to spend as little on security as possible, increasing it only when absolutely necessary.

Software vendors also have little incentive to conduct research and development on security measures because their customers (i.e., infrastructure managers) have difficulty evaluating the effectiveness and implementing additional security measures. Although they could (and often do) educate their customers as to existing risks, one can skeptically view such information as self-interested. "[W]hen the quality is not readily observable to the customer, and special effort or cost must be incurred to assess the quality . . . competition among sellers for customers' dollars tends to lower the quality[.]"[66]

Another core challenge to software security is that making software more secure can interfere with or make day-to-day activities more difficult for users. For example, a utility must provide electricity consistently and without interruption. If security software interferes with or delays repair efforts, the utility managers might avoid using it so the efforts of their maintenance professionals are not delayed. As a result, software vendors profit from speed to market and unique features instead of a more secure product.[67] "Indeed, the current maxim among software companies appears to be 'ship now, patch later'—a policy that has produced a software infrastructure riddled with security holes."[68] As long as market incentives favor infrastructure managers and software vendors at the expense of the public, critical infrastructure security will remain insufficient.

---

[65] Goetz, *supra* note 56, at 34.

[66] Karim Jamal & Shyam Sunder, *Monopoly or Competition: Standard Setting in the Private and Public Sector* 10 (preliminary draft, 2007).

[67] Alderson & Soo Hoo, *supra* note 22, at 8.

[68] *Id*. This dynamic may be changing with the development of Secure by Design efforts as described in more detail below.

3. Inter-temporal Choice Problem

The inter-temporal choice problem describes the situation in which individuals must evaluate and assign value to outcomes that will happen at different points in time—one immediately, and another in the future.[69] A student who chooses to watch a football game instead of studying for the next day's chemistry test allocates more value to the game than her education or grades. Because uncertainty surrounds the future outcome (the student could perform very well on the test despite a lack of studying), and people are generally impatient and prefer immediate gratification, economic theory indicates that many assign more value to the immediate implication than the future benefit.[70]

In the cybersecurity context, infrastructure managers must decide whether to implement high-cost security measures today or potentially face a security breach in the future.[71] By choosing to adopt only minimal security measures at little or no cost today, money can be applied to seemingly more acute needs (i.e., payroll, product maintenance, customer upgrades, advertising). Without reliable information to confirm the high risk of future breach, cost of cleanup, or significant reputational repercussions, managers are unlikely to spend money on increased security measures in the short term.

In an encouraging trend, cybersecurity spending has increased in recent years due to a number of high-profile attacks and security breaches in the commercial sector in 2011 (dubbed "The Year of the Hack").[72] Although all of the publicity is increasing the availability of information, it has unexpected consequences. Roberts commented that, in his experience, publicity is actually causing complacency as society begins to consider hacks normal. Further, hacks thus far have happened in the general commercial setting. Although much can be learned from them, more detailed and reliable information about the costs and implications of attack in the critical infrastructure sector must be made available to increase focus on security measures. Without such information, infrastructure managers will continue to favor short-term spending over valuable long-term security investments.

4. Bounded Rationality

"Bounded rationality occurs when individuals' rationality is constrained by imperfect information, cognitive limitations, . . . time pressures[,]"[73] or extremely complex circumstances. In bounded situations, it is impossible to know all of the information and fully understand it. As a result, individuals rely on heuristics[74]—consistent measures such as rules of thumb, established techniques, or standardized procedures—to support problem-solving. Although helpful, these techniques can have negative consequences. When individuals rely on heuristics to make decisions, they may "fear

[69] Daniel Read, *Intertemporal Choice* 1 (London Sch. of Econ. and Political Sci., Working Paper No. LSEOR 03.58, 2003).

[70] *Id.* at 2.

[71] Baker, Waterman & Ivanov, *supra* note 44, at 9-11.

[72] Nathan Eddy, *Cyber-Security Spending to Hit $60 Billion in 2011*, EWeek.com, Dec. 2, 2011, http://www.eweek.com/c/a/Security/Cyber-Security-Spending-to-Hit-60-Billion-in-2011-121173/; Leibowitz, *supra* note 7. Ironically, during the three hour summit the CIA's website was taken down by Anonymous. Matthew J. Schwartz, *CIA Website Hacked, Struggles to Recover*, InformationWeek.com, Feb. 13, 2012, http://www.informationweek.com/news/security/attacks/232600729.

[73] Michelle Baddeley, *Information Security: Lessons from Behavioral Economics*, Network 5 (2011).

[74] *See e.g.,*Suren Basov, Liam Blanckenberg & Lata Gangadharan, *Behavioural Anomalies, Bounded Rationality and Simple Heuristics* (The University of Melbourne, Working Paper No. 2012, 2007).

things that are not dangerous, and . . . not fear things that impose serious risks."[75] Vivid and easily imagined situations, for example, are considered more realistic than less vivid examples. The global preoccupation with the horrific September 11 attacks on the World Trade Center in New York City led to a highly elevated fear of terrorist attacks in the United States; higher than the evidence justified.[76] On the contrary, events that are not as vivid or recent are difficult to evaluate or understand, and the potential of the occurrence may be underestimated.[77]

Extreme complexity, insufficient information, and the unknown cost of a cyberattack limit available information on which infrastructure managers can rely, forcing them to act in bounded rationality. Fundamentally, the technology on which critical infrastructure relies is constantly in flux, making solutions unbelievably complex. That technology makes up the interconnected infrastructure system, vulnerable to security failures in any connected element and its supply chain. In such a situation, decision-makers cannot connect the cost of security to its benefits. Instead, they frequently believe they have either overspent on security (if no attack occurs) or underspent (if an attack occurs, but managers don't know how much more security would have prevented it).

To make matters worse, industry players "do not know how to value (i) confidentiality of information, (ii) integrity of information, or (iii) the pain of dealing with recovery from an attack's effects."[78] If it is impossible to quantify the risk or impact of attack, corporate leaders either view the threat as unimportant or hopeless. Under such constraints limiting detailed and digestible threat information, decision-makers are unlikely to adopt additional security measures to protect their software or infrastructure.

5. Negative Externalities

Negative externalities exist when parties to a transaction do not internalize the cost of the transaction. Instead, third parties bear the cost. Negative externalities allow critical infrastructure managers to avoid much of the cost of an insecure infrastructure, causing a divergence between the private and social costs of insecurity. If the market pricing mechanism fails to align private and social costs such that the optimal private amount is greater than or less than the socially optimal amount, a market failure exists.

A common example of negative externalities happens in the environmental context. A chemical plant may produce harmful air pollution. The plant owner could internalize the cost of the pollution by spending the money necessary to filter or reduce toxic pollutants. Alternatively, he could let the pollutants filter out into the surrounding community and internalize nothing. The released pollutants represent an externality, the cost of which a third party (in this case the surrounding community) must internalize.

Like the errant pollutants, an insecure critical infrastructure imposes negative externalities on

[75] Cass R. Sunstein, *Misfearing: A Reply* 2 (John M. Olin Law & Economics Working Paper NO. 274, 2006).

[76] *Id.* at 8.

[77] Mulligan & Schneider, *supra* note 14, at 73.

[78] *Id.*

the public.[79] A simple example demonstrates why some critical infrastructure managers are unlikely to take into account the harmful externalities of a critical infrastructure attack.[80] A utility evaluates corporate spending in light of business missions and objectives. Because the most pressing business concern is continuity of service at a reasonable price, a CEO is likely to allocate significant funds to support that goal. Protecting the integrity of the system against hackers is an important concern, but the amount of security investment will depend on the perceived risk of attack. That risk is a factor of the likelihood of a successful attack and the financial implication of that attack.

Level of Security	Likelihood of Successful Attack	Cost of Security	Expected Loss from Breach	Total Expected Cost	Externalities The Public Incurs
High	0.3	$0.5M	$0.3M	$0.8M	?
Low	0.7	$0.0M	$0.7M	$0.7M	?

Using the chart laid out above, an executive could spend half a million dollars to implement high security measures that allow only 30% likelihood of a successful breach by the attacker, or he could spend a nominal amount on basic security measures that would allow a 70% likelihood of successful attack. If the estimated cost of breach is $1 million, high security measures under an expected attack would cost a total of $800,000, while lower security measures would produce a total cost of only $700,000. A profit-maximizing executive could save an estimated $100,000 by instituting minimal security measures.

This risk matrix takes into account only the estimated cost of a successful attack to the organization, and it fails to account for the cost to the public or other systems using the same critical infrastructure network.[81] Those externalities could be significant if the utility is shut down for weeks or even months. The infrastructure manager who fails to protect his own system creates vulnerabilities and associated losses for the entire interconnected system and the public. Yet unless his is forced to factor those externalities into his risk analysis, he is not incentivized to increase security.

D. Solutions

Asymmetric information, misaligned incentives, inter-temporal choice, bounded rationality, and negative externalities cause cybersecurity market failures, give private actors insufficient ability or incentive to invest in cybersecurity. These market failures, in addition to the public good-like qualities, mean that cybersecurity is likely to be underprovided across many sectors. Insufficient critical infrastructure cybersecurity increases the likelihood of a catastrophic event and jeopardizes the nation's economic, military, political, and environmental safety.

Government traditionally responds to such a threat by modifying market incentives and compelling production of the good. Although many summit participants agreed that some government intervention would improve the state of affairs, no consensus existed as to the level or structure of such intervention. Regardless, Congress is currently considering legislation to avert

[79] Johannes M. Bauer & Michel van Eeten, *Securing Cyberspace: Realigning Economic Incentives in the ICT Value Net*, WebScience 2 (2009) http://journal.webscience.org/171/1/Bauer_VanEeten_WebSci09_Athens_fin.pdf.

[80] This example is adapted from Goetz, *supra* note 56, at 35.

[81] *Id.* at 36.

cybersecurity market failures. It is clear that legislation designed to deter every possible cybersecurity risk will inevitably fail because absolute security is not attainable.[82] *The appropriate policy goal should be to eliminate all reasonably avoidable risk based on best practices that balance both the relevant benefits of cybersecurity investment and the relevant harm from failing to invest.* A focus on "vulnerabilities whose exploitation (i) is sufficiently likely to occur based on perceived threats and (ii) could enable expensive (by some cost measure) system compromises"[83] is much more realistic. With this in mind, the following sections address the effectiveness of proposed market incentives and governance structures to aid regulators in determining the most appropriate legislative regime to correct market failures.

IV. Correcting Market Failures

"[Ensuring] that actors contribute to public cybersecurity requires interventions to overcome positive and negative externalities that lead rational individuals to underinvest."[84] Government can help accomplish this by modifying market incentives in a way that helps create a business case for security investment. In doing so, market players will see a reason to develop processes and strategies to improve systems and identify and resolve risks and vulnerabilities. Summit participants identified that market incentives are working in some critical infrastructure sectors. Others, like "utilities, oil and gas, transport, telecommunications, chemical, emergency services, and postal and shipping industries[,]" remain vulnerable to attack, indicating the failure of free market incentives.[85]

One reason for underinvestment in these sectors is a lack of financial justification. The cost of security is expensive and the impact of an attack is very difficult to quantify. For example, although nearly impossible to assess over time, it is estimated that the energy grid requires a nearly $3.7 billion investment today.[86] Such an investment would be easy to justify if used to defend against a concrete harm. However, despite circumstantial evidence strongly supporting the threat, a critical infrastructure attack is impossible to quantify in advance. To make the cost of insecurity tangible, economic incentives must directly impact the financial well-being of private sector critical infrastructure managers and their supply chains.

However, for economic incentives to work, market players must be accountable for and understand the implications of their actions. Well-defined legal duties will allow market players to clearly understand their responsibilities, see a need to reduce risks, and be held accountable for failing to adopt security measures. With duties defined, limitations on liabilities created by those duties can incentivize action. Other economic incentives include mandatory disclosure requirements, robust insurance markets, direct expenditures, and government procurement. This section will first evaluate the difficulties in defining duties. It will then consider the effectiveness of proposed market incentives,

---

[82] Mulligan & Schneider, *supra* note 14, at 72-73.

[83] *Id.* at 73. Mulligan & Schneider term managing these risks the Doctrine of Risk Management and argue that it is more likely to increase security than the *Doctrine of Prevention* (absolute security goals) or the *Doctrine of Deterrence through Accountability* (criminalizing attacks). *Id.* at 72-75.

[84] *Id.* at 77.

[85] Fran Howarth, *Critical Infrastructure Under Attack*, Computer Weekly Blog (Feb. 10, 2011, 6:11 PM), http://www.computerweekly.com/blogs/Bloor-on-IT-security/2011/02/critical-infrastructure-under-attack.html.

[86] MIT Energy Initiative, *supra* note 16, at 210.

suggesting which might be successful and which will likely fail to encourage proper security measures.

A. Defining Legal Duties

Summit participants agreed that clearly defining legal duties allows for accountability and gives market players the ability to understand their required roles and the associated cost of failing to meet them.[87] At this time, the legal duties of most critical infrastructure market players have not been well defined. Some legal scholars believe that officers and directors (of ISPs or critical infrastructure managers) already have a fiduciary duty to secure the company's systems against attack, and that the common law imposes a duty to provide cybersecurity, the violation of which sounds in tort.[88] Yet market players other than officers and directors are likely to influence the state of cybersecurity, and we know little about these duties. Without clear definitions, economic incentives will have little impact on security. However, summit participants agreed that defining duties will not be any easy task.

To begin, unintended consequences of defined duties are likely. Therefore, government must guard against potential pitfalls by carefully imposing, defining, and clarifying the scope of the duty and associated liabilities. Only those able to affect the state of cybersecurity should have a duty to act, and that duty should only extend as far as it provides a net social benefit.[89] For example, although software producers design secure products when released to the market, those products are connected to a network of insecure legacy systems that make it impossible for the software to be constantly secure.[90] Burdening software producers with a duty to create completely secure products is not the proper regulatory solution because producers are not in complete control of the software. Additionally, strict duties force software producers to choose between security and product cost and speed to market, possibly diminishing the availability of software.[91] If not carefully guarded against, these types of unintended consequences could greatly harm industries supporting critical infrastructure.

Even if duties are perfectly defined and properly allocated, it is impossible to avoid all risk and extremely difficult to allocate fault. As previously discussed, all risk cannot be eliminated. Ari Schwartz, Senior Advisor to the United States Department of Commerce, commented that all market players assume that at one point they will the subject of an attack. When an attack does occur, the

---

[87] *See* Bruce Schneier, *Liability Changes Everything*, Schneier Blog (Nov. 2003), http://www.schneier.com/essay-025.html; Douglas Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 221, 221 (2006). Increased criminal liability for hackers presents another solution, the viability and effectiveness if which is not addressed in this document.

[88] Steven R. Jacobs & Stephanie L. Chandler, Business Leaders Must Address Cybersecurity Risk, Jackson Walker L.L.P. 1 (2011). Proving negligence in the information technology world comes with its own set of difficulties. A successful claimant will need to prove (1) a duty was owed, (2) the duty was breached, (3) the breach caused the harm, and (4) the amount of harm caused by the negligent act. Even by clarifying the legal duties, the intangible nature of technology (especially when the offender's operations are clandestine) makes proving the other elements of a negligence claim difficult.

[89] Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 17 Wm. & Mary L. Rev. 239, 265 (2005).

[90] Task Force on Security Across the Software Development Cycle, Process to Produce Secure Software, National Cyber Sec. Summit 7 (Samuel T. Redwine, Jr. & Noopur Davis, eds. 2004) ("Contrary to what most users and even many developers assume, security functionality does not necessarily provide genuine security; security is a systems property emerging from the totality of system behavior.").

[91] Timothy B. Lee, *So Sue Me: Are Lawyers Really the Key to Computer Security?*, ArsTechnica, July 2011, http://arstechnica.com/tech-policy/news/2011/07/will-your-employer-get-sued-for-your-security-screw-ups.ars; Alderson & David Soo Hoo, *supra* note 22, at 9 (explaining that allocating liability to software vendors may drive many from the open source market).

many interconnected market players make it equally impossible to determine who is at fault. For example, most software is "written and upgraded by different coders at different times, and usually with no master plan, say experts. [It often contains] a patchwork of code, objects and platforms with known vulnerabilities[.]"[92] This is especially true in the cloud where applications are tacked and merged together with new and legacy systems, increasing complexity and vulnerability.[93] In the aftermath of an attack, it would be nearly impossible to determine which software producer is responsible for the harm.[94]

The summit discussion did not delve into the details of imposing duties or liabilities, but the difficulty in implementing such regimes was clearly apparent. However, it was clear that the difficulty of allocating responsibility and identifying the cause of the harm makes it unlikely that market players will willingly let their Congressional representatives pass legislation imposing cybersecurity duties. If they are defined, they must be crafted with a contract law framework in mind. As Brian Hendricks, Head of Technology Policy Nokia Siemens Network, noted during the discussion, many companies will attempt to contract their duties away as they do in most other circumstances today. Despite these inherent difficulties, participants agreed that defining duties and liabilities will help industry players understand the implications and costs of failing to implement security measures.

B. Possible Economic Incentives

Economic incentives are financial incentives used to elicit desired behavior by targeting industry self-interest. Proposed incentives include liability limitations, mandatory disclosure requirements, cyberinsurance, direct incentives, and government procurement. To produce the intended result, incentives must be thoughtfully and carefully tailored to the industry, market player, and risk. For example, R&D tax incentives "may be the most attractive option for an IT security vendor, while a defense firm may be more interested in procurement options, an electric utility in a streamlined regulatory environment or an IT-user enterprise in an insurance discount and risk transfer[.]"[95] Improperly tailored incentives will waste time and money, and possibly cause unintended consequences.

1. Liability Limitations

Once legal duties are created, regulators can incentivize investment in cybersecurity measures by extending new limitations on liabilities. Because liability limitations can greatly benefit corporations, they can align corporate and public policy goals in favor of security measures. Types of limitations include eliminating liability entirely, limiting non-economic damages,[96] capping actual damages, or

---

92 Deb Radcliff, *Code Surety: Secure by Design*, SCMagazine, Mar. 1, 2012, http://www.scmagazine.com/code-surety-secure-by-design/article/228646/.

93 *Id.*

94 A small but growing number of software producers are learning to adapt to the current market. "Secure by design" efforts and similar innovative attempts to create secure software from the ground up by building planning and maintenance into the development architecture are increasing. *Id.*

95 Bus. Software Alliance et al., Improving our Nation's Cybersecurity Through the Public-Private Partnership 11 (2011).

96 Non-economic damages may include damages for pain and suffering, humiliation, embarrassment, worry, mental distress, loss of enjoyment of normal activities, benefits and pleasure of life, loss of mental or physical health, well-being, or bodily functions, loss of consortium, society, and companionship, or loss of love and affection.

eliminating punitive damages. These limitations incentivize self-regulation through significant financial implications. If companies know that compliance limits their potential liability, they can know and prepare for potential costs in case of a disaster. This is most important in high capital or risky industries critical to national independence, innovation, growth, and competitiveness. Without limiting liability, damages awarded in a tort suit could be so great that potential market players may never enter the market and critical infrastructure services would be underprovided.[97]

Safe harbor protections—one common example of liability limitations—might be particularly helpful in critical infrastructure cybersecurity because they can incentivize security measures and facilitate self-regulation. These legal protections can do so in two ways: (1) operators that comply with approved self-regulatory guidelines are "deemed to be in compliance" and (2) there is "flexibility in the development of self-regulatory guidelines" that "[take] into account industry-specific concerns and technological developments."[98] Existing legislation is helpful in determining how best to implement safe harbor protections. The Children's Online Privacy Protection Act (COPPA), for example, "provides both federal and state enforcement mechanisms and penalties against operators who violate the provisions of the implementing regulations."[99] The statute establishes an optional safe-harbor program as an alternative means of compliance for operators that follow self-regulatory guidelines, which must be approved by the FTC under a notice and comment procedure.[100] COPPA requires that approved safe harbor programs engage in ongoing monitoring of their members' practices to ensure compliance,[101] and firms that resist joining remain subject to statutory requirements. Although critics argue that COPPA is not effective, Congress determined that the safe-harbor provisions do in fact effectively enforce the goals of the legislation.[102]

Despite the benefit of liability limitations, they may not effectively incentivize additional security. First, without well-defined duties, limitations may have not effect at all. After all, if the threat of suit in the face of uncertain liability (as exists today) does not incentivize adoption of security measures, further reducing liability will do little good. If a local utility, for example, is not legally liable for failing to use security software, reducing that liability will not suddenly encourage adoption.

Additionally, the possibility of creating reverse security incentives exists. In industries where risk is erratic and uncertain, or potentially very great (i.e., offshore drilling accident or a critical infrastructure attack), liability limitations may favor less security by allowing infrastructure managers to factor the cost of liability into their risk calculation and hedge against that risk with insurance or pass the costs along to customers (if in an unregulated industry). The Oil Pollution Act of 1990,

---

[97] Blair N.C. Wood, *The Oil Pollution Act of 1990: Improper Expenses to Include on Reaching the Limit on Liability*, 8 Appalachian L.J. 179, 185 (2009) ("It is well established that limits on liability are necessary for the stability of certain industries and for the stability of the U.S. economy. These limits are an incentive to encourage companies to take part in potentially hazardous activities such as transporting oil. Without the institution of reasonable limits on liability, companies would be discouraged from participating in these types of businesses, many of which are essential to the economy.").

[98] Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes* 394-96 (New York University Public Law and Legal Theory, Working Paper No. 181, 2010).

[99] *Id.* at 395.

[100] *Id.* at 395-96.

[101] *Id.* at 397-98.

[102] *Id.* at 405.

for example, created strict liability for oil spills, but capped claims for offshore drilling accidents at $75 million. By limiting the cost of lawsuit, it intended to encourage investment in the industry despite a high cost of capital. In 2010 this cap produced the opposite effect. The Center for American Progress testified before Congress that the cap allowed careless behavior by the companies involved in the Gulf of Mexico oil spill, and that "raising or eliminating the cap would have changed company behavior."[103] As such, limiting liability allowed managers to factor risk into their pricing structure instead of attempting to avoid it by implementing costly security measures. In these instances, liability limitations and caps deny just and fair recovery of damages and undermine deterrence goals for critical infrastructure managers.[104]

Finally, liability limitations should be structured carefully to produce a financial incentive clearly tied to appropriate outcomes. When liability regimes are clearly defined and entities face obvious and discernibly high costs for failing to adopt required security measures, they are more likely to adopt those measures. However, the cost of investment must be less than the economic benefit provided by the liability limitation. For example, if the liability limitation benefits a utility by $30,000, but the cost of security over time is $100,000, there is no incentive to incur the cost of security. Further, if the liability limitations are not tied to continuously improved or outcome-based standards, the limitation will be ineffective in the face of changing technology and result in a "check the box" mentality. Ultimately, if the liability limitations are awarded in light of clearly defined liabilities and structured properly, this type of economic incentive can reinforce national policy goals. If they are improperly structured or awarded when liabilities are uncertain, not only will they fail to increase security measures, but they will produce dangerous unintended consequences.

2. Mandatory Disclosure Requirements

Mandatory disclosure requirements for critical infrastructure vulnerabilities and breaches represent another economic incentive solution that can manage risk and increase transparency. Many states have enacted similar disclosure laws for data breaches by requiring notice to customers when breaches occur.[105] Driving the laws is the belief that companies will want to avoid the high cost of bad publicity and will therefore proactively adopt additional security measures. Increased transparency around breaches also provides valuable information that can help companies better understand the risk and return on security investment.[106] Unfortunately, it is still unclear whether these data breach laws achieve their intended purpose, as empirical evidence indicates that they have only nominally

[103] Andrew F. Popper, *Capping Incentives, Capping Innovation, Courting Disaster: The Gulf Oil Spill and Arbitrary Limits on Civil Liability*, 60 DePaul L. Rev. 975, 990 (2011). The British Petroleum oil spill off the Gulf Coast caused 11 deaths, spilled approximately 185 million gallons of oil, and produced billions of dollars of economic loss to the shipping, fishing, and tourist industries. Tamara Lush, *Gulf Oil Rig Workers' Families: Remembering the 11 Who Died*, Huffington Post, May 4, 2010, http://www.huffingtonpost.com/2010/05/04/gulf-oil-rig-workers-fami_n_562239.html; Susan Lyon & Daniel J. Weiss, *Oil Spills By the Numbers*, Ctr. for Am. Progress, Apr. 30, 2010, http://www.americanprogress.org/pressroom/releases/2010/04/oilspill_bythenumbers.html; *Gulf of Mexico (2010)*, N.Y. Times (last viewed Apr. 25, 2012), http://topics.nytimes.com/top/reference/timestopics/subjects/o/oil_spills/gulf_of_mexico_2010/index.html?offset=0&s=newest.

[104] Popper, *supra* note 103, at 989.

[105] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Ground*, 63 Stan. L. Rev. 247, 292-93 (2011).

[106] Mulligan & Schneider, *supra* note 14, at 74.

reduced identity theft.[107]

At the summit, many participants expressed skepticism at the benefit of disclosure regulations for critical infrastructure. Roberts reiterated that shaming mechanisms diminish in effectiveness as hacks become a regular occurrence. Further, attribution is not always easy in the cyber context. If disclosure exists but the cause of the vulnerability or the harm is too difficult to identify, shaming does little to rectify the problem.

3. Cyberinsurance Market

A robust cyberinsurance market may also promote adoption of security measures, encourage best practices, create industry standards, and limit critical infrastructure losses.[108] Today, however, the percentage of critical infrastructure insured against attack remains woefully low. If government can incentivize a strong cyberinsurance market, insurers can police adoption of standards and best practices and increase the baseline level of security.

As with any other industry, cyberinsurance shifts the risk and cost of attack away from critical infrastructure managers by allowing them to contract away the downside of an attack.[109] However, for "cyber-insurance to be an effective tool in encouraging the adoption of best practices, cyberinsurers should conduct further research on authoritative risk indicators; compile data on security breaches and the implementation of preventative measures; and develop actuarials that accurately assess the risk of cyberthreats and the cost of harms that result from online attacks."[110] Cyberinsurers, who have a lot of "skin in the game" if an attack occurs, can use this information to demand and reward security measures and best practices.[111] Much like car insurance providers reward their insured for precautionary measures and careful driving practices,[112] cyberinsurers could offer lower premiums for those who adopt additional security. If insurance providers are able to document the level of industry preparedness and better understand the state of security, insurance premiums will be more reasonable and insurance policies increasingly available.

We can learn much from the more robust cyberinsurance market existing in the commercial context. Such policies are frequently found in professional liability and in errors and omissions liability contracts.[113] Disclosure laws and increasingly available information on attacks in the commercial context,

---

107 Sasha Romanosky, Rahul Telang, & Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. of Pol'y Analysis & Mgmt. 256, 256 (2011) (an empirical study indicating that the data breach reporting laws in effect between 2002 and 2007 reduced identity theft by about 2%).

108 Internet Policy Task Force, Cybersecurity: Innovation and Internet Economy, Dept. of Commerce 24-27 (2011).

109 Moore, *supra* note 54, at 115 (2010).

110 Internet Policy Task Force, *supra* note 108, at 25.

111 Moore, *supra* note 54, at 115 (2010).

112 *How Snapshot Works,* Progressive Ins. http://www.progressive.com/auto/snapshot-how-it-works.aspx (last visited Apr. 26, 2012).

113 Sarah Coffey, *Liberty Mutual Unit Enters Burgeoning Cyber Insurance Market*, Boston Bus. J., March 2, 2012, http://www.bizjournals.com/boston/print-edition/2012/03/02/liberty-mutual-unit-enters-burgeoning.html (describing the growing market insuring data privacy breaches and technology errors and omissions).

for example, proved to be one catalyst for increased availability of insurance.[114] Extending disclosure laws to critical infrastructure could have the same effect. The Securities and Exchange Commission regulation that requires companies to provide a "description of relevant insurance coverage"[115] is one type of regulatory nudge that can significantly increase the adoption of cyberinsurance in the critical infrastructure context.

Other lessons can be learned from the fact that cyberinsurers in commercial contexts do not always act as anticipated. Instead of basing criteria on security measures, they consider factors like firm size.[116] They are also not amassing claim histories, which would help transparency efforts.[117] Policies are also generally limited to small types of harms as "[some] do not offer policies for computer viruses because reinsurance companies, which insure the insurers, are often nervous about widespread attacks that can affect multiple insurers at once[.]"[118] The 2011 attack on Sony, in which the personal information of 24.6 million users was stolen,[119] is a good example of the type of wide-spread impact that scares insurers today.

As in the Sony matter, the advent and development of technology creates tension in insurance contracts, which produces uncertainty about enforceability. "[As] technology evolves, [insurers] are creating new policies to address the latest threats, including the risk of data loss and business disruptions from cloud computing."[120] Although contracts reflecting new technology will increase the success of security measures, contracts failing to cover new types of attacks are ineffective. For example, Sony's insurer, Zurich American Insurance, argued that Sony's insurance policy did not cover the cyberattacks.[121] If instances like these are prevalent and parties cannot rely on insurance contract, the cyberinsurance market in the critical infrastructure context will prove less valuable than anticipated.

4. Direct Expenditures

Direct expenditures, another possible economic incentive, are awarded "when the government takes taxpayer dollars and gives them to others to spend for a specific purpose."[122] Direct spending allows the government to identify and resolve delayed adoption of security measures. For example, if it is determined that utility providers require security measures unnecessary in other critical infrastructure

114 John Doernberg, *New Cybersecurity Disclosure Guidance for Public Companies: Focusing Attention, Raising Questions*, William Gallagher Assoc., 4-5 (2011), http://www.wgains.com/Assets/WhitePapers/NewCyberDisclGuidance.pdf.

115 *Id.*

116 Moore, *supra* note 54, at 115.

117 *Id.* at 115.

118 Gerald Smith, *Cyber Insurance Offers Peace of Mind from Digital Disaster*, Huffington Post, Sept. 30, 2011, http://www.huffingtonpost.com/2011/09/30/cyber-insurance_n_989573.html.

119 Jason Schreier, *Sony Hacked Again; 25 Million Entertainment Users' at Risk*, Wired, May 2, 2011, http://www.wired.com/gamelife/2011/05/sony-online-entertainment-hack/.

120 Smith, *supra* note 118.

121 Nicole Perloroth, *Insurance Against Cyber Attacks Expected to Boom*, Bits Blog, Dec. 23, 2011, http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom/ ("At last count, it had 100 million compromised customer accounts, and Sony anticipated the debacle would cost $200 million. With 58 class-action suits in the works, that may be wishful thinking.").

122 *Tax Expenditures 101: What They Are and How They Slip Under the Radar*, Ctr. for Am. Progress, Apr. 15, 2010, http://www.americanprogress.org/issues/2010/04/tax_expenditures101.html.

sectors, direct expenditures can incentivize those managers to adopt such measures without overly broad measures. Therefore, direct expenditures can limit wasteful awards on those who do not need the nudge, and can be structured to effectively address long-term goals.

Melodi Gates, an associate at Patton Boggs LLP and prior CISO in the telecommunications industry, pointed out that the meaningful use incentives for electronic health records, as created in the American Recovery and Reinvestment Act of 2009 (ARRA), represents one example of how dynamic direct expenditures can be.[123] The Act allocated $2 billion for the creation and development of health information exchanges through "meaningful use" of health information technology.[124] To incentivize continued development of these systems past initial adoption, funding is awarded in connection with criteria that evolve over time.[125] Stage 1 sets the baseline for adoption, and stages 2 and 3 develop that baseline over five years.[126] The full impact of this type of direct expenditure has yet to be seen, but it is clear that these direct expenditures can be targeted. As a result, they may provide an effective method to develop and improve security measures beyond minimum standards and best practices.

Grant funding, another form of direct spending, has been proposed as a way to incentivize cybersecurity measures and might be effective in limited instances. Government grants should require adoption of (at least) minimum security requirements, i.e. encryption, virus scanning software, etc. The security requirements (at best) should be specific to the grant recipient, thereby including detailed and protective security requirements. The types of applicable grants could include national security grants, emergency preparedness and response, research and development, funding to purchase security equipment, and to train security personnel.[127] In attaching security requirements to existing grants, taxpayers will pay little in administrative fees while greatly benefitting from increased adoption of security measures.

Including additional requirements in grant proposals is not without drawbacks, however. Grant eligibility is limited to certain entities that are able to navigate the already difficult regulatory process, making the incentive relatively limited in scope. By adding cybersecurity requirements, grant compliance will be more difficult and costly for applicants. These costs will likely be passed along to consumers. Further, security requirements and standards set in the initial grant could be quickly outdated due to technological development. And, if they are too strict, the benefit of the grant may be delayed or become too costly to implement. Regardless, the costs may be justified by the security and reinforce the benefit of direct expenditures.

5. Government Procurement Process

"The federal government procures billions of dollars of goods and services annually."[128]

[123] 42 U.S.C.A. §§300jj-33 (h)(2009).

[124] ARRA HITECH FAQs Related to HIE, HIMSS Health Information Exchange 1, 3 (2009).

[125] *Id.* at 3.

[126] *Overview- EHR Incentive Programs*, CMS.gov, https://www.cms.gov/EHRIncentivePrograms/30_Meaningful_Use.asp#BOOKMARK2 (last visited Apr. 25, 2012).

[127] Bus. Software Alliance et al., *supra* note 95, at 11.

[128] *Government Contracting,* U.S. Chamber of Commerce, http://www.uschamber.com/issues/govtcontracting, (last visited Apr. 25, 2012).

Each procurement contract presents an opportunity to increase cybersecurity compliance by requiring that contractor and subcontractor security measures align with industry standards. The government should use these opportunities to incentivize a culture of security by prioritizing security standards in procurement processes and incentivizing proactive security measures and the purchase of cyberinsurance.[129]

Unfortunately, increased bidding requirements will make the procurement process more costly for contractors and the government. Contractors will have to pay more to adopt security measures and implement best practices. Further, the lack of transparency into the effectiveness of those measures will make it difficult for government to ensure compliance. For example, one company could easily spend far less on security measures than another who pays more money to provide the best security available. Efforts by government to test and verify security measures will increase the cost of the procurement process further. However, the benefit of additional security makes the procurement process low hanging fruit in critical infrastructure cybersecurity. In those sectors of critical infrastructure not already incentivized to adopt sufficient security measures, these and other economic incentives can help increase the baseline level of cybersecurity protection in the United States.

V. Strategies for Improved Governmental Oversight of Cybersecurity Measures

In addition to economic incentives, summit participants discussed the proper regulatory structure. Although they did not agree that government action is necessary, many participants argued that a single coordinating entity leading the cybersecurity effort could help resolve many current regulatory issues. As it exists today, for example, regulation and oversight is fractured and imposes requirements that are confusing and inconsistent.[130] This section will explain why a politically centralized national cybersecurity effort administered in a decentralized manner (i.e., regulatory authority is coordinated by a centralized federal entity which delegates to local and regional offices or entities with the power to carry out final execution) can help overcome improper incentives and the jurisdictional turf wars caused by a fragmented regulatory environment. Although consensus did not exist at the summit, evidence suggests that the Department of Homeland Security may be the best-equipped entity to lead that effort at this time.

A. Current Regulatory Environment

The interconnected nature of critical infrastructure required national direction through a comprehensive national policy setting forth goals and means to achieve them. Today's regulatory environment, consisting of state and federal oversight, addresses sector-specific security issues in an inconsistent, underinclusive, confusing, and reactive manner.[131] Various governing federal and state agencies and regulatory bodies constitute what the Center for Strategic and International Studies (CSIS) called a "fleet of well-meaning bumper cars[.]"[132] Additionally, "a variety of different laws,

---

[129] Larry Clinton, *Cyber-Insurance Metrics and Impact on Cyber-Security*, Ins. Sec. Alliance, http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf.

[130] Critical Infrastructure Protection, *supra* note 17, at 23-31.

[131] John Grant, *Will There be Cybersecurity Legislation?*, 4 J. Nat'l Sec. L. & Pol'y 103, 107 (2010).

[132] Commission on Cybersecurity for the 44th Presidency, Securing Cyberspace for the 44th Presidency, Ctr. for Strategic and Int'l Studies, 1, 36 (2008) [hereinafter Securing Cyberspace for the 44th Presidency].

administered by different agencies—or sometimes by no agency at all—setting forth divergent requirements governing the treatment of information by type and business sector"[133] is largely ineffective.

To take just three examples of fragmented regulation: the Health Insurance Portability and Accountability Act of 1996 (HIPAA) governs the security and privacy of health care records[134]; the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 protects personal financial information[135]; and the Federal Energy Regulatory Commission, pursuant to its statutory authority, sets and enforces regulatory standards in the energy industry, albeit only for interstate services. In addition to regulations like these that address only portions of the overall critical infrastructure framework, cooperation among industry players is challenged by the failure to coalesce around the development, diffusion, and assurance of best practices.[136] When standards and best practices are not adopted across critical infrastructure sectors, significant vulnerabilities remain.

Varying and inconsistent definitions of the cyberthreat across industries creates a separate problem.[137] If entities do not know how "electronic attacks" differ from "virus encounters," "virus disasters," "data intrusions," and "security incidents," coordination attempts will be of little or no benefit.[138] As an example, an audit of critical infrastructure managers in the electric utility industry in 2009 produced evidence that no common understanding of "critical" exists. In that audit, 73% of the industry claimed to have no critical infrastructure, which meant many entities were not taking sufficient protective measures.[139] "Standardization of vulnerabilities, types of attack, and techniques used in attacks can permit cross-project analysis that suggests best practices involving the most cost-effective technologies, policies, procedures, and organizational structures."[140] As a result, standards and best practices will be more effective.

"[The] effective management of cybersecurity risks requires alignment and integration of homeland and economic security, national security and intelligence, national defense, law enforcement, trade, and diplomatic functions."[141] Although independent industry cooperation and self-regulation improves the odds of critical infrastructure security, the discussion on market incentives explains

---

133 Bamberger & Mulligan, *supra* note 105, at 257.

134 Tim Wafa, *How the Lack of Prescriptive Technical Granularity in HIPAA Has Compromised Patient Privacy*, 30 N. Ill. U. L. Rev. 531, 541-42 (2010) (HIPAA is largely considered ineffective due to voluntary regulations and flexible standards (including implement standards that "meet [provider] needs" "whenever deem[ed] appropriate,") that leave the law devoid of "teeth" and vulnerable to abuse.).

135 *Codified at* 15 U.S.C. §§ 6801, 6809, 6821, and 6827.

136 A recent Government Accountability Office report details federal and sector-specific agency guidance and oversight for standard-setting and enforcement. *See generally*, Critical Infrastructure Protection, *supra* note 17.

137 Cybersecurity Economic Issues, RAND 2 (2008).

138 *Id.*

139 Joel Brenner, America the Vulnerable 100-01 (2011). The definition of critical infrastructure is an issue. Having previously been defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters," this definition may not be applicable to future cybersecurity legislation. 42 USC § 5195C(e) (2001),

140 Cybersecurity Economic Issues, *supra* note 137, at 2.

141 Mission Critical: A Public Strategy for Effective Cybersecurity, Bus. Roundtable 6 (2011).

why private firms have been thus far unable to overcome the challenges to effective cooperation. And, they will continue to fail without "some mechanism for constraining economic self-interest."[142] Coordinated government oversight can play a role in diminishing self-interested incentives. As one commentator put it, "Independent efforts will not be sufficient to address this challenge without a central coordination mechanism, an updated national strategy, an action plan developed and coordinated across the Executive Branch, and the support of Congress."[143] The government's ability to incentivize private action in a way that leverages the deep expertise held in agencies like the DHS (including the United States Computer Emergency Readiness Team (US-CERT)), the Department of Defense (DOD), the National Institute for Standards and Technology (NIST), the Federal Energy Regulatory Commission (FERC), and many others puts it in the position to correct the current market failure. With an overarching policy that clarifies regulatory roles and supports and facilitates public and private sector coordination and self-regulation, critical infrastructure will become increasingly secure.[144]

B. Jurisdictional Complexity and Turf Wars

Identifying a single government office or agency to lead the effort would create clarity and avoid jurisdictional delay and turf wars both among agencies and with the public.[145] One obvious possibility to take this role is the Department of Homeland Security. "DHS oversees critical infrastructure protection, operates the United States Computer Emergency Readiness Team (US-CERT), oversees implementation of the Trusted Internet Connection initiative, and takes other actions to help secure both the Federal civilian government systems and the private sector [systems]."[146] The agency also started the National Cybersecurity and Communications Integration Center (NCCIC), a watch and warning center that combined the U.S. Computer Emergency Readiness Team and the National Coordinating Center for Telecommunications, and integrated the National Cybersecurity Center (NCSC).[147] This expertise gives the DHS a distinct advantage over alternative agencies.

The DOD plays a separate, yet limited, role in critical infrastructure protection as both a Federal department and as a Sector-Specific Agency in the Defense Industrial Base.[148] It has authority over some foreign networks not under the purview of the CIA, but has no ability to act on domestic

---

142 Rubinstein, *supra* note 98, at 368.

143 Cyberspace Policy Review, White House 7 (2010).

144 *See generally* Mulligan & Schneider, *supra* note 14.

145 Kevin P. Newmeyer, *Who Should Lead U.S. Cybersecurity Efforts*? 3 Prism 115, 122 (2011).

146 Memorandum from Peter Orszag, Director, Office of Management and Budget, & Howard Schmidt, Special Assistant to the President and Cybersecurity Coordinator, to the heads of executive departments and agencies (July 6, 2010) *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf [hereinafter Orszag & Schmidt memorandum]; Kate Brannen, *Jurisdiction Issues Complicate Defense Cybersecurity Role*, FederalTimes, Feb. 11, 2011, http://www.federaltimes.com/article/20110211/AGENCY02/102110303/ ("'There is no clear delineation of responsibilities between the government, the military and the private sector,'" said Gerry Cauley, president and CEO of the North American Electrical Reliability Corp. (NERC).).

147 Commission on Cybersecurity for the 44th Presidency, Cybersecuirty Two Years Later, Ctr. for Strategic & Int'l Studies 6 (2011).

148 *DoD's Roles and Responsibilities*, The Office of the Under Secretary of Defense for Policy http://policy.defense.gov/hdasa/dcip/roles.aspx (last visited Apr. 25, 2012).

networks that are not its own systems.[149] However, DOD networks intermingle and rely heavily on civilian-provided networks, lines of communications, hardware and software, as well as support and maintenance of government computer systems.[150] Separating military and civilian networks, therefore, is nearly impossible,[151] giving the DOD some authority in the case of a national security threat. Although the DHS and DOD attempt to support each other to protect national cybersecurity, as evidenced by the DOD-DHS Memorandum of Agreement of October 2010,[152] many jurisdictional issues remain.[153]

To make matters more confusing, various other bodies from different arms of the government retain some element of jurisdictional oversight, including the Federal Trade Commission (an independent agency) under Section 5 of the FTC Act, the Federal Energy Regulatory Commission (an independent agency), the Federal Communications Commission (an independent agency), the Securities and Exchange Commission (an independent agency), the National Security Agency (an Executive Branch agency), the Federal Bureau of Investigation (an Executive Branch agency), National Institute for Standards and Technology (of the Department of Commerce in the Executive Branch), the Department of State (an Executive Branch department with foreign policy oversight over international communication and information policy), and many more.[154] "Which government agency responds to a cyber attack depends on where the attack originated, and this is an incredibly difficult thing to decipher in the cyber world" where it may take months to determine the culprit and even longer to determine his or her location.[155]

Placing comprehensive authority in a single governing entity could begin resolving regulatory confusion and turf wars to eliminate confusion, inconsistency, and delay.[156] Although a single governing agency may not completely resolve these issues, allowing the fragmented status quo to continue will allow gaping vulnerabilities in critical infrastructure security to remain.

---

[149] Ellen Nakashima, *Cyber-Intruder Sparks Massive Federal Response—and Debate Over Dealing with Threats*, WASH. POST, Dec. 8, 2011, http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story_3.html.

[150] Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1535 (2010).

[151] *Id.*

[152] Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity (Oct. 13, 2010), *available at* http://info.publicintelligence.net/DOD-DHS-MoA.pdf.

[153] Nakashima, *supra* note 149.

[154] Renay San Miguel, *Political Turf Wars Drive Out US Cybersecurity Chief*, TECHNEWSWORLD, Mar. 9, 2009, http://www.technewsworld.com/story/Political-Turf-Wars-Drive-Out-US-Cybersecurity-Chief-66431.html (Rod Beckstrom, former director of the National Cybersecurity Center at DHS, cited agency turf wars with the NHS when he left the position in 2009.).

[155] Brannen, *supra* note 146; It is not always possible to determine the culprit, even after significant effort. Tracing an attack to an IP address or a computer does not mean officials will ever determine who sat behind that computer. Jensen, *supra* note 150, at 1538.

[156] Even with clear Congressional jurisdiction and authority vested in a single agency, separation of powers issues remain wherein the President and the Executive Office may act in accordance with inherent Constitutional authority (i.e. War Powers Act). JOHN ROLLINS & ANNA HENNING, COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY IMPLICATIONS, CONGRESSIONAL RESEARCH SERVICES 9 (2009).

C. Governing Entity

To manage a national cybersecurity policy effectively, a single government office or agency leading the effort can help create clarity and minimize the many jurisdictional obstructions. The proper entity must have the authority to create and implement national policies through public and private critical infrastructure oversight.[157] This authority necessitates a broad cross-industry understanding of the cyberenvironment. It also requires a level of operational expertise to effectively partner with public and private critical infrastructure managers and stakeholders to implement ground-level strategy and oversee the standard-setting process. Proposed legislation suggests authority in many agencies, including the Department of Defense, the Executive Office of the President, various industry-specific agencies, and the Department of Homeland Security. At the summit discussion, Weiser teed up the issues surrounding these various regulatory options. The following section analyzes the viability of each, taking into account arguments made by participants at the summit. Although no participant considered the DHS an ideal solution, a majority agreed that the DHS's existing regulatory authority, institutional knowledge, and cybersecurity expertise puts it in the best position to manage this effort.

It is worth separately noting that despite the entity or entities given leadership in the cybersecurity effort, all summit participants agreed that no leader(s) will be effective without both authority and resources. Hendricks expressed skepticism that Congress will accomplish the goal of providing both the authority and the necessary resources in the current fiscal climate unless legislators are realistic about the needs of such a large national undertaking. If Congress fails to do this, any entity will be toothless and unsuccessful.

1. Department of Defense

Although well-situated to lead a military response, the Department of Defense (DOD) is likely not the proper entity to lead civilian cybersecurity efforts. Some commentators argue for strong DOD leadership because of its central role defending national security,[158] but few summit participants believed that the DOD is in the best position to lead the cybersecurity defense effort.

The DOD's mission is to provide the military forces needed to deter war and to protect the security of our country.[159] As a federal agency, the DOD is mandated to work with other federal agencies to "prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit" critical infrastructure and key resources.[160] As a sector-specific agency in the Defense Industrial Base, the DOD must work with all relevant agencies (both state and federal) to protect critical infrastructure, evaluate the vulnerability of the sector, encourage risk-management strategies,

[157] Grant, *supra* note 131, at 115 (explaining the need for a large agency with significant authority over every element of national cybersecurity, as well as the cost of creation and the political resistance to doing so.).

[158] *See* Jensen, *supra* note 150.

[159] *The Executive Branch,* The White House, http://www.whitehouse.gov/our-government/executive-branch (last visited Apr. 25, 2012).

[160] *Homeland Security Presidential Directive 7: Critical Infrastructure, Identification, Prioritization, and Protection*, Homeland Sec., http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1 (last visited Apr. 25, 2012) [hereinafter *Homeland Security Presidential Directive 7*].

and support sector-coordinating efforts that identify and mitigate threats to critical infrastructure.[161] Although it does not have oversight of civilian systems that are not its own, it relies so heavily on civilian infrastructure that it could have authority over these systems in the event of an attack.[162] The unavailability of critical infrastructure "could critically hinder the DOD's ability to project, support, and sustain forces and operations worldwide."[163]

Not only does the DOD rely on private sector infrastructure, but it coordinates closely with industry to erect and implement safe and secure systems. For example, it is involved in strategic decisions to determine where telecommunications systems will be erected.[164] It therefore has a deep understanding of industry cyberenvironments, giving it the insight which might allow it to help develop standards and best practices. Most importantly, if a cyberwar begins, it is the DOD that the President and civilians will turn to for aid.[165] At the summit, one participant stated that the DOD's military role may make it the most appropriate leader because it has a very good understanding of execution in times of action. Its leaders understand that failure can mean death. The other alternatives do not have the same sense of urgency, he said.

Although experienced in execution during trying times, the DOD does not have the experience or ability to effectively lead the domestic effort, and its history of secrecy will prevent legislators from considering it the cybersecurity leader. As an example, U.S. Cyber Command formed in 2009 to coordinate military and counter-terrorism efforts to protect defense networks and infrastructure.[166] However, the effort still lacks cross-sectorial authority, leaving the DOD weak in the face of a cyberattack. "The mission of U.S. Cyber Command is to defend the military networks," Gen. Keith Alexander, NSA director and head of cyber command, said in an April [2010] speech in Rhode Island. "I do not have the authority to look at what's going on in other government sectors, nor what would happen in critical infrastructure."[167] This important and fundamental aspect of national cyberstrategy belongs to the DHS.[168]

In addition to a lack of full access to domestic critical infrastructure, there is concern that the DOD is too clandestine to effectively communicate with private critical infrastructure managers. Secrecy is engrained in military operations, a trait that will limit the exchange of information with other agencies and the public sector.[169] Also, because many defense activities are classified, there is concern that cybersecurity information might be used for purposes unconnected to critical infrastructure

---

161 *DoD's Roles and Responsibilities*, *supra* note 148.

162 Jensen, *supra* note 150, at 1562-63.

163 Defense Infrastructure: Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure, U.S. Gov't Accountability Office 1 (2007).

164 Joint Communications System, Def. Technical Info. Ctr. xi (2010).

165 Jensen, *supra* note 150, at 1563.

166 *Id.* at 1560-61.

167 Nakashima, *supra note 149*.

168 *Id.*; Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. Nat'l Security L. & Pol'y 233, 243 (2010).

169 Information Sharing, Monitoring, and Countermeasures in the Cybersecurity Act, S. 2105, and the SECURE IT Act, S. 2151, Ctr. for Democracy & Tech. 4 (2012).

security.[170] For these reasons, legislators are unlikely to feel comfortable giving a primarily military entity focused on offensive measures the leading cybersecurity role.[171]

2. Executive Office of the President

Because no single agency has clear federal cybersecurity authority, and because of the power and influence on international affairs, some have argued that the Executive Office of the President should create a cybersecurity czar to manage that effort.[172] Summit participants did not discuss this alternative, but other commentators have proposed it as a viable alternative.

In 2009 the president created the position of Cybersecurity Coordinator. This position is an administrative and coordination position that reports to the national security adviser and the senior White House economic adviser. The Coordinator does not establish policies or standards and does not have direct access to the President.[173] If the power of the position were expanded, the individual could establish the national strategy, coordinate public and private activity, and set standards without the jurisdictional turf wars evidenced in other government agencies.[174] The individual would also have access to the international community, a key player in U.S. cybersecurity.

Both the Congressional Research Service and John Grant, former Minority Counsel for the Senate Committee on Homeland Security and Governmental Affairs, explain that it is unrealistic to believe that the Executive Office has the resources or ability to lead the cybersecurity efforts. Enforcing national strategy, coordinating all public-private partnerships, and establishing standards would require significant manpower and monetary support, neither of which the office currently possesses.[175] Although the Office could build its resources, doing so would require it to essentially create a new agency, thereby duplicate efforts currently directed toward the DHS.

There is also ambiguity around the ability of the White House to address and resolve security vulnerabilities in the public and private sector without specific Congressional authorization.[176] The "war powers" may allow the office to act in the face of cyberwarfare, but the "[many] facets of the [cybersecurity initiative] – such as components directing planning, development, and education – fall outside of traditional definitions of war[.]"[177] Furthermore, if given the Congressional authority to oversee operational coordination among agencies and sectors in response to a national cybersecurity threat, the "potential for requests for testimony and documents, and potentially subpoenas: matters that cause separation-of-powers battles between the branches[,]"[178] would significantly slow the

---

170 Kim Zetter, *DHS, Not NSA, Should Lead Cybersecurity, Pentagon Official Says*, Wired, Mar. 1, 2012, http://www.wired.com/threatlevel/2012/03/rsa-security-panel/.

171 Nakashima, *supra note 149*.

172 Securing Cyberspace for the 44th Presidency, *supra* note 132, at 1-2.

173 Cyberspace Policy Review, *supra* note 143, at 8-10.

174 Rollins & Henning, *supra* note 156, at 17.

175 Grant, *supra* note 131, at 108.

176 *Id.*

177 Rollins & Henning, *supra* note 156, at 10.

178 Coldebella & White, *supra* note 168, at 243.

Office's response and diminish its effectiveness.

3. Various Regulatory Bodies

The suggestion that "[entities] that currently regulate an element of critical infrastructure that has been defined as higher risk should be responsible for oversight"[179] seems promising. Yet because many do not have the resources or expertise to lead the effort, Weiser stated that industry regulators fit better in a supportive role.

Designated sector-specific agencies, as set forth in Homeland Security Presidential Directive 7 (HSPD-7) include the Department of Agriculture (agriculture, food), Health and Human Services (public health, healthcare, and food), Environmental Protection Agency (water, water treatment), Department of Energy (energy), Department of the Treasury (banking and finance), Department of the Interior (national monuments and icons), and Department of Defense (defense industrial base).[180] These and other agencies understand their sectors with a breadth and depth unsurpassable by another agency. They understand the implications for standards and best practices such that giving another agency the ability to regulate would open the door to unnecessary error and abuse.

Until now, however, few threats have required national coordination in the way that the cybersecurity threat does. Even the highway systems rely heavily on state and local governments to adopt and identify uniform standards and best practices.[181] The last global war cannot even compare to the level of preparedness necessary to address the cyberthreat because only recently have our critical systems been so interconnected.[182] If a power plant was attacked in World War II, the plant might have failed and harmed only the citizens relying upon on it for energy. Today, if the electricity grid is hacked, not only will electricity outages affect hundreds of thousands of Americans, but the hackers could also affect the telecommunications system, the water supply system, and much more.

As Weiser noted, sector agencies often lack the resources or incentives to understand cybersecurity on a national scale. This creates a siloed perspective and response, resulting in "turf wars" and gridlock. The Environmental Protection Agency (EPA), for example, could choose to prioritize water treatment over energy production, creating a possible conflict with the wishes of the Department of Energy. In such a case, EPA-generated standards might satisfy the needs of their constituents but do too little to protect other parties in other industries. Standards and best practices must not only meet minimum security requirements for the sector, but minimum requirements for the nation to protect the other interconnected critical infrastructure entities.

Weiser noted that many of these agencies either do not want the additional authority or are less sophisticated with security than the DHS. He suggested that perhaps the default authority

---

179 Recommendations of the Cybersecurity Task Force, U.S. House of Representatives 9 (2011).

180 *Homeland Security Presidential Directive 7*, *supra* note 160.

181 *Washington State County Road Standards*, Municipal Research and Servs. Ctr. of Wash., http://www.mrsc.org/subjects/transpo/stand/cordstand.aspx (evidencing the procedure by which Washington State adopts its road standards and best practices) (last visited Apr. 25, 2012).

182 Ian Ellefsen & Sebastiaan von Solms, *Critical Information Infrastructure Protection in the Developing World*, *in* Critical Infrastructure Protection IV 30-31 (Tyler Moore & Sujeet Shenoi eds., 2010).

could rest with a single entity, like the DHS, unless the sector specific agencies choose to take on the task. Building on the DHS oversight authority, each agency could maintain a complementary role in overseeing cybersecurity. It seemed clear among participants, however, that the various sector entities might take on authority despite an inability to effectively champion security measures, which would leave the entire infrastructure vulnerable. As a result, a strong DHS leadership may be the best solution.

4. The Department of Homeland Security

The 2002 law creating the Department of Homeland Security combined "computer security centers from the FBI, the Defense Department, the Commerce Department and the Energy Department."[183] In many ways the agency stands out as the entity best-prepared to manage the cybersecurity efforts. However, it is clear that without additional and clearly defined authority and resources to manage the public and private efforts, it will continue to fail.

The DHS's mission is to prevent and disrupt terrorist attacks; protect the American people, our critical infrastructure, and key resources; and respond to and recover from incidents that do occur.[184] Its knowledge of the cybersecurity environment spans many sectors, and it possesses the authority to coordinate and enforce the national cybersecurity strategy. The Secretary of the DHS can protect information shared by the private sector[185] and obtain critical information from other government agencies,[186] thereby diminishing concern for information security. (This ability to share information while protecting privacy and civil rights is critical to achieve effective public-private partnerships.) The Secretary may also lead a civilian response to a cyberattack[187] because she is the coordinating federal official for terrorist attacks, major disasters, and other emergencies.[188] Finally, the department may

[183] Declan McCullagh, *Homeland Security Flunks Cybersecurity Prep Test*, CNet.com, May 26, 2005, http://news.cnet.com/2100-7348_3-5722227.html?tag=mncol;txt.

[184] *The Executive Branch*, *supra* note 159; It is also responsible for overseeing the government-wide and agency-specific implementation of and reporting on cybersecurity policies and guidance; overseeing and assisting government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity; overseeing the agencies' compliance with FISMA and developing analyses for OMB to assist in the development of the FISMA annual report; overseeing the agencies' cybersecurity operations and incident response and providing appropriate assistance; and annually reviewing the agencies' cybersecurity programs. Orszag & Schmidt memorandum, *supra* note 146.

[185] *The Executive Branch*, *supra* note 159 (citing 6 U.S.C. §§131-133 (2006), which allow the Secretary to use Protected Critical Infrastructure Information (PCII) authorities.).

[186] *Id*. (citing 6 U.S.C. §§121-122 (2006)).

[187] *Id.* (citing Homeland Security Presidential Directive 5, Management of Domestic Incidents, Feb. 23, 2003, available at http://www.fas.org/irp/offdocs/nspd/hspd-5.html).

[188] "Pursuant to the Homeland Security Act of 2002, the Secretary is responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. The Secretary shall coordinate the Federal Government's resources utilized in response to or recovery from terrorist attacks, major disasters, or other emergencies if and when any one of the following four conditions applies: (1) a Federal department or agency acting under its own authority has requested the assistance of the Secretary; (2) the resources of State and local authorities are overwhelmed and Federal assistance has been requested by the appropriate State and local authorities; (3) more than one Federal department or agency has become substantially involved in responding to the incident; or (4) the Secretary has been directed to assume responsibility for managing the domestic incident by the President." Homeland Security Presidential Directive (HSPD) 5: Management of Domestic Incidents, 39 Weekly Comp. Pres. Doc. 280, 281 (2003).

develop standards for cybersecurity across the critical infrastructure sectors[189] and shield sellers and purchasers of technology designed to ward off cyber-terrorism from certain types of liability.[190] With this authority over many areas crucial to critical infrastructure protection, the DHS may be the best fit to help guide state and private entities in their efforts to protect critical infrastructure.[191]

Having developed these core competencies since 2003, the DHS possesses the institutional knowledge and ability in the field on a scale that no other single agency has or could acquire for years to come. Many, however, are skeptical of the DHS's ability to lead national cybersecurity in its current form. The Government Accountability Office released a report in 2009 stating that DHS failed to "fully satisfy its cybersecurity responsibilities designated by the 2003 National Strategy to Security Cyberspace."[192] In prior statements, Melissa Hathaway, former senior director for cyberspace at the National Security Council under President Obama,[193] commented that the DHS will have difficulty leading the federal cybersecurity effort because its role is not sufficiently defined. She stated, that "[we] appear to be asking DHS to take on new cybersecurity roles and missions while it is establishing its basic core competencies. Is this reasonable? Do we want DHS to become a first party regulator?"[194] She believes that DHS would have to adopt a "customer service" business model to deliver "timely and actionable cyber security threat, vulnerability, mitigation and warning information."[195]

At the summit, many participants also noted that the DHS today lacks clearly defined authority and Congress must act immediately to correct this shortcoming. Yet legislative clarity is necessary but not sufficient; simply giving DHS a vast degree of more responsibility in an area where it does not possess the clear authority to act or has limited institutional competence—without examining and improving its institutional capabilities—would be a mistake and likely lead to adverse consequences.

As Weiser noted, we are left with a "as compared to what?" problem. He explained that although the DHS is an imperfect agency to play a singularly important role in cybersecurity, it is better to work toward that goal than leave cybersecurity in dispersed pockets of disaggregated authority with little specific expertise. Summit participants did agree that if Congress is to give the DHS authority over cybersecurity, legislators must clearly define its jurisdiction, authority, and resources, or it will remain an empty vessel.

---

189 *The Executive Branch*, *supra* note 159 (citing 6 U.S.C. §321m (2007)). In addition to the 18 identified critical infrastructure industries, the "Department shall also evaluate the need for and coordinate the coverage of additional critical infrastructure and key resources categories over time[.]" Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, 39 Weekly Comp. Pres. Doc. 1816, 1818 (2003).

190 *The Executive Branch*, *supra* note 159 (citing Support Anti-terrorism by Fostering Effective Technologies Act of 2002, 6 U.S.C. §§441-444 (2006), which gives DHS authority over anti-terrorism technologies.).

191 Coldebella & White, *supra* note 168, at 235.

192 Eric Jensen, *Part I: Ten Questions: Responses to the Ten Questions*, 27 Wm. Mitchell L. Rev. 5049, 5059 (2011).

193 *Melissa Hathaway*, Belfer Center, http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html (last visited Apr. 25, 2012).

194 Ellen Cannon, *DHS's Role in Cyber Security Debated: Is It Up to The Job?*, Examiner.com, June 27, 2011, http://www.examiner.com/homeland-security-in-chicago/dhs-s-role-cyber-security-debated-is-it-up-to-the-job#ixzz1ekZcGHzQ.

195 *Id.*

VI. The Proper New Role for Coordinated Leadership: Supporting, not Supplanting, the Private Sector

Once it is established which entity or entities will lead the national cybersecurity effort, interaction with private sector critical infrastructure managers must be structured to effectively exchange information, set proper security standards, and enforce those standards consistently. Uncertainty exists as to whether that role should be supportive or directive. Regardless, if it is not structured correctly, "[a] centrally planned, one-size-fits-all regulatory scheme would almost certainly eliminate useful, industry-developed security measures and replace them with an ill-fitting, nondynamic slate of requirements."[196]

Literature on governance indicates that centralized decision-making raises significant issues when it comes to applying policies "on the front lines."[197] This is particularly true with regard to information overloads at the top-level (especially in complex situations like cybersecurity), remoteness from work performed, and lack of motivation and effort as autonomy is reduced.[198] To address these obstacles, it is imperative that the leading agency or agencies stay engaged with all sector entities, and that those entities have the power and authority to carry out national policies in a distributed manner. Policy and technological solutions that do not work within legacy networks and are not properly imposed at every level will be useless.[199] On the other hand, well-structured national principles and policy goals that incentivize effective public-private partnerships in various critical infrastructure sectors, facilitate information-sharing, and develop and enforce outcome-based standards and best practices for all system users and their supply chains stand a chance of increasing security. This section will describe how best to accomplish these goals within a centralized policy framework.

A. Public-Private Partnerships

Public-private partnerships are necessary to cybersecurity because the claim that government can micro-manage every aspect of cybersecurity and dictate best practice is hubris. Neither will it benefit society if private industry requires government assistance to effectively address every element of a secure infrastructure. Public-private partnerships act as a strong voice for industry players while also possessing access to the highest levels of government.[200] These partnerships benefit all parties by allowing government and industry to work together to accomplish mutual goals to facilitate government strategy development in light of private-sector needs, innovation, and resources.[201] After all, industry is the most knowledgeable about its business. It has the operational knowledge necessary to address day-to-day issues, market considerations, and innovative solutions.

Current federal law does emphasize the need for public-private partnerships in cybersecurity

---

196 Coldebella & White, *supra* note 168, at 241.

197 *See generally*, Steven Kelman, Central Government and Frontline Performance Improvement: the Case of "Targets" In the United Kingdom, Ash Inst., John F. Kennedy School of Gov't, Harvard Univ. 39 (2006).

198 *Id.*

199 Mulligan & Schneider, *supra* note 14, at 70.

200 *Economic Development Reference Guide*, Int'l Econ. Dev. Council, http://www.iedconline.org/?p=Guide_Partnerships (last visited Apr. 25, 2012); Cyber Storm III Final Report, Dept. Homeland Sec.16 (2011).

201 Cyberspace Policy Review, *supra* note 143, at 18-19.

through the Homeland Security Act of 2002 (which created DHS), the Homeland Security Presidential Directive 7 (HSPD-7), and the National Infrastructure Protection Plan (NIPP).[202] The Homeland Security Act makes DHS responsible for working with the private sector to develop and promote best practices, and HSPD-7 identifies certain sector-specific agencies to coordinate critical infrastructure protection.[203] NIPP uses a partnership model to coordinate security efforts with the private sector by forming government oversight councils and encouraging voluntary associations.[204] Despite these efforts, the public-private partnerships and relationships have not corrected the market failure that exists because they are under-empowered and frequently informal.

Designing effective public-private partnerships to leverage sector-specific insights, institutional knowledge, and private resources, while ensuring national overarching goals are not only properly established but efficiently enforced is no easy task.[205] At a meeting in Hong Kong in 2010, Melissa Hathaway noted that other countries like Brazil and Malaysia have more successful public-private partnership examples than the U.S.[206] Many domestic public-private partnerships "are not effective because the government is not focused in their efforts[,]" she explained.[207] By considering past examples and recent efforts to define effective public-private partnerships, current and future public-private partnerships can be improved.

The following suggestions for effective structure include recommendations from the Intelligence and National Security Alliance (INSA) analysis of public-private partnerships, as well as the findings of two high-profile partnerships in the U.S. cybersecurity industry (the Conficker Working Group[208] and the National Cybersecurity and Communications Integration Center).[209] Lessons learned from these entities provide numerous suggestions for successful partnerships in critical infrastructure cybersecurity with regard to partnership structure and information-sharing.[210]

---

[202] CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 17, at 5-6.

[203] *Id.*

[204] *Id.*

[205] *See* Rubinstein, *supra* note 98; *see e.g.,* Philip J. Weiser, *The Future of Internet Regulation*, 43 U.C. DAVIS L. REV. 529 (2009).

[206] *Melissa Hathaway: America Has Too Many Ineffective Private-Public Partnerships*, THE NEW NEW INTERNET, http://www.thenewnewinternet.com/2010/10/12/melissa-hathaway-america-has-too-many-ineffective-private-public-partnerships/ (last visited Apr. 25, 2012).

[207] *Id.*

[208] The Conficker Working Group, was formed to address the Conficker worm that targeted the Microsoft Windows operating system to create botnets. The group of private sector companies came together voluntarily and included AOL, Cisco, Facebook, ICANN, Microsoft, Georgia Institute of Technology, and many more. CONFICKER WORKING GROUP: LESSONS LEARNED (2010).

[209] The National Cybersecurity and Communications Integration Center (NCCIC) is a "center responsible for the production of a common operating picture for cyber and communications across the federal, state, and local government, intelligence and law enforcement communities and the private sector." To evaluate the resilience of the public-private partnership, NCCIC ran a series of tests, known as Cyber Storm. The final iteration, Cyber Storm III, was DHS's capstone national cybersecurity war game designed to evaluate how a public-private partnership would work in practice today. *About the National Cybersecurity and Communications Integration Center (NCCIC)*, DEPT. OF HOMELAND SEC., http://www.dhs.gov/xabout/structure/gc_1306334251555.shtm (last visited Apr. 25, 2012). ADDRESSING CYBER SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIP: AN ANALYSIS OF EXISTING MODELS, INSA (2009). Conficker and NCIC are two of the most relevant examples. More than 55 government initiated cybersecurity partnerships have been documented, 30 of which were started by DHS. THE CIP REPORT, CTR. FOR INFRASTRUCTURE PROTECTION & HOMELAND SEC.12 (2011)

[210] CYBER STORM III FINAL REPORT, *supra* note 200, at 15-16.

At the outset, it is clear that the roles, responsibilities, and authority of partnership members must be well-defined to avoid confusion and delay. The relationship between the partnership members must be based on maintained trust and balanced control. Such a balance can be achieved by requiring "a statutory foundation for the implementation of each partnership," making "the process as . . . open and reviewable as possible, from conception to completion[. . . Carefully negotiating] and formally [establishing] the terms and conditions of the partnership agreement"[211] is also important. Industry groups should take the lead on partnership tasks, and those groups should be both sufficiently interested in obtaining a proper outcome and sized and organized to represent the constituency without delaying response caused by too many members.[212] With this foundation in place, information sharing and standard setting will be effectively achieved and enforced.

B. Information Sharing

Information sharing and access to critical data between and among the public and private sectors is imperative to success. With an interconnected critical infrastructure, exchanging timely information on attacks and vulnerabilities can be used as an early warning incentivizing proactive defense measures. Information shared must clearly identify the type, value, timeliness, and implication of an attack, because without this context, information is ineffective.[213]

Efforts to exchange information between industries and government, and even within government agencies, raise acute privacy concerns.[214] Many in the public sector are concerned with giving government increased "ability to investigate, collect information in an unfettered manner about, and regulate or otherwise interfere with, private activities on the internet."[215] Paul Ohm, Associate Professor of Law at the University of Colorado, commented that even with statutory protections limiting what government can do with private information, we run the risk that such protections could be later stripped away. Edward Felten, a professor of Computer Science and Public Affairs at Princeton University, added that if government's role is merely the middleman in an information exchange, it probably does not need to be involved.

Yet the private sector benefits from government information, which allows it to improve product quality, as Hendricks noted, and response. But governments also hesitate to disclose law enforcement or intelligence information for fear of releasing sensitive details, "botching investigations[,] or compromising sources and methods."[216] When government does communicate information to its

---

[211] Stephen P. Mullin, *Public-Private Partnerships and State and Local Economic Development: Leveraging Private Investment*, U.S. Eco. Dev. Admin. 15 (2002).

[212] Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models, INSA 4 (2009).

[213] Cyber Storm III Final Report, *supra* note 200, at 16; Phil Williams, Casey Dunlevy, & Tim Shimeall, *Intelligence Analysis for Internet Security*, Software Engineering Inst., http://www.cert.org/archive/html/Analysis10a.html (last visited Apr. 25, 2012).

[214] When initially proposed the National Strategy for Trusted Identities in Cyberspace (or NSTIC), which would allow individuals to authenticate their online presence, met public skepticism due to perceived slippery slope of government control and bureaucratic slowdown. Michael Hickins, *Cyber-Security Czar Defends Government Role*, Wall. St. J. Blogs (Feb. 15, 2011, 12:01 PM), http://blogs.wsj.com/digits/2011/02/15/cyber-security-czar-defends-government-role/.

[215] Addressing Cyber Security Through Public-Private Partnership: An analysis of Existing Models, Intelligence and Nat'l Sec. Alliance 11 (2009) [hereinafter Addressing Cyber Security Through Public-Private Partnership]; Cybersecurity: Evaluating the Administration's Proposals, Ctr. for Democracy & Tech. 6 (2011).

[216] Coldebella & White, *supra* note 168, at 240.

constituencies, that information is often raw and sector specific, compounding digestibility issues.[217]

Although many information-sharing partnerships exist in critical infrastructure, few effectively overcome these issues. U.S.-CERT[218] and the National Cybersecurity and Communications Integration Center (NCCIC)[219] are heavily government centric and do not necessarily avoid privacy concerns. Many Industry-specific Information Sharing and Analysis Centers (ISACs)[220] have also fallen short due to antitrust, customer privacy, or trade secrecy concerns. As a result, many participants go to an ISAC hoping to receive rather than to provider information.[221] Rick Dakin, CEO, Co-Founder and Chief Security Strategist at Coalfire Systems, recommended one ISAC—the financial services ISAC (FC-ISAC)—as an example of information sharing that does work. He described how broad industry participation and rapid discussion of emerging threats greatly enhances industry response. Yet to improve effective communication, he noted, there must be greater participation and contributions from the intelligence community. To achieve similar success, industry actors should be incentivized to use ISACs to their full potential.

As an alternative solution to a public-private information-sharing partnership, legislators proposed an independent third-party clearing house that eliminates identifying information before exchanging it between government and industry.[222] This structure would be similar to the National Cyber-Forensics Training Alliance, a non-profit corporation which "functions as a conduit between private industry and law enforcement with a core mission to identify, mitigate and neutralize cyber crime."[223] The NCFTA works to organize the collection and sharing of information among subject matter experts in both the public and private sector, including CERT and the FBI, to address identified threats.[224]

Although a private third-party clearinghouse structured in this way can increase oversight and control of information exchanged with government or industry, this solution is not without its

---

217 Williams, Dunlevy, & Shimeall, *supra* note 213.

218 CERT, as part of the DHS National Cyber Security Division, "supports information sharing and collaboration on cybersecurity with the private sector operators of critical infrastructures and with state and local governments." Cybersecurity: Evaluating the Administration's Proposals, *supra* note 215, at 7 n.16.

219 NCCIC, also within the DHS, was designed to improve response to critical infrastructure attack. *About the National Cybersecurity and Communications Integration Center (NCCIC)*, *supra* note 209.

220 ISACs were created to provide a way for private industry actors to share information with one another and with government more freely than in the past. For example, the Communications ISAC brings together providers and hardware and software vendors to share information under the coordinating auspices of DHS's National Coordinating Center. It is a good example of what competing companies can do when they cooperate in emergency situations.
Fact Sheet: Communications Infrastructure Information Sharing and Analysis Center, U.S. Dept. of Homeland Security (2012).

221 ISACs were created in the past decade to provide a way for private industry actors to share information with one another and with government more freely than in the past have fallen short. For example, The Communications ISAC brings together providers and hardware and software vendors to share information under the coordinating auspices of DHS's National Coordinating Center.

222 *House GOP Task Force Issues Cybersecurity 'Blueprint'; Favors Private Sector Incentives*, Rep. Mac Thornberry, Oct. 16, 2011, http://www.thornberry.house.gov/News/DocumentSingle.aspx?DocumentID=268802.

223 Nat'l Cyber-Forensics & Training Alliance, http://www.ncfta.net/ (last visited Jan. 14, 2012).

224 *About Us*, Nat'l Cyber-Forensics & Training Alliance, http://www.ncfta.net/about-ncfta (last visited Jan. 14, 2012).

own problems.[225] Adding an additional element to information exchange process, for example, could make the flow sluggish. Industry coordination between competitors also raises antitrust issues,[226] but legislation can eliminate this concern by protecting good faith exchanges.[227] Consequently, a third-party clearinghouse would address many information exchange issues and should be considered by Congress and industry.

Although various options were discussed, summit participants did not agree on the appropriate structure of information-sharing exchanges. One participant stated that involving too many parties limits effectiveness. Smaller communities made up of industry players with common business problems can build trust and act in real time, sharing information without the worry of attribution or public exposure that comes with larger information-sharing regimes. Gronberg countered that with structure and a core entity facilitating the process, there is great benefit from cross-sectorial information exchanges. Many parties can benefit from broad knowledge, which provides all of the pieces to the puzzle. The alternative would mean those participating in smaller exchanges miss information not immediately attributed to their industry or sector. Although no final decision on structure was reached during the discussion, participants did agree that information-sharing promotes transparency, increases data availability, and is fundamental to cybersecurity efforts. Because direct communication with the DHS is largely ineffective, alternative solutions that provide complete, timely, and relevant information must be adopted.

C. Determining Standards and Best Practices

Industry adoption of appropriate consensus standards and best practices for managing security programs and implementing standards (i.e., vulnerability management, asset management, threat detection, code reviews, etc.) will give rise to increased levels of defense, better detection of attacks and vulnerabilities, and timely response to attacks. Long-term and self-sustaining security is a fundamental concern in setting cybersecurity standards. Although regulators and industry have made significant strides in setting standards and best practices, more can be done to better define performance goals, acceptable risk levels, and methods of achieving them.

The cyber "arms races"[228] between hackers and infrastructure managers due to rapid technological changes is a reality we must address. In a recent example, the Conficker working group combatted at least five versions of the Conficker malware. The malicious software used flaws in Microsoft Windows system to form a botnet using "the most advanced technology available. . . including code that had been devised in academia only months before."[229] When the working group's efforts became public, creators of the malware adapted Conficker C (the fourth version) specifically

[225] *See generally*, Mullin, *supra* note 211, at 12 (citing B. Guy Peters, *'With a Little Help From Our Friends': Public-Private Partnerships as Institutions and Instruments*, *in* Partnerships in Urban Governance: European and American Experience 11 (1998).)

[226] Eric Chabrow, *Law Interfering with Cybersecurity,* GovInfoSecurity, June 14, 2011, http://www.govinfosecurity.com/blogs.php?postID=986.

[227] *Id.*

[228] *Industry Concerned About DHS Standards on Cybersecurity*, Homeland Sec. Newswire, June 23, 2010, http://www.homelandsecuritynewswire.com/industry-concerned-about-dhs-standards-cybersecurity.

[229] John Markoff, *Defying Experts, Rogue Computer Code Still Lurks*, N.Y. Times, Aug. 27, 2009, at A1.

to remediation efforts by, among other things, allowed peer-to-peer connection for the first time to avoid using the Internet.[230] If the group did not constantly improve its efforts, it would have failed. Standards must reflect this need to constantly update defensive efforts and best practices, because if standards are low or insufficient at any level (the system, subnet, LAN, WAN, Internet, or PC), a false sense of security could result. If infrastructure managers believe meeting minimum standards will protect them, or if they are not compelled to continuously increase security, critical infrastructure will remain in jeopardy.

Outcome-based standards or self-determined standards have the best chance of surviving technology development because they are defined by results (performance goals or risk levels) instead of particular technologies.[231] Processes and professionals that implement standards and best practices are equally as important and must also be well-defined, as Gates suggested at the summit. In establishing these dynamic standards and best practices, regulators and the private sector may use a mix of approaches. These options include detailed prescriptive rules (regulators identify technology and specific circumstance for its use), a broad legal framework (outcome-based standards and best practices determined by government), legal reinforcement of industry-established standards (industry determines standards/best practices and government reinforces them),[232] and industry regulation (industry self-regulates through cooperative entity or the like).[233]

Today, all of these models are employed.[234] And although guidance for critical infrastructure entities exists from both regulators and industry,[235] it is often confusing, inconsistent, burdensome, and stagnant in light of ever-changing technology.[236] This is the case because sector-specific agencies "have not identified . . . key cybersecurity guidance applicable to or widely used in each of their respective critical infrastructure sectors."[237] As a result, so much information is available that infrastructure

---

230 Conficker Working Group: Lessons Learned, *supra* note 208, at 7.

231 *Performance and Risk-Based Standards*, Workforce Planning Assoc. Inc., http://www.wfpa.us/performancerisk-based-standards (last visited Apr. 25, 2012); John Linkous, *Avoiding the Cookie Cutter The Need for Outcomes-Based Cybersecurity Regulation*, AOL Government, Sept. 14, 2011, http://gov.aol.com/2011/09/14/avoiding-the-cookie-cutter-the-need-for-outcomes-based-cybersec/.

232 The North American Electric Reliability Corporation (NERC) is a good example of how a public-private partnership can effectively structure standard-setting. Originally a voluntary organization regulating electric power companies, NERC created delivery standards reflecting the expectations of its members. To allow for greater enforcement, FERC now federally sanctions the standards which are determined by constituent and user input to reflect behavior and conduct standards. Most importantly, the standards are legislatively reinforced. Addressing Cyber Security Through Public-Private Partnership, *supra* note 215, at 7.

233 Paul N. Otto, Note, *Reasonableness Meets Requirements: Regulating Security and Privacy in Software*, 59 Duke L.J. 309, 322-34 (2009).

234 *C*ritical Infrastructure Protection, *supra* note 17, at 11.

235 Entities like the American National Standards Institute (ANSI) support the development of industry standards and give credibility to the process by ensuring consensus, openness, due process, supporting data, and equal access. *Standards Activities Overview*, ANSI, http://www.ansi.org/standards_activities/overview/overview.aspx?menuid=3 (last visited Jan. 14, 2012). In cybersecurity, ANSI-HSSP "catalog[s], promote[s], accelerate[s] and coordinate[s] the timely development of consensus standards within the national and international voluntary standards systems intended to meet identified homeland security needs, and communicate[s] the existence of such standards appropriately to governmental units and the private sector." *ANSI Homeland Security Standards Panel*, ANSI, http://www.ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?menuid=3 (last visited Jan. 14, 2012).

236 *Id.*

237 *C*ritical Infrastructure Protection, *supra* note 17, at 34.

managers have difficulty determining what is most applicable and how to coordinate their efforts.[238]

One possible solution to uncertainty around standards and best practices is to let the various sectors determine and implement their own in accordance with national policies. Many legislative proposals have included language to this effect because legislators realize that it is nearly impossible for government to determine what works in real time.[239] The anticipated result, Gronberg stated, is that industry practice will turn into a standard of care that courts are willing to enforce. The tension with this solution is that some industries will allow their standards to remain low or underdeveloped, or perhaps no standard may coalesce. Therefore, government must adopt policies that incentivize highly evolved standards and best practices in accordance with national policies.

D. Enforcement

Enforcement of liability regimes, standards, and best practices, is a key element of the cybersecurity picture. Without it, critical infrastructure will remain vulnerable. Summit discussants considered the benefits of creating accountability regimes, as well as focusing on prevention and risk management. Once the structure of legal duties and economic incentives is in place, both the government and industry self-regulation can provide enforcement mechanisms. However, because government involvement is time-consuming and extremely costly for taxpayers, self-regulation should be encouraged.

Some have criticized proposed cybersecurity legislation as being "long on carrot and short on stick."[240] For example, in an initial draft of the President's proposal, DHS was given authority over cybersecurity but could not "issue a shutdown order, require use of a particular measure or impose fines, civil penalties, or monetary liabilities on the owner or operator of the covered critical infrastructure as a result of such review."[241] At the summit, Dakin reinforced the benefit of statutory enforcement measures by describing HIPAA. From his perspective, not until the Health Information Technology for Economic and Clinical Health Act (HITECH) defined civil liabilities and consequences for violations of HIPAA did action toward government goals progress.[242]

Yet many summit participants identified distinct barriers to enforcement in the cyber context, even if consequences are clearly defined: namely, attribution and compliance. Many times it is nearly impossible to determine the cause of the harm. For example, even if malware is traced to an IP address, it is often the case that the owner of the IP address did not cause the harm.[243] And, when

---

238 *Id.*

239 *See e.g.,* Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act, 112th Cong. 3-4 (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cybersecurity-regulatory-framework-for-covered-critical-infrastructure-act.pdf.

240 William Jackson, *White House's Cyber Plan is Weak on Enforcement*, Gov't Computer News, May 27, 2011, http://gcn.com/Articles/2011/05/30/Cybereye-Obama-cyber-plan-weak-on-enforcement.aspx?Page=1.

241 Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act, *supra* note 241, at 7.

242 *HIPPA Violations and Enforcement*, Am. Med. Assoc., http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page (last visited Apr. 25, 2012).

243 Kenneth Lieberthal & Peter W. Singer, *Cybersecurity and U.S.-China Relations*, Brookings, vii (2012).

harm is traceable, the party causing it may not be liable if the harm occurred despite compliance with standards and best practices. Summit participants identified both of these issues as particularly significant challenges in cybersecurity enforcement.

Shelanski suggested, and many summit participants agreed, that joint and several liability is a possible solution to the attribution problem. Under such a regime, a court can hold two or more entities liable if their acts individually contributed to the harm. The plaintiff may recover full damages from any one of the defendants. Then it is then up to the defendants who paid the damages to seek contribution from the others. Because cybersecurity civil claims are likely to be pursued through tort actions, joint and several liability is appropriate.

But joint and several liability will not solve every problem, especially in cases where compliance with standards and best practices at issue. Establishing compliance could determine whether a party is liable and to what degree. To avoid an impasse where proof of compliance is difficult to obtain, some have suggested third-party auditors evaluate and certify industry behavior. The credit card industry used third-party auditors to certify adherence to payment processes set by the industry.[244] Yet many critics believe third-party auditors will certify compliance whether or not it actually exists because they are paid by the entities they evaluate.[245] If so, third-party auditors will be ineffective. However, if industry regulators can eliminate conflicts of interest and ensure the adequacy of compliance audits, perhaps the solution is viable. To do so, regulators must have the resources to evaluate third-party audits, and that funding is hard to come by.[246]

Mulligan argued that prevention, mitigation, and recovery strategies were more aligned with the goal of improving cybersecurity. Focusing on punishment, compensation, and restitution, she said, leads to a "whack-a-mole" response that does nothing to promote investments to deliver real time, consistent security. Economic incentives can be used to encourage a pro-active cybersecurity culture by focusing on prevention, identification, containment, and risk mitigation. Participants discussed the implications of economic incentives to include (among other things) the creation of better systems, a focus on identification and resolution of risks by those closest to the problem, and the facilitation of strategies that reduce know vulnerabilities. Other potential solutions, not discussed at the summit, support evaluation of the quality and efficacy of products on the market and include certification (i.e., TRUSTe), ranking systems, pass/fail grading system, or numerical awards. Such tactics could be enforced by a mix of expert evaluations based on set standards, ratings (i.e., consumer reports), meters (i.e., Nielsen's, movies, books), and much more.[247] Consumer-driven activities (voting with your feet) can also help enforce sufficient security measures when consumers stop relying on or purchasing services from providers that are insecure. However, until consumers are made fully aware of the cybersecurity risk and such risks are transparent, consumer-driven mechanisms are unlikely to successfully enforce security standards and best practices in critical infrastructure.

---

[244] Kim Zetter, *McCain: Cybersecurity Ineffective Without NSA Monitoring the Net*, Wired, Feb. 16, 2012, http://www.wired.com/threatlevel/2012/02/cybersecurity-act-of-2012/.

[245] Kim Zetter, *In Legal First, Data-Breach Suit Targets Auditor*, Wired, June 2, 2009, http://www.wired.com/threatlevel/2009/06/auditor_sued/.

[246] *Id.*

[247] Karim Jamal & Shyam Sunder, *Regulation, Competition and Independence in a Certification Society: Financial Reports vs. Baseball Cards* 8-9 (2007), *available at* http://mba.yale.edu/faculty/pdf/sunders_baseballcards.pdf.

E. Technology Professionals and Continued Research and Development

Summit participants strongly agreed that technology professionals must be at the core of the cybersecurity discussion and that their role must be secured through legislation. "We need tens of thousands of educated security professionals," said Tim Brown, Professor of Electrical, Computer, and Energy Engineering and Director of the Interdisciplinary Telecommunications Program at the University of Colorado. As technology and security attack efforts constantly change, these professionals are best suited to understand that dynamic and help produce sufficient standards and best practices. Unfortunately, decision-makers do not always include technology professionals in the security discussion, Mulligan added. Technology professionals think differently, she said, and keep everyone else on their toes. Consensus existed on this point, as other summit participants agreed with her contentions.

To ensure a flourishing number of experienced and knowledgeable professionals are available, we must invest in educational programs that span all levels of training (elementary, secondary, higher education, certification programs).[248] Educational opportunities currently range from boot camps to higher education programs,[249] but credentials are not yet standardized. Campbell called these programs a step in the right direction, but Ohm identified a need for more structure around them. Without standardized program requirements, certifications do not guarantee a minimum level of training, knowledge, or ability. Ohm explained that he cannot tell much about a professional's ability from a Certified Information Systems Security Professional (CISSP) credential on a resume. Many participants agreed that increased federal government funding and support of these programs can help ensure the qualifications of security professionals in the field.[250] By building a strong and thorough cyber security curriculum, the United States will foster a knowledge base ready to meet security needs and create innovative solutions. "Knowledgeable developers are less likely to build systems that have vulnerabilities . . . and thus are more likely[] to embrace leading-edge preventions and mitigations."[251] Dan Jones, University of Colorado Office of Information Technology, explained that this means the critical infrastructure supply chain will eventually be more trusted and secure.

VII. Conclusion

As the cybersecurity summit came to a close, it was clear the group agreed that the threat to critical infrastructure is real and growing. Although some expressed exasperation at the complexity of the situation, evidencing frustration with the likelihood that vulnerabilities will remain despite extraordinary effort, many agreed that something can and must be

[248] National Cybersecurity Research and Development Challenges, *supra* note 32, at 5.

[249] William Jackson, *Cybersecurity Boot Camps are a Start Toward a Skilled Workforce*, Gov't Computer News, Aug. 9, 2010, http://gcn.com/articles/2010/08/09/cybereye-cybersecurity-boot-camps-address-the-growing-need-for-skilled-workforce.aspx.

[250] Other incentives to incorporating security training in curricula exist. John Dickson, *How Do We Get More Security Concepts Taught in Higher Education?*, Denim Group, May 16, 2011, http://blog.denimgroup.com/denim_group/2011/05/how-do-we-get-more-software-security-concepts-taught-in-higher-education.html (ideas proposed include hiring students and interns from professors who teach these concepts, suggesting relevant thesis topics, private security companies serve on boards and advisory panels, donate funding and other resources to institutions).

[251] Mulligan & Schneider*, supra* note 14, at 78.

done to address the issue. Increasing the security baseline and modifying current market incentives will likely impede many attempts to attack United States critical infrastructure. A national cybersecurity policy designed to eliminate reasonably avoidable risks based on best practices is one important way to align public and private goals. The DHS appears to be best suited to manage this effort, but no clear agreement existed among the participants on this point. Yet they all agreed that any entity or entities leading the cybersecurity effort must have both the authority and the resources to get the job done. Without proper backing, any entity with oversight will be toothless.

Accountability, prevention, and risk-management were all mentioned as ways to incentivize adoption of security measures. Although all agreed that it is often very difficult to determine the cause of a cyberattack, defined legal duties and liability regimes will allow for better accountability. With that in place, economic incentives will be more effective as market players come to understand the financial and legal implications of failing to act. Other economic incentives that could increase the baseline of security include limitations on liability, mandatory disclosure requirements, robust insurance markets, direct incentives, and government procurement.

To support public and private sector efforts encouraged by legal duties and economic incentives, enforcement mechanisms and public-private partnerships sustained through complete and timely information-sharing were discussed. Domestic public-private partnerships often fail, but we can learn from those failures to improve future interactions. Summit participants agreed that failure is also likely without sufficient information-sharing.

Finally, the participants agreed that information technology professionals are fundamental to long-term security. Without them, standards and best practices will be ineffective. To ensure availability and quality of these professionals, educational programs must be incentivized and developed through increased federal funding.

Cybersecurity Roundtable Participants

Meg	Ambrose	ATLAS Institute
Rajat	Bhargava	Still Secure
Kevin	Brown	University of Colorado- Student
Tim	Brown	University of Colorado
Dave	Campbell	Electric Alchemy
Rick	Dakin	CoalFire
Pierre	de Vries	Silicon Flatirons Senior Fellow
Edward	Felten	Princeton University
Melodi	Gates	Patton Boggs
Michael	Glenn	Century Link
Adam	Golodner	Cisco
Dick	Green	Silicon Flatirons Senior Fellow
Kevin	Gronberg	Senior Counsel, Committee on Homeland Security
Jason	Haislmaier	Byan Cave Holme, Roberts & Owens
Dale	Hatfield	Silicon Flatirons Senior Fellow
Brian	Hendricks	Nokia Siemens Networks
David	Huberman	Webroot
Dan	Jones	University of Colorado Office of Information Technology
Monisha	Merchant	U.S. Senator Michael Bennet
Deirdre	Mulligan	University of California Berkeley School of Information
Paul	Ohm	University of Colorado, Associated Professor
Preston	Padden	Silicon Flatirons Senior Fellow
Chris	Roberts	One World Labs
Howard	Shelanski	Georgetown University Law Center
Ari	Schwartz	United States Department of Commerce
Joe	Waz	Silicon Flatirons Senior Fellow
Phil	Weiser	University of Colorado