CYBERSECURITY IN CRITICAL INFRASTRUCTURE SECTORS: A PROACTIVE APPROACH TO ENSURE INEVITABLE LAWS AND REGULATIONS ARE EFFECTIVE

CHRIS LAUGHLIN*

INTRODUCTION 346
I. ADDITIONAL CYBERSECURITY LAWS AND REGULATIONS ARE BOTH NECESSARY AND INEVITABLE 352
A. Advanced Persistent Threats 352
B. Government Motivations as Related to APTs 354
C. Private Sector Motivations as Related to APTs 356
II. A FRAMEWORK FOR DEVELOPING NEW LAWS AND REGULATIONS 358
A. APT Protection by All Critical Infrastructure Companies 360
1. APTs are the new norm 360
2. Protecting against APTs protects against common threats 361
3. No exemption for small and mid-sized companies 361
4. Inaction or inadequate action now results in reactive laws and regulations later 362
B. Laws and Regulations Developed by Industry-Led Public-Private Partnerships 363
1. Private sector-led approach 364
2. Government contributions 366
C. Sector-Specific Laws and Regulations Under Expert Agencies 368
CONCLUSION 370

* J.D. Candidate, 2016, University of Colorado Law School and Lead Production Editor, Colorado Technology Law Journal. This note would not have been possible without the invaluable guidance and feedback from Blake Reid, Paul Ohm, Phil Weiser, and Admiral David Simpson. Thank you to my student note editor, Neal Vickery, and the entire CTLJ team for their support throughout the process. Special thanks to my friends and family for their encouragement and patience throughout the note writing process.

INTRODUCTION

Today, our government and the critical infrastructure sectors that provide essential services to Americans are constantly under attack.[1] These institutions face sophisticated cyberattacks from individual hackers, coordinated hacker organizations, terrorist groups, and enemy nation-states.[2] Over the "past decade, the frequency, scale, and intensity of attacks have continually increased."[3]

History shows that when the United States is attacked, our government responds with legislation that is designed to secure our assets, protect our people, and prevent such attacks from occurring again. This held true following World War II when, with the attack on Pearl Harbor still in recent memory, Congress passed the "National Security Act of 1947," which established nearly all of the institutions in the United States' national security bureaucracy.[4] Following the 1993 World Trade Center bombing and the Oklahoma City bombing, Congress passed the "Antiterrorism and Effective Death Penalty Act of 1996," which strengthened the government's ability to prosecute and punish terrorists and created other tools to help deter terrorist attacks.[5] Then, in 2001, following the September 11th attacks on the World Trade Center, Congress passed the "USA PATRIOT Act," which increased the government's surveillance and counterterrorism capabilities.[6]

Thus far, cybersecurity breaches in the United States have not resulted in death or severe damage to our national security or critical infrastructure,[7] but the threat is substantial and common consensus is that

1. Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1506 (2013).

2. AMIT AGRAWAL & JACK LAWSON, U.S. EXECUTIVE ORDER 13636 AND CRITICAL SECURITY CAPABILITIES TO CONSIDER 3 (Steve Grobman ed., 2014), http://www.intel.in/content/dam/www/public/us/en/documents/white-papers/critical-security-capabilities-paper.pdf; *Cybersecurity Threats Impacting the Nation: Hearing Before the Subcomm. on Oversight, Investigations, and Mgmt., Comm. on Homeland Sec.,* 112th Cong. 3 (2012) [hereinafter *Hearing*] (statement of Gregory C. Wilshusen, Director of Information Security Issues), http://www.gao.gov/assets/600/590367.pdf.

3. Shane Tews & James Cunningham, *The Road Ahead for Cybersecurity*, AM. ENTERPRISE INST.: TECHPOLICYDAILY.COM (June 16, 2014, 6:00 AM), http://www.techpolicydaily.com/technology/road-ahead-cybersecurity/.

4. DOUGLAS T. STUART, CREATING THE NATIONAL SECURITY STATE 1–4 (2008).

5. *Exploring HeinOnline: Antiterrorism and Effective Death Penalty Act of 1996*, HEINONLINE (Nov. 28, 2009), http://help.heinonline.org/2009/11/exploring-heinonline-antiterrorism-and-effective-death-penalty-act-of-1996.

6. ERIC ROSENBACH & AKI J. PERITZ, CONFRONTATION OR COLLABORATION? CONGRESS AND THE INTELLIGENCE COMMUNITY 92 (2009), http://belfercenter.ksg.harvard.edu/files/IC-book-finalasof12JUNE.pdf; *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 8, 15, 18, 22, 31, 42, 49, and 50 U.S.C.).

7. MILES KEOGH & CHRISTINA CODY, NAT'L ASS'N OF REGULATORY UTIL. COMM'RS,

a successful attack with severe results is on the horizon.[8] Most of the prominent attacks to date were designed to steal consumer data or disrupt activities of corporations in non-critical sectors.[9] Even the breach of the Office of Personnel Management ("OPM") system—where hackers stole personal information for over twenty-two million government employees and applicants—did not target critical infrastructure.[10] However, sophisticated hacker groups, terrorists, and enemy nation-states are not just interested in gaining or exposing sensitive information; they are also working toward disabling government operations and critical infrastructure and destroying our national and economic security.[11] There have been successful critical infrastructure attacks in other countries, such as the disablement and physical destruction of a German steel plant,[12] the

CYBERSECURITY FOR STATE REGULATORS 2.0 4 (2013), http://csrc.nist.gov/cyberframework/rfi_comments/040513_naruc.pdf; Steve Grobman, *Out of Aspen: State of Critical Infrastructure Cybersecurity, 2015*, INFORMATIONWEEK DARK READING (Jul. 22, 2015, 7:00 PM), http://www.darkreading.com/partner-perspectives/intel/out-of-aspen-state-of-critical-infrastructure-cybersecurity-2015/a/d-id/1321425.

8. *See, e.g.*, Michael Hayden, Curt Hébert & Susan Tierney, Opinion, *How to Protect Our Electric Grid*, USA TODAY (Mar. 4, 2014, 6:00 AM), http://usat.ly/1i2vJbb; MICHAEL HAYDEN, CURT HÉBERT & SUSAN TIERNEY, BIPARTISAN POLICY CTR., CYBERSECURITY AND THE NORTH AMERICAN ELECTRIC GRID: NEW POLICY APPROACHES TO ADDRESS AN EVOLVING THREAT 9 (2014), http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf.

9. In July 2015, hackers released personal information for nearly thirty-three million members of the website Ashley Madison. Dan Goodin, *Ashley Madison Hack Is Not Only Real, It's Worse Than We Thought*, ARS TECHNICA (Aug. 19, 2015, 12:22 AM), http://arstechnica.com/security/2015/08/ashley-madison-hack-is-not-only-real-its-worse-than-we-thought/. In December 2014, Sony was hacked to disrupt the upcoming release of their movie *The Interview*. The hackers released sensitive company information and disrupted other company operations. Michael Cieply & Brooks Barnes, *Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm*, N.Y. TIMES (Dec. 30, 2014), http://nyti.ms/1y4Z68J. In September 2014, Home Depot reported that fifty-six million credit card accounts were compromised in an attack. Shelly Banjo, *Home Depot Hackers Exposed 53 Million Email Addresses*, WALL ST. J. (Nov. 6, 2014, 8:03 PM), http://on.wsj.com/1sb3lXD. In December 2013, customer and credit card information for up to 110 million Target customers were hacked. Jia Lynn Yang & Amrita Jayakumar, *Target Says Up to 70 Million More Customers Were Hit by December Data Breach*, WASH. POST (Jan. 10, 2014), http://wpo.st/-W4K1. *See also* Roland L. Trope & Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks That Target and Degrade the Grid*, 40 WM. MITCHELL L. REV. 647, 671–72 (2014) (discussing the nature of attacks for most companies).

10. Cory Bennett, *OPM Hack Hit over 22 Million People*, THE HILL (July 9, 2015, 3:12 PM), http://thehill.com/policy/cybersecurity/247410-report-opm-hack-hit-over-25-million-people.

11. Danielle Warner, *From Bombs and Bullets to Botnets and Bytes: Cyber War and the Need for a Federal Cybersecurity Agency*, 85 S. CAL. L. REV. POSTSCRIPT 1, 11 (2012); *see also Hearing*, *supra* note 2, at 5. In March 2016, the Department of Justice indicted contractors for Iran's Islamic Revolutionary Guards Corps on charges "they carried out cyberattacks on dozens of American banks and tried to take over the controls of a small dam in a suburb of New York." David E. Sanger, *U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam*, N.Y. TIMES (Mar. 24, 2016), http://nyti.ms/1Rjmo2P.

12. TREND MICRO & ORG. OF AM. STATES, REPORT ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE IN THE AMERICAS 9 (2015), http://www.trendmicro.com/cloud-

destruction of an oil pipeline in Turkey,[13] the Stuxnet attack that destroyed Iran's nuclear centrifuges,[14] and a virus that erased critical files on over thirty thousand devices used by Saudi Arabia's state-owned oil company.[15] These real-world examples demonstrate what could be the most basic consequences of a successful critical infrastructure attack in the United States. American critical infrastructure is not immune from such an attack.[16] Hackers have successfully breached companies in American critical infrastructure sectors.[17] Cyber-perpetrators are on the offense and our defenses are falling behind.[18] A Pew study found that 61% of experts believed "a major [cyber]attack causing widespread harm would occur by 2025."[19] In a more recent survey, 48% of critical infrastructure executives "believe it is likely that a cyberattack on critical infrastructure, with the potential to result in the loss of human life, could happen within the next three years."[20]

"Critical infrastructure" is 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."[21] Presidential Policy Directive Twenty-one, "Critical Infrastructure Security and Resilience," identifies sixteen critical infrastructure sectors.[22] Each sector relies to varying

content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf.

13. Jordan Robertson & Michael Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*, BLOOMBERG BUS. (Dec. 10, 2014, 3:00 AM), http://bloom.bg/16MOY9e.

14. Michael B. Kelley, *The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought*, BUS. INSIDER (Nov. 20, 2013, 12:58 PM), http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11#ixzz3O5NLRK5Q.

15. MICHAEL E. BLEIER, TIMOTHY NAGLE & CHRISTOPHER J. FATHERLEY, REED SMITH, THE CURRENT STATE IN FINANCIAL SERVICES CYBERSECURITY 7 (2013). Another suspected attack was the nationwide Internet outage in North Korea that some attribute to U.S.-China efforts in response to the Sony hack. Nicole Perlroth & David E. Sanger, *North Korea Loses Its Link to the Internet*, N.Y. TIMES (Dec. 22, 2014), http://nyti.ms/1GPHDCg.

16. *See* KEOGH & CODY, *supra* note 7, at 4–5.

17. Siobhan Gorman, August Cole & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, WALL ST. J. (Apr. 21, 2009, 12:01 AM), http://www.wsj.com/articles/SB124027491029837401.

18. *See* DELOITTE & TOUCHE, TRANSFORMING CYBERSECURITY IN THE FINANCIAL SERVICES INDUSTRY 5 (2014), http://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA_Transforming_Cybersecurity_05122014.pdf.

19. PEW RESEARCH CTR., CYBER ATTACKS LIKELY TO INCREASE 6–7 (2014), http://www.pewinternet.org/files/2014/10/PI_FutureofCyberattacks_102914_pdf.pdf.

20. Press Release, Intel Corporation, New Survey Reveals Critical Infrastructure Cybersecurity Challenges (July 20, 2015), http://www.mcafee.com/us/about/news/2015/q3/20150720-01.aspx.

21. Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 12, 2013).

22. The sixteen critical infrastructure sectors are: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public

degrees on computers, networks, and automated systems.[23] Many of these sectors have secured their physical infrastructure, but several are lagging behind in developing security against fast-paced changes in cyber-warfare.[24] A successful cyberattack on a power plant, water treatment facility, or commercial airline system could have devastating impacts on our safety and our economy.[25]

In February 2013, after several failed attempts by Congress to pass cybersecurity legislation, President Obama issued Executive Order 13636, "Improving Critical Infrastructure," to address our unprotected and under protected critical resources.[26] The order included several provisions to improve the security and resiliency of critical infrastructure sectors, including a directive for the National Institute of Standards and Technology ("NIST") to develop a cybersecurity framework to reduce cyber risks to critical infrastructure.[27] "The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[28] In February 2014, NIST released the "Framework for Improving Critical Infrastructure Cybersecurity" ("NIST Framework").[29] It was designed to enable all critical infrastructure organizations "to apply the

health, information technology, nuclear, transportation systems, and water systems. Directive on Critical Infrastructure Security and Resilience, 2013 DAILY COMP. PRES. DOC. 92, 10–11 (Feb. 12, 2013).

23. AGRAWAL & LAWSON, *supra* note 2, at 8; *See also* DEP'T OF HOMELAND SEC., RECOMMENDED PRACTICE: DEVELOPING AN INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY INCIDENT RESPONSE CAPABILITY iii (2009), https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf (explaining that many critical infrastructure sectors, such as food and water, rely on Industrial Control Systems, which can be a target of cyberattacks).

24. *See* Press Release, Am. Pub. Power Ass'n et al., The Electric Power Industry Is United in Its Commitment to Protect Its Critical Infrastructure (Feb. 2014), http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Joint%20Trades%20Physical%20Security%20Backgrounder.pdf; DELOITTE & TOUCHE, *supra* note 18, at 5.

25. Susan Joseph, *A Cybersecurity Framework for the Nation's Critical Infrastructure*, CABLELABS, http://www.cablelabs.com/a-cybersecurity-framework-for-the-nations-critical-infrastructure-how-cablelabs-is-helping/ (last visited Mar. 8, 2016); Eric Engleman, *The Telecom Industry's Pushback Against Cybersecurity*, BLOOMBERG BUS. (Mar. 7, 2013), http://www.bloomberg.com/bw/articles/2013-03-07/the-telecom-industrys-pushback-against-cybersecurity; *see also* HAYDEN, HÉBERT & TIERNEY, CYBERSECURITY AND THE NORTH AMERICAN ELECTRIC GRID, *supra* note 8, at 9 (discussing the substantial secondary impacts of a power outage).

26. ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 2–3 (2013), https://www.fas.org/sgp/crs/natsec/R42114.pdf; Exec. Order No. 13636, *supra* note 21, at 11739.

27. Exec. Order No. 13636, *supra* note 21, at 11740–41.

28. *Id.*

29. NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

principles and best practices of risk management to improving the security and resilience of critical infrastructure."[30] The NIST Framework explicitly states that it was not meant to replace existing practices, but is rather meant to complement those practices and provide structure among all the existing standards and frameworks.[31] Use of the NIST Framework is voluntary[32] and it was designed for broad applicability, not to address specific cybersecurity risks in each critical infrastructure sector.[33]

Recent legislation, while potentially providing some benefits, has not directly targeted cybersecurity for critical infrastructure or addressed some of the more pressing cybersecurity challenges.[34] The Cybersecurity Enforcement Act of 2014 directed NIST to coordinate relevant federal agencies to work with other countries to create international cybersecurity standards.[35] The reports released by NIST in December 2015 laid the groundwork for that coordination.[36] Also in December 2015, Congress included the Cybersecurity Act of 2015 in the omnibus spending bill that was later signed by the President.[37] This act addressed one of the contentious issues by allowing companies to voluntarily share information about cyberthreats and defensive measures with the federal government while providing them with some protection from liability.[38] Moreover, in February 2016, President Obama signed an executive order creating the Commission on Enhancing National Cybersecurity, which is tasked with releasing a report in December 2016 with recommendations on actions that can be taken over the next decade to strengthen cybersecurity in the public

30. *Id.* at 1.

31. *Id.* at 13.

32. *Id.* at 2.

33. *See* Karen Epper Hoffman, *Following the Framework: Government Standards*, SC MAG. (June 2, 2014), http://www.scmagazine.com/following-the-framework-government-standards/article/346294.

34. Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y, 341, 377 (2015).

35. Jennifer Huergo, *Interagency Report Advocates Support for International Cybersecurity Standardization*, NIST TECH BEAT (Aug. 11, 2015), http://www.nist.gov/itl/201508_cyber_standards_working_group_report.cfm.

36. *See* INT'L CYBERSECURITY STANDARDIZATION WORKING GRP., NISTIR 8074 VOLUME 1: INTERAGENCY REPORT ON STRATEGIC U.S. GOVERNMENT ENGAGEMENT IN INTERNATIONAL STANDARDIZATION TO ACHIEVE U.S. OBJECTIVES FOR CYBERSECURITY, NIST (2015), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf; INT'L CYBERSECURITY STANDARDIZATION WORKING GRP., NISTIR 8074 VOLUME 2: SUPPLEMENTAL INFORMATION FOR THE INTERAGENCY REPORT ON STRATEGIC U.S. GOVERNMENT ENGAGEMENT IN INTERNATIONAL STANDARDIZATION TO ACHIEVE U.S. OBJECTIVES FOR CYBERSECURITY, NIST (2015), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf.

37. Peter Carey, Keith M. Gerver & Kenneth L. Wainstein, *President Obama Signs Cybersecurity Act of 2015 to Encourage Cybersecurity Information Sharing*, NAT'L L. REV. (Jan. 2, 2016), http://www.natlawreview.com/article/president-obama-signs-cybersecurity-act-2015-to-encourage-cybersecurity-information.

38. *Id.*

and private sectors, including critical infrastructure sectors.[39]

America's interest in protecting our critical infrastructure from national security threats is in tension with America's interest in allowing the private sector to provide many essential services in critical infrastructure sectors.[40] The private sector controls over 85% of cyber-relevant critical infrastructure in the United States.[41] While the private sector has incentives to protect these assets from cyberthreats, they may not align exactly with the interests of the government or the public. Since the release of the NIST Framework, there has been much discussion about whether a voluntary framework will help encourage, let alone ensure, that private companies adequately protect our critical infrastructure sectors.[42] Even the new legislation is receiving criticism as a relatively modest change that is inadequate to address threats against critical infrastructure in a changing cybersecurity landscape.[43] As such, the debate about whether there must be additional laws or regulations requiring companies to take certain actions continues.

That debate is moot. The current patchwork of cybersecurity laws and regulations is not sufficient to protect U.S. national security.[44] Additional cybersecurity laws and regulations are not just necessary, they are inevitable. Thus, private companies, Congress, and agencies should focus on developing them in a way that ensures a high level of protection and promulgating them before a major attack occurs. Section I will show why additional cybersecurity laws and regulations are necessary and inevitable by analyzing Advanced Persistent Threats and the government and private-sector motivations related to those threats. Section II will describe the framework that should be implemented to ensure that new laws and regulations are effective.

39. Press Release, White House, Executive Order: Commission on Enhancing National Cybersecurity (Feb. 9, 2016), https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity. The author hopes members of the commission will consider the recommendations made in Section II of this note during their analysis.

40. *See* DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 8 (2011), http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

41. Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 276 (2013).

42. JONES DAY, THE CYBERSECURITY DEBATE: VOLUNTARY VERSUS MANDATORY COOPERATION BETWEEN THE PRIVATE SECTOR AND THE FEDERAL GOVERNMENT 2, 5 (2013); *see also* Gautham Nagesh, *FCC Urges Industry-Led Approach on Cybersecurity*, WALL ST. J. (June 12, 2014, 1:37 PM), http://on.wsj.com/1irf8NU.

43. Carey, Gerver & Wainstein, *supra* note 37.

44. Mercedes K. Tunstall, *The Path to Comprehensive Cybersecurity Laws in the United States*, *in* UNDERSTANDING DEVELOPMENTS IN CYBERSPACE LAW 61, 62 (2015 ed.).

I. ADDITIONAL CYBERSECURITY LAWS AND REGULATIONS ARE BOTH NECESSARY AND INEVITABLE

An independent water treatment facility in Boulder, Colorado might not have reason to believe that North Korean cyber-soldiers will launch an attack on their facility. From their perspective, it may not be in their best financial interest to spend their limited resources to protect against such an unlikely attack. From the government's national security perspective, that is just the type of vulnerability such attackers may be seeking. It could have a substantial impact on the citizens and the economy in the area, as well as on government resources needed to recover from the attack.

The gap between government and private sector motivations makes additional legislation and regulations addressing private sector cybersecurity practices in critical infrastructure sectors both necessary and inevitable. There are three pieces that, together, establish this premise. First, Advanced Persistent Threats ("APTs") can result in successful and disruptive critical infrastructure cyberattacks. Second, the government has an interest in protecting against APTs. Third, private companies rely on a risk-based approach that does not focus on protecting against APTs. Because the private sector is not taking sufficient steps to protect against APTs, government intervention is necessary and inevitable.

A. Advanced Persistent Threats

Many existing frameworks, including the NIST Framework, focus on protecting against common cyber threats using basic, but highly effective, best practices.[45] "A traditional model of cyber defense might be designed to prevent hackers from penetrating the network and therefore to stop breaches from occurring."[46] Common cyber threats include phishing emails, malware, and Trojan horses.[47] These threats are usually executed using social engineering, where the hacker manipulates an individual's trust, behavior, or identity to gain access to information.[48] These types of attacks constitute at least 85% of all attacks, so it is no wonder that a risk-

45. Bob Withers, *Following Security Best Practices is Good but May Not Be Enough*, GLOBAL KNOWLEDGE (May 20, 2014), http://blog.globalknowledge.com/technology/security/following-security-best-practices-is-good-but-may-not-be-enough.

46. INTERNET SEC. ALL., THE ADVANCED PERSISTENT THREAT: PRACTICAL CONTROLS THAT SMALL AND MEDIUM-SIZED BUSINESS LEADERS SHOULD CONSIDER IMPLEMENTING 4 (2013), http://isalliance.org/publications/2013-06-06-ISA_APT_Paper-Practical_Controls_for_SMBs.pdf.

47. Roger A. Grimes, *The 5 Cyber Attacks You're Most Likely to Face*, INFOWORLD (Dec. 4, 2012), http://www.infoworld.com/article/2616316/security/the-5-cyber-attacks-you-re-most-likely-to-face.html.

48. AM. PUB. TRANSP. ASS'N, CYBERSECURITY CONSIDERATIONS FOR PUBLIC TRANSIT 4 (2013), http://www.apta.com/resources/standards/2014%20Q2%20Public%20Comment/RP_cyber_security_considerations_%20PUB_COMMENTS_V10%2012%2019%2013.pdf.

based approach would focus on protecting against them.[49] These types of cyberattacks generally have minimal impact on national security.[50] They are more likely to result in an individual's computer being used as a bot, identity theft, or data loss and any resulting financial loss or costs.[51] However, they can have a more significant impact when used as part of an APT attack.

Sophisticated cyberattackers generally use common cyberattack methods as one piece of a larger, coordinated cyberattack strategy.[52] An APT is a multi-step attack designed to infiltrate a system and remain there undetected for a long period of time to obtain high-value information.[53] Common cyberattack methods, such as phishing emails, are often the first step in the multistep process,[54] but under an APT attack, the perpetrator will focus on its target until it finds a way into the system.[55] Attacks are adapted in response to the level of success or failure with which they affect a target organization.[56] Once an unsuspecting user opens the attachment in a phishing email, for example, the network is exposed to APT infiltration.[57] When the attacker gains entry, he "establishes residence" in the system and creates a "backdoor" to allow remote command control.[58] This allows the attacker to operate in the system undetected.[59] The information obtained from these hacks can be used for immediate disruption or future harm.[60] It is these types of attacks that are causing major data breaches and being used for cyber-espionage to cripple critical

49. Teplinsky, *supra* note 41, at 313.

50. *See generally* Pierluigi Paganini, *2013 – The Impact of Cybercrime*, INFOSEC INSTITUTE (Nov. 1, 2013), http://resources.infosecinstitute.com/2013-impact-cybercrime/ (discussing the economic impact of the most common cyber-crime acts).

51. Bots are security-compromised computers that make up a network controlled by bot-net operators and are used to coordinate more sophisticated attacks and to distribute phishing schemes, spam, and malware attacks on other computers. *Hearing*, *supra* note 2, at ii, 3; *see also* Pierluigi Paganini, *supra* note 50.

52. INTERNET SEC. ALL., *supra* note 46, at 4.

53. *Advanced Persistent Threats: How They Work*, SYMANTEC, http://www.symantec.com/theme.jsp?themeid=apt-infographic-1 (last visited Mar. 9, 2016).

54. BLEIER, NAGLE & FATHERLEY, *supra* note 15, at 8.

55. *Advanced Persistent Threats*, *supra* note 53.

56. AM. PUB. TRANSP. ASS'N, *supra* note 48, at 4.

57. BLEIER, NAGLE & FATHERLEY, *supra* note 15, at 7.

58. *Id.* at 8. For example, suspected Chinese hackers built their own backdoor in the OPM system to effectuate a long-lasting breach. Evan Perez & Shimon Prokupecz, *U.S. Data Hack May be 4 Times Larger than the Government Originally Said*, CNN (last updated June 23, 2015, 10:59 PM), http://www.cnn.com/2015/06/22/politics/opm-hack-18-milliion/.

59. Perez & Prokupecz, *supra* note 58.

60. For example, "a cyberattack on an energy delivery system can have significant impacts on the availability of a system to perform critical functions as well as the integrity of the system and the confidentiality of sensitive information . . . . [that] could impact national security, public safety, and the economy." ENERGY SECTOR CONTROL SYS. WORKING GRP., CYBERSECURITY PROCUREMENT LANGUAGE FOR ENERGY DELIVERY SYSTEMS 1 (2014), http://energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf. *See also* Teplinsky, *supra* note 41, at 258–59.

infrastructure.[61]

B. Government Motivations as Related to APTs

The increased size and frequency of large breaches and the growing likelihood of a successful attack on our critical infrastructure underlie the government's motivations for safeguarding against APTs. Recent cyber breaches have been broad, encompassing millions of Americans, and prominent in the public discourse.[62] These well-known attacks have become part of the 2016 presidential campaign[63] and Congressional discourse.[64] From 2009 through 2014, over 110 bills and resolutions were introduced in Congress related to cybersecurity.[65] Each bill failed to pass because it did not strike the right balance between private and public interests, or the right balance between a cross-sector, high-level approach versus a comprehensive, sector-specific approach.[66] Even the legislation that passed in December 2014 and December 2015 is insufficient either because it does not directly address critical infrastructure cybersecurity or because it does so inadequately for the changing cybersecurity landscape.[67] As such, the narrative in favor of additional cybersecurity legislation continues.[68] A "cyber Pearl Harbor"[69] attack on our critical infrastructure will only speed up the process.[70] Congressional leaders and

61. *See* Teplinsky, *supra* note 41, at 257; Warner, *supra* note 11, at 11.

62. Teplinsky, *supra* note 41, at 271; *see also* Goodin, *supra* note 9; Cieply & Barnes, *supra* note 9.

63. *See generally* Joseph Cox, *Let's School the Presidential Hopefuls on Cybersecurity*, WIRED (Aug. 14, 2015, 7:00 AM), http://www.wired.com/2015/08/lets-school-presidential-hopefuls-cybersecurity/ (highlighting comments by presidential candidates regarding cybersecurity).

64. Eric Geller, *The Major Challenges Facing America's Ambitious New Cybersecurity Plan*, DAILY DOT (Dec 1, 2015, 9:08 AM), http://bit.ly/1lsmecD ("Cybersecurity has never been a more popular topic in Washington than it is right now.").

65. FISCHER, *supra* note 26, at 2.

66. *Id.*; JONES DAY, *supra* note 42, at 2; *see also* STEPHEN M. SPINA & J. DANIEL SKEES, MORGAN LEWIS, ELECTRIC UTILITIES AND THE CYBERSECURITY EXECUTIVE ORDER: ANTICIPATING THE NEXT YEAR 3–4 (2014), http://www.lexology.com/library/detail.aspx?g=11283a4a-7ebd-4f30-9e94-9e08da5c7f1c ("The Democratic legislative proposals, typified by the Cybersecurity Act of 2012, focused on a mandatory cybersecurity compliance regime overseen by the Department of Homeland Security . . . . The Republican legislative approach, typified by . . . [the SECURE IT Act], emphasized improved information sharing between the government and the private sector so that private industry could become aware of emerging threats far more quickly.").

67. *See* Huergo, *supra* note 35; Carey, Gerver & Wainstein, *supra* note 37.

68. Keith Wagstaff, *Hack to the Future: Experts Make 2016 Cybersecurity Predictions*, NBC NEWS (Jan. 2, 2016, 6:23 AM), http://nbcnews.to/1O0ZaJQ.

69. This phrase was coined by Deputy Defense Secretary John Hamre and used again by Defense Secretary Leon Panetta. Jon Oltsik, *Protecting Critical Infrastructure*, CIPHER BRIEF (Nov. 22, 2015), https://www.thecipherbrief.com/article/protecting-critical-infrastructure.

70. One Congressional representative was recently quoted as saying that "[i]n the event of a cyber Pearl Harbor, the public will demand that Congress regulate, and standards will be imposed and there'll be no getting around that." Kenneth Corbin, *A 'Cyber Pearl Harbor' Could*

the president would be forced to take action, just as they did with legislation following Pearl Harbor, the 1993 World Trade Center attack, and the attacks on September 11, 2001.[71]

This narrative is coupled with actions by government agencies and public comments by agency heads about the need for additional cybersecurity protections. The Obama administration argues that some sector-specific government agencies have the option to impose cybersecurity requirements on the entities under their purview.[72] Additionally, "under current law . . . many [federal agencies] have sector-specific cybersecurity responsibilities for critical infrastructure, such as the Department of Transportation for the transportation sector."[73] As one nuclear industry executive put it, "if an industry led effort is not deemed adequate by the industry regulatory body, then additional regulation is likely to ensue."[74]

The Securities and Exchange Commission ("SEC") is increasingly curious about the cybersecurity defenses of private companies under its purview. Former SEC Commissioner Luis Aguilar noted that "there is no doubt that the SEC must play a role in [cybersecurity]" and he advised companies that they should have response plans for cyberattacks in place.[75] In November 2014, the Commission passed new regulations for certain market participants that require comprehensive policies and procedures for information technology, appropriate corrective action when systems issues occur, notifications to the SEC when problems occur, and annual reviews of their automated systems.[76]

The Federal Communications Commission's ("FCC") Communications Security, Reliability and Interoperability Council ("CISRIC") released a report with implementation guidance for the NIST Framework and voluntary mechanisms to ensure that "communication

Mean New Security Mandates, CIO (Oct. 12, 2015, 5:51 AM), http://www.cio.com/article/2991484/cyber-attacks-espionage/a-cyber-pearl-harbor-could-mean-new-security-mandates.html.

71. *See* James Arden Barnett, Jr., *Cybersecurity: Fixing Policy with New Principles and Organization, in* RECENT TRENDS IN NATIONAL SECURITY LAW 25, 32–33 (2014).

72. Nagesh, *supra* note 42; *see also* Patricia Paoletta, *The Cybersecurity Overreach: A Few Harsh Words About the President's Cybersecurity Executive Order, Along with a Better Solution*, 14 ENGAGE: J. FEDERALIST SOC'Y PRAC. GROUPS 81, 84 (2013).

73. FISCHER, *supra* note 26, at 4.

74. PERRY PEDERSON, LANGNER GRP., A COST-EFFICIENT APPROACH TO HIGH CYBER SECURITY ASSURANCE IN NUCLEAR POWER PLANTS 3 (2014) (emphasis omitted), http://www.langner.com/en/wp-content/uploads/2014/04/High-Cyber-Security-Assurance-in-NPPs.pdf.

75. Ed Silverstein, *SEC Continues to Warn U.S. Businesses About Risk of Cyber Attacks*, INSIDE COUNSEL (Sept. 25, 2014), http://www.insidecounsel.com/2014/09/25/sec-continues-to-warn-us-businesses-about-risk-of.

76. Press Release, U.S. Sec. & Exch. Comm'n, SEC Adopts Rules to Improve Systems Compliance and Integrity (Nov. 19, 2014), https://www.sec.gov/News/PressRelease/Detail/PressRelease/1370543496356.

providers are taking the necessary measures to manage cybersecurity risks."[77] Still, FCC Chairman Tom Wheeler previously expressed that he is not against taking regulatory action if private company efforts are inadequate. While the Chairman urges companies to take the lead on securing networks because regulations could not be as responsive as best practices developed by private companies, he noted that voluntary efforts must be "more demonstrably effective than blindly trusting the market" to prevent regulations.[78]

The likelihood of agency action may increase following the release of a Government Accountability Office ("GAO") report that examined the oversight of critical infrastructure cybersecurity by sector-specific agencies.[79] The GAO concluded that twelve sectors do not have performance metrics to "measure and report on the effectiveness of all of their cyber risk mitigation activities or their sectors' cybersecurity posture."[80] The report further called out private sector companies on which the agencies rely to share the information necessary to measure their efforts.[81]

Finally, the Federal Trade Commission ("FTC"), while not a sector-specific agency, has also jumped into the fold to protect consumers' interests when companies fail to implement adequate cybersecurity.[82] A federal appeals court unanimously ruled that the agency could proceed with a suit against a hotel chain whose network was infiltrated by hackers three times in three years.[83] President Obama even suggested "broadening the FTC's authority to allow it to set cybersecurity standards that companies would be required to meet."[84]

C. Private Sector Motivations as Related to APTs

The private sector's ideal solution to cybersecurity for privately owned critical infrastructure is a risk-based approach augmented by public-private partnerships.[85] Private companies largely approve of the

77. COMMC'NS SEC., RELIABILITY & INTEROPERABILITY COUNCIL IV, WORKING GROUP 4, CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES (2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

78. Nagesh, *supra* note 42.

79. Cory Bennett, *Feds Lack Method to Grade Critical Infrastructure Cybersecurity*, THE HILL (Nov. 20, 2015, 4:36 PM), http://thehill.com/policy/cybersecurity/260963-feds-lack-method-to-grade-critical-infrastructure-cybersecurity.

80. *Id.*

81. *Id.*

82. Katie Bo Williams, *Appeals Court Rules FTC's Authority Extends to Cybersecurity*, THE HILL (Aug. 24, 2015, 1:32 PM), http://thehill.com/policy/cybersecurity/251803-appeals-court-ftcs-authority-extends-to-cybersecurity.

83. *Id.*

84. *Id.*

85. Letter from R. Bruce Josten, Exec. Vice President Gov. Affairs, U.S. Chamber of Commerce, to Harry Reid & Mitch McConnell, U.S. Senators 1–2 (Jan. 30, 2012),

NIST Framework because it is risk-based and was developed with extensive input from the private sector.[86] Some private entities even support "carefully crafted and narrowly tailored" legislation,[87] like the Cybersecurity Act of 2015.[88] However, the private sector is generally wary of additional cybersecurity laws or regulations that might mandate specific standards or technology.[89] The private sector puts forth four main arguments against regulations and broadly-scoped legislation. First, such requirements could increase business expenses and overhead as well as misallocate company resources.[90] Second, companies would be forced to focus on compliance with measures that quickly become out-of-date and ineffective, rather than on methods to address current and future threats.[91] Third, such requirements would disincentivize the public-private partnerships that are already addressing the challenges.[92] Fourth, the regulations would not necessarily improve cybersecurity,[93] particularly when the government does not have a great track record for protecting against cyber breaches.[94]

Inherent in the private sector's preferred risk-based approach is a cost-benefit analysis.[95] Under a risk-based cybersecurity approach, private companies determine the probability of cyberattacks occurring at various levels of magnitude and the costs and measures necessary to prevent each type of attack.[96] When the costs to protect the company from an attack outweigh the costs to recover from an attack, companies are typically willing to accept the risks rather than invest in protecting against them.[97] APTs are unlikely to occur and costly to prevent, constituting only 15% of all cyberattacks.[98] So it may not be in a company's best interest to spend

https://www.uschamber.com/sites/default/files/documents/files/120130_ComprehensiveCybersecurityLegislation_Reid_McConnell.pdf.

86. Joseph, *supra* note 25; Hoffman, *supra* note 33.

87. Letter from Josten, *supra* note 85, at 1.

88. Carey, Gerver & Wainstein, *supra* note 37.

89. JONES DAY, *supra* note 42, at 2.

90. Letter from Josten, *supra* note 85, at 1.

91. *See* Larry Clinton, *Federal Red Tape Increases Threat of Cyberattacks*, STARS & STRIPES (Apr. 25, 2012), http://www.stripes.com/federal-red-tape-increases-threat-of-cyberattacks-1.175540; *see also* HERITAGE FOUND., SOLUTIONS 2014 167 (2014), http://thf_media.s3.amazonaws.com/2014/pdf/Solutions-2014.pdf.

92. Letter from Josten, *supra* note 85, at 1.

93. *See id.*; HERITAGE FOUND., *supra* note 91, at 167.

94. Jody Westby, *The Government Shouldn't Be Lecturing Private Sector on Cybersecurity*, FORBES (June 15, 2015, 2:05 PM), http://www.forbes.com/sites/jodywestby/2015/06/15/the-government-shouldnt-be-lecturing-the-private-sector-on-cybersecurity/.

95. INTERNET SEC. ALL., *supra* note 46, at 5.

96. Teplinsky, *supra* note 41, at 311; *see also* INTERNET SEC. ALL., *supra* note 46, at 4 (discussing the economic incentive to deploy less secure systems).

97. *See* Teplinsky, *supra* note 41, at 311.

98. Sales, *supra* note 1, at 1517. Basic cyberthreats make up 85% of all threats and the remaining advanced threats make up the other 15%. *See* Teplinsky, *supra* note 41, at 313.

resources to protect against them.[99] In fact, some companies may just buy insurance to cover these unlikely threats.[100]

Private companies also lack incentive to invest in protecting against APTs because they do not internalize the negative and positive externalities of a successful cyberattack.[101] For example, if a cyberattacker disables a power generation facility, the operator may have to invest in new computer systems and infrastructure and it will lose some revenue from its customers.[102] However, the federal government will step in to assist with getting the systems operational and finding the perpetrator.[103] The people who would suffer the most are those without power.[104]

II. A FRAMEWORK FOR DEVELOPING NEW LAWS AND REGULATIONS

Since additional cybersecurity laws and regulations are both necessary and inevitable, it is necessary to create a regime that will ensure the highest level of protection from APTs before a successful attack occurs. The private sector and government should focus on APTs and work together to develop laws that create a framework for flexible regulations to protect each critical infrastructure sector.

The best laws and regulations will be developed in ways that address the concerns and interests of both the government and the private sector. To reiterate, the government has an interest in protecting against all cybersecurity threats to critical infrastructure.[105] It will not tolerate a market-based solution that does not attempt to address unlikely, but highly-impactful threats.[106] The private sector places high value on a non-statutory and non-regulatory risk-based approach.[107] Companies generally share a concern that a government solution would increase expenses, misallocate resources, focus on compliance, decrease public-private partnerships, and ultimately result in little to no actual cybersecurity benefits.[108]

99. INTERNET SEC. ALL., *supra* note 46, at 5. Critical infrastructure owners are challenged to develop compelling business cases for investing in control systems security. *Hearing*, *supra* note 2, at 8.

100. Matthew Cohen, *Comment: Cybersecurity Lessons from the Financial Sector*, INFOSECURITY (Jan. 9, 2014), http://www.infosecurity-magazine.com/opinions/comment-cybersecurity-lessons-from-the-financial; Teplinsky, *supra* note 40, at 316.

101. Sales, *supra* note 1, at 1507.

102. *Id.* at 1508.

103. *See id.* at 1507.

104. "A targeted cyber-attack . . . on the power system could lead to huge costs, with sustained outages over large portions of the electric grid and prolonged disruptions in communications, health care delivery and food and water supplies." Hayden, Hébert & Tierney, *How to Protect Our Electric Grid*, *supra* note 8.

105. *See supra* Section I.B.

106. *Id.*

107. *See supra* Section I.A.

108. *Id.*

National security laws or regulations should not be a license to direct all cybersecurity practices of private companies whose operations may touch the national security sphere. Private companies make a compelling argument against overregulation. While technological developments move quickly, it can take years for the government to create new laws and regulations.[109] The government should not be in the business of mandating cybersecurity practices that will be obsolete before the legislation reaches the president or the regulations make it through a notice and comment rulemaking.[110]

Cybersecurity laws should be designed to protect against APTs, while also addressing the private sector's interests and concerns. While the private sector may prefer no new laws or regulations, it is possible to develop a cybersecurity system that addresses unlikely, high-impact threats in an effective way that does not burden the private sector. Using these interests and concerns as the standard would help garner support and promote adoption of the new regime by private companies.[111] It would also align with the government's interest in private-sector economic growth. After all, it is not in the government's interest to take away from the economic vitality of private companies without actually increasing critical infrastructure protection from cyberthreats.

There are four parts that will ensure that the public and private sector interests are met when a new cybersecurity regime is developed. First, new laws and regulations should ensure critical infrastructure companies of all sizes protect against APTs. Second, thoughtfully developed laws and regulations created before a successful major attack will prevent reactive measures after a major attack. Third, the requirements should be developed through industry-led public-private partnerships. Fourth, the requirements should be under the authority of the government agency responsible for each critical infrastructure sector.

109. Clinton, *supra* note 91, HERITAGE FOUND., *supra* note 91, at 167; Robert Kenneth Palmer, *Critical Infrastructure: Legislative Factors for Preventing A "Cyber-Pearl Harbor*,*"* 18 VA. J.L. & TECH. 289, 341 (2014).

110. "The pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rule-making." Julian Hattem, *FCC Head Wants Businesses to Step up Online Security*, THE HILL (June 12, 2014, 11:59 AM) (internal quotation omitted), http://thehill.com/policy/technology/209161-fcc-head-wants-businesses-to-step-up-online-security.

111. MIKE MCCONNELL ET AL., BOOZ ALLEN HAMILTON, THE CYBERSECURITY EXECUTIVE ORDER: EXPLOITING EMERGING CYBER TECHNOLOGIES AND PRACTICES FOR COLLABORATIVE SUCCESS 8 (2013), http://www.boozallen.com/media/file/BA13-051CybersecurityEOVP.pdf.

A. APT Protection by All Critical Infrastructure Companies

While APTs constitute only 15% of cyberattacks, they pose a large threat to critical infrastructure security.[112] An effective defense against these threats is possible by "enabling security protocols that make sensitive or valuable data so hard to steal that the effort isn't worth the reward."[113] There are three reasons that cybersecurity laws and regulations should ensure critical infrastructure companies of all sizes protect against APTs. First, APTs are becoming the new norm for cyber threats. Second, focusing on APTs will ensure that companies are also protected from common cyberattacks. Third, cyberattackers will target small and mid-sized companies that have less protection, but that can still result in disruptive and destructive attacks.

1. APTs are the new norm

Compliance with best practices in cybersecurity frameworks may give companies a false sense of security.[114] Even if fully implemented, today's best practices lack the sophistication to protect against most full-scale APTs.[115] Meanwhile, APTs are becoming the new norm for cyber threats,[116] yet companies underestimate their risk.[117] With this mindset, there is no incentive for them to deploy more secure systems.[118] It is typically only after a company suffers a successful attack that they and other companies in the industry tend to harden their security.[119] Companies need to rethink their approach to cybersecurity "from walling off the system to detecting, monitoring and mitigating attacks on the system."[120] Creating laws and regulations that require companies to focus on APTs

112. *See* Teplinsky, *supra* note 41, at 234.

113. Jeffrey Carr, *Opinion: Retaliation Against China is the Wrong Reaction to OPM Hack*, CHRISTIAN SCI. MONITOR (Aug. 2, 2015), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0804/Opinion-Retaliation-against-China-is-the-wrong-reaction-to-OPM-hack.

114. Withers, *supra* note 45.

115. Basic cyber hygiene "is unlikely to eradicate the threat of cyber intrusion posed by nation-states and other sophisticated actors." Melanie J. Teplinsky, *Cybersecurity and the Cyberthreat Deterrence Trend*, *in* RECENT TRENDS IN NATIONAL SECURITY LAW 85, 89 (2015 ed.)

116. INTERNET SEC. ALL., *supra* note 46, at 3.

117. PRICEWATERHOUSECOOPERS, KEY FINDINGS FROM THE 2013 US STATE OF CYBERCRIME SURVEY 15 (2013), http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/us-state-of-cybercrime.pdf. *See also* Dan O'Shea, *A Critical Time for Critical Infrastructure*, LIGHTREADING (Aug. 13, 2015), http://www.lightreading.com/ethernet-ip/critical-infrastructure/a-critical-time-for-critical-infrastructure/a/d-id/717504 (noting that a recent report "suggests that operators of critical infrastructure might be over-confident in their ability to defend against attacks and misunderstand the scale of the current threat environment.").

118. INTERNET SEC. ALL., *supra* note 46, at 5.

119. Withers, *supra* note 45.

120. INTERNET SEC. ALL., *supra* note 46, at 6.

will address the lack of incentive, creating stronger protection on the front end, before critical infrastructure attacks occur.

2. Protecting against APTs protects against common threats

Focusing companies on protecting against APTs does not mean that threat protection against common cyberattack methods will go by the wayside. As previously noted, APTs currently make up a small portion of cyberthreats. Common threats make up the larger portion and can be mitigated by basic cybersecurity efforts.[121] However, companies that protect against APTs will inherently protect against common cyberthreats that are often one step in the APT attack method.[122] It is easier to be prepared for less drastic attacks when prepared for the worst-case scenario.[123]

3. No exemption for small and mid-sized companies

Measures to protect against APTs will be insufficient if they do not apply to small and mid-sized companies. Intuitively, it is hard to imagine that hacker organizations and nation-states would target small, little-known companies.[124] However, small, medium, and large companies today are interconnected and interdependent. Many large companies already have advanced cybersecurity systems that make it difficult for hackers to successfully mount direct attacks.[125] As such, hackers are beginning to turn to small and mid-sized companies, which often do not consider themselves targets and thus are less likely to have robust cybersecurity protection.[126] These companies may be contractors for larger companies, part of a larger company's supply chain, or simply have a wealth of information on their own that could be valuable to hackers.[127] The cybersecurity breach that compromised over fifty-six million credit card accounts of Home Depot customers was traced back to a breach at a small Home Depot vendor company.[128] The successful breach at OPM was also the result of IT system access through a vendor.[129] Other small

121. "[O]ver 80% of the cybercrime committed last year could have been avoided through better self-defense practices by individuals – or cyber hygiene." Tews & Cunningham, *supra* note 3.

122. *See supra* Section I.A.

123. KEOGH & CODY, *supra* note 7, at 5.

124. "The common perception is that this threat has been focused on large companies and governments." INTERNET SEC. ALL., *supra* note 46, at 1.

125. INTERNET SEC. ALL., *supra* note 46, at 1.

126. *Cybersecurity*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/navigation-structure/cybersecurity (last visited Mar. 9, 2016).

127. *Id.*

128. Banjo, *supra* note 9.

129. Perez & Prokupecz, *supra* note 58.

businesses could be directly responsible for critical infrastructure. For example, a successful attack on a small water treatment operator could impact several thousand people. Ensuring that companies of all sizes are protected will meet the government's interest in preventing all critical infrastructure threats.

4. Inaction or inadequate action now results in reactive laws and regulations later

The PATRIOT Act was lengthy, broad in scope, and passed very quickly.[130] Passage of the act in this manner was understandable under the circumstances. Time was of the essence following the September 11th attacks and the United States needed to ensure its national security regime could protect against another attack.[131] However, it was only after the act was passed that legislators and the public understood the full depth of authority the act gave to our government.[132] Since then, many have criticized the level of authority it instituted and the necessity of certain provisions.[133]

We have an opportunity to develop cybersecurity laws and regulations that address the interests of both the government and private sector and effectively mitigate the risk of APT attacks on our critical infrastructure sectors before a successful major attack occurs. If new measures are not developed or do not address APTs and there is a successful APT attack, there will be political pressure for reactive legislation to address the perceived cause of the attack.[134] This legislation will likely fall outside the framework prescribed here. It may be developed hastily, without private company leadership, creating disparities between companies of different sizes, or with inadequate public sector resources, resulting in ineffective policy that focuses more on inconsequential compliance than actual protection.[135]

A system that effectively addresses public and private sector concerns must be thoughtfully developed in order to facilitate a more effective response and faster recovery. Government efforts to address

130. *See* Toni Locy, *Patriot Act Blurred in the Public Mind*, USA TODAY (Feb. 25, 2004, 4:34 PM), http://usatoday30.usatoday.com/tech/news/techpolicy/2004-02-25-patriot-main_x.htm.

131. Brian B. Kelly, *Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform*, 92 B.U. L. REV. 1663, 1698 (2012).

132. Locy, *supra* note 130.

133. Jeffrey Rosen, *The Patriot Act Gives Too Much Power to Law Enforcement*, N.Y. TIMES: ROOM FOR DEBATE (Sept. 8, 2011, 11:54 AM), http://nyti.ms/1fQIRQR; *see generally* Kyle Welch, *The Patriot Act and Crisis Legislation: The Unintended Consequences of Disaster Lawmaking*, 43 CAP. U. L. REV. 481 (2015).

134. *See* Teplinsky, *supra* note 41, at 287.

135. *See id.* at 295.

cybersecurity thus far have not proven effective.[136] Two-thirds of cybersecurity professionals in a recent survey believe that the threat landscape is much worse or somewhat worse than it was in 2013.[137] Thirty percent of those professionals believe that the government cybersecurity strategy lacks clarity and thoroughness, while another 47% only believe the strategy is somewhat clear and thorough.[138] In order to effectively protect against APTs, the government must clarify its objectives as prescribed throughout this section.

One barrier to thoughtfully developed, comprehensive legislation may be that some advocates say we should only focus on improving areas of clear consensus such as information sharing, law enforcement, standard setting, and increasing research and development.[139] Focusing on areas of consensus is absolutely necessary, however, it will not be sufficient, as private critical infrastructure companies are already failing to address the advanced threats they face today,[140] let alone the evolving threats of tomorrow.[141] Taking the time to create a system that allows these companies to address evolving threats will ensure long-term protection.[142]

B. Laws and Regulations Developed by Industry-Led Public-Private Partnerships

There are several factors that weigh in favor of using public-private partnerships to address critical infrastructure cybersecurity threats. The use of these partnerships to address cybersecurity is already widely supported by both the public and private sectors.[143] It is also important to look at what the public sector and the private sector separately bring to the public-private partnership model. The private sector has expertise about their companies to know where their cybersecurity stands now and what needs to be done to effectively increase their protection without misallocating company resources.[144] As such, the private sector should take the lead on developing the new regime. However, government

136. Jon Oltsik, *Cybersecurity, Critical Infrastructure, and the Federal Government*, NETWORK WORLD (Apr. 29, 2015, 7:07 AM), http://www.networkworld.com/article/2916573/cisco-subnet/cybersecurity-critical-infrastructure-and-the-federal-government.html.

137. *Id.*

138. *Id.*

139. *See* Teplinsky, *supra* note 41, at 295.

140. Withers, *supra* note 45.

141. MCCONNELL ET AL., *supra* note 111, at 6.

142. *Id.*

143. Letter from Josten, *supra* note 85, at 1; Press Release, The White House, Securing Cyberspace – President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts (Jan. 13, 2015), http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

144. Sales, *supra* note 1, at 1518.

participation adds important pieces to make this a reality. The government has incentive, information, financial resources, and the ability to facilitate coordination among private companies.

The private sector and government should work together to protect against APTs in each critical infrastructure sector. Some argue that the government should be minimally involved.[145] This is not only unrealistic,[146] it is unnecessary and unwise. Eighty-three percent of cybersecurity professionals in one survey believe that the federal government should be more involved in cybersecurity strategies.[147] Additionally, private sector companies have already expressed support for public-private partnerships to address cybersecurity threats.[148] In fact, public-private partnerships in cybersecurity for critical infrastructure already exist.[149] The NIST Framework was not the government's first foray into cybersecurity for these sectors. While the NIST Framework incorporated many industry best practices, public-private partnerships have long existed in the financial, energy, and water sectors.[150] There is no reason this willingness to cooperate should not be utilized to develop a solution on common ground.[151] Private sector companies will benefit from the government's resources and threat knowledge, while ensuring that laws and regulations set realistic expectations that do not result in misallocated resources.[152] The government should create public-private partnerships that give private companies the resources to address APTs.

1. Private sector-led approach

The path to new cybersecurity laws and regulations should be an industry-led approach.[153] Private companies are the experts on their

145. *See generally* Paoletta, *supra* note 72, at 84.

146. *See supra* Section I.B.

147. Oltsik, *supra* note 136.

148. Intel Corporation, *supra* note 20 (noting that 86% of executives in critical infrastructure organizations in one survey believe that cooperation between the public and private sectors on infrastructure protection is critical to successful cyber defense). *See also* Letter from Josten, *supra* note 85, at 1.

149. *See* BLEIER, NAGLE & FATHERLEY, *supra* note 15, at 4–5 (explaining that the financial sector leads other critical infrastructure industries in cybersecurity protection in no small part due to a public-private partnership).

150. *See, e.g.*, *id.* at 5; *Standards*, NERC, http://www.nerc.com/pa/stand/Pages/default.aspx (last visited Mar. 9, 2016); Michael Deane, *Water Utility Sector Works in Partnership to Meet Cyber Security Challenges*, HUFFINGTON POST (Feb. 4, 2014, 5:59 AM), http://www.huffingtonpost.com/michael-deane/water-utility-sector-work_b_4373213.html.

151. MCCONNELL ET AL., *supra* note 111, at 8.

152. Sales, *supra* note 1, at 1518.

153. The Advanced Cyber Security Center argues that "[a] new national strategy that incentivizes and supports industry initiatives rather than depending on legislation best positions us to take on the cyber challenge," but given the necessity of legislation, an industry-led approach to developing legislation is the next best thing. ADVANCED CYBER SECURITY CTR., ADVANCED CYBER SECURITY CENTER ROLLOUT 2 (2013) (emphasis omitted), http://csrc.

systems; they know them best and are therefore in the best position to identify the cybersecurity measures necessary to protect them.[154] Furthermore, the private sector can best leverage the government's interests and resources to ensure the laws and regulations address current problems.

Private companies are concerned that some members of Congress believe laws and regulations will be a silver bullet that eliminates cyberthreats.[155] There is no more a perfect solution to cybersecurity than there is to physical security.[156] The private sector is right to be wary of additional laws and regulations driven by a desire to have perfect protection. Laws created under the guise of seeking perfection are more likely to realize the private sector's concern that the laws will focus on compliance rather than effectiveness.[157] Such laws will likely also require companies to use extensive resources in an attempt to achieve perfection.[158]

Allowing the private sector to lead the development of new laws and regulations will ensure that the new measures take a realistic approach to addressing threats.[159] However, the private sector cannot simply prescribe a specific approach without explanation. Industry must effectively embark on an education campaign for our legislators, informing them that a perfect solution is unrealistic and setting expectations for a highly effective cybersecurity system that may, at the same time, unfortunately still result in some successful attacks.[160]

A government-led cybersecurity framework also runs the risk of mandating specific technologies.[161] This would lead to one-size-fits-all outcomes or artificially chosen winners and losers among cybersecurity product developers.[162] This would disincentivize or disadvantage new entrants into the cybersecurity industry and, in turn, would result in less competition-driven innovation in new cybersecurity products. In short, such an approach would lay the foundation for a monopolized cyber-defense industry that will eventually become ineffective at developing products that protect against ever-diversifying threats.

---

nist.gov/cyberframework/rfi_comments/040813_advanced_cyber_security_center.pdf.

154. Sales, *supra* note 1, at 1518.

155. David Inserra & Paul Rosenzweig, *Continuing Federal Cyber Breaches Warn Against Cybersecurity Regulation*, HERITAGE FOUND. (Oct. 27, 2014), http://www.heritage.org/research/reports/2014/10/continuing-federal-cyber-breaches-warn-against-cybersecurity-regulation.

156. MCCONNELL ET AL., *supra* note 111, at 6; Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1019 (2014).

157. *See* Paoletta, *supra* note 72, at 84.

158. Teplinsky, *supra* note 41, at 232.

159. Sales, *supra* note 1, at 1556.

160. MCCONNELL ET AL., *supra* note 111, at 6.

161. Letter from Josten, *supra* note 85, at 2.

162. *Id.*

The private sector can best focus on developing a regime that addresses the actual challenge of protecting against APTs. Some argue that the United States should create a new government agency that oversees cybersecurity for all sectors.[163] This suggestion misses the mark. We should not attempt to do more than is necessary to achieve the goal, and such an approach may actually have unintended consequences, especially those that the private sector fears will come to fruition.

The new regime should address only the actual problems that exist. As previously discussed, the private sector does not have adequate incentive to address APTs.[164] Additionally, many companies do not have the information available to know the extent of what they need to protect against.[165] Finally, there is not enough coordination among companies in critical sectors to ensure that they are working together to address the threats for companies of all sizes.[166] A new cybersecurity regime should be designed to address these concerns only. As such, while the private sector takes the lead on developing a framework for APT protection, the government should provide the incentive, information, coordination, and financial resources to make this possible.

2. Government contributions

The government is in the best position to provide the incentive, information, coordination, and financial resources to allow the private sector to address APTs. As a preliminary matter, the government can serve as a clearinghouse for the types of attacks that are taking place.[167] This is in no small part because the government is the target of so many attacks.[168] It can aggregate public and private sector information to provide insight

163. One commentator suggests that such an approach could be modeled after Israel's system. Eli Sugarman, *What the United States Can Learn from Israel About Cybersecurity*, FORBES (Oct. 7, 2014, 8:54 AM), http://www.forbes.com/sites/elisugarman/2014/10/07/what-the-united-states-can-learn-from-israel-about-cybersecurity. This commentator notes that the Israeli system is, in part, a product of the mindset of their citizens, who accept such a broad approach. He further notes that such a system, if adopted in the U.S., would help educate the public on the significance of cybersecurity threats. This system misses the mark for Americans, who value private sector leadership, and only seek such extensive government solutions when absolutely necessary. Additionally, the American public is already beginning to understand the significance of cyberthreats, a hot topic in the public discourse. *See* Warner, *supra* note 11, at 11. In February 2015, President Obama announced the creation of the Cyber Threat Intelligence Integration Center, a new agency that will analyze cyberthreats and coordinate strategy. It does not have authority over private-sector practices. Ellen Nakashima, *New Agency to Sniff Out Threats in Cyberspace*, WASH. POST (Feb. 10, 2015), http://wpo.st/6aNK1.

164. *See supra* Section I.C.

165. Sales, *supra* note 1, at 1518.

166. *Id.* at 1530.

167. Trautman, *supra* note 34, at 360.

168. Javier Ortiz, *Government Needs the Private Sector to Improve Cybersecurity*, THE HILL (Aug. 6, 2014, 1:00 PM), http://thehill.com/blogs/congress-blog/technology/214361-government-needs-the-private-sector-to-improve-cybersecurity.

on the cyberthreat landscape to private entities that will allow them to address security holes in their systems that could make them subject to such attacks.[169] In December 2015, Congress passed and the President signed new legislation that facilitates information sharing between private companies and the government.[170] Prior to passage of the law, companies feared they would be held liable if they self-reported that they fell victim to a cyberattack.[171] Companies were also wary to share information about when they were attacked for fear that it would have an economic impact on their business.[172] Consequently, a company in one sector might not have known what cyberattacks were being launched on a company in the same sector, preventing it from protecting against the same attack should it be the next target.[173] The lack of information-sharing ultimately resulted in a weakness in the private sector's cybersecurity efforts. Because the new law gives companies a way to confidentially share information with the government and avoid liability, it is a step in the right direction.[174] However, it is not yet clear how effective the law will be, particularly because it is voluntary.[175] As such, additional measures may be needed to spur information sharing.

The government is also in the best position to provide coordination among companies in each sector, and cross-sector coordination as necessary. Some sectors have trade groups that coordinate cybersecurity efforts,[176] but these groups do not necessarily have membership from a large majority of companies in each sector and they may exclude companies on the fringes—those that are smaller or that have a different business model. Some existing public-private partnerships, particularly in the financial sector, have already shown how coordination can have an effective impact on cybersecurity practices.[177] The government's

169. Josephine Wolff, *Unto the Breach*, SLATE (June 19, 2014, 12:02 PM), http://www.slate.com/articles/technology/future_tense/2014/06/fcc_chairman_tom_wheeler_on_regulating_cybersecurity.html.

170. Carey, Gerver & Wainstein, *supra* note 37.

171. JONES DAY, *supra* note 42, at 2. "Businesses need certainty that threat information voluntarily shared with the government would be exempt from public disclosure and prohibited from use by officials in regulatory matters. Legislation needs to provide legal protection for companies that guard their own networks in good faith or disclose cyber threat information with appropriate entities." Letter from Josten, *supra* note 85, at 3 (emphasis omitted).

172. N. ERIC WEISS, CONG. RESEARCH SERV., R43821, LEGISLATION TO FACILITATE CYBERSECURITY INFORMATION SHARING: ECONOMIC ANALYSIS 5 (2015), http://fas.org/sgp/crs/misc/R43821.pdf.

173. *See* Sales, *supra* note 1, at 1529.

174. Carey, Gerver & Wainstein, *supra* note 37.

175. *Id.*

176. Charlie Mitchell, *Industry Sectors Taking Different Approaches to Cyber Framework*, INSIDE CYBERSECURITY (June 9, 2014), http://insidecybersecurity.com/Cyber-General/Cyber-Public-Content/industry-sectors-taking-different-approaches-to-cyber-framework/menu-id-1089.html.

177. BLEIER, NAGLE & FATHERLEY, *supra* note 15, at 4–5.

coordination efforts will bring a wider swath of private companies into the fold.

Financial resources may be the largest barrier for companies to protect against APTs. There are two sides to this issue. First, the government is not a bank that can simply dole out money when the private sector is not apt to make investments for its own protection. The private sector has to realize that, if unaddressed, a point would come where the economic losses from cybersecurity breaches from APTs will exceed the costs of protecting against these threats.[178] As such, the private sector should have the incentive to invest in stronger cybersecurity measures. However, the costs to protect against evolving threats will also continue to increase.[179] The government is in the best position to help the private sector offset these expenses.[180] The government also has the incentive to provide these resources as a result of its desire to protect against APTs.[181] If the choice is between the government spending tax money to create an agency that can oversee national cybersecurity in the private sector or the government investing in private companies to allow them to develop cybersecurity, the latter option will better ensure that the financial resources are used by private companies to create a system that effectively prevents APTs. These resources will be particularly important for small companies, who lack resources, but which the government has a high interest in protecting.[182] Some options for government funding of private-sector APT protection efforts include direct funding, matching funds, grants, and tax credits.[183]

C. Sector-Specific Laws and Regulations Under Expert Agencies

Cross-sector, comprehensive cybersecurity laws and regulations would not be effective. Threats to the food production industry will not be the same as the financial industry, which will not be the same as the defense industry.[184] Any sort of comprehensive framework is likely to be ineffective in addressing the specific needs of each sector.[185] In fact, companies will spend more time trying to show that they are meeting the expectations of the comprehensive framework than they will actually

178. In 2012, cybercrimes cost U.S. companies an average of $8.9 million. JONES DAY, *supra* note 42, at 2.

179. SPINA & SKEES, *supra* note 66, at 3.

180. *See* Cohen, *supra* note 100.

181. *See supra* Section I.B.

182. *See supra* Section II.A.3.

183. Robert Gyenes, *A Voluntary Cybersecurity Framework Is Unworkable—Government Must Crack the Whip*, 14 U. PITT. J. TECH. L. POL'Y 293, 311 (2014); ADVANCED CYBER SECURITY CTR., *supra* note 153, at 2; Palmer, *supra* note 109, at 365.

184. *See* Hoffman, *supra* note 33, at 3; MCCONNELL ET AL., *supra* note 111, at 4.

185. MCCONNELL ET AL., *supra* note 111, at 4.

protecting against the threats that particular sector is most likely to face.[186] Their compliance may be no more than mapping their cyber practices to the framework, rather than actually implementing practices that the framework requires.[187]

A regulatory regime based on the NIST Framework would be particularly problematic. The NIST Framework was designed to provide high-level guidance to all critical infrastructure sectors, not to address the particularities of each individual sector's cybersecurity needs.[188] As such, some private companies have a legitimate concern that the NIST Framework is the first step in promulgating regulations.[189] Such an approach would make their concern of an ineffective, compliance-based system a reality.[190]

Congress should give sector-specific agencies the flexibility to work with companies in their sectors to develop regulations that are sector-appropriate.[191] One method to achieve this would be through the "sector-based risk assessments already being conducted by DHS [Department of Homeland Security] (or a sector-specific agency) and industry under the National Infrastructure Protection Plan."[192] Congress should also work to reduce "fragmented and often conflicting burdens" developed by regulatory agencies that have oversight over multiple sectors.[193] One option would be to pass legislation that harmonizes efforts between agencies to avoid turf wars, including designating DHS to play a supporting role for sector-specific agencies. "New legislation should not create parallel or duplicative authorities to address cybersecurity threats and vulnerabilities as businesses tend to prefer working with a single agency."[194] Each agency a company deals with necessarily increases costs. Instead, "legislation should support efforts that genuinely enhance

186. Letter from Josten, *supra* note 85, at 3.

187. For example, early use of the NIST Framework has entailed companies and sectors mapping their existing practices and frameworks to the NIST Framework rather than implementing new practices driven by the Framework. Dale Peterson, *NIST Cybersecurity Framework – 3 Months Later*, DIGITAL BOND (May 19, 2014), http://www.digitalbond.com/blog/2014/05/19/nist-cybersecurity-framework-3-months-later.

188. Palmer, *supra* note 109, at 346; BOOZ ALLEN HAMILTON, CYBER SOLUTIONS HANDBOOK: MAKING SENSE OF STANDARDS AND FRAMEWORK 4 (2014), http://www.boozallen.com/content/dam/boozallen/documents/Cyber-Solutions-Handbook.pdf.

189. Nagesh, *supra* note 42.

190. Palmer, *supra* note 109, at 362.

191. "The U.S. is hampered by an outdated bureaucratic structure that empowers military and intelligence agencies over civilian ones – even those civilian agencies with technical knowledge and skills." Sugarman, *supra* note 163. "[T]he involvement of each critical infrastructure sector in crafting a sector-specific cybersecurity framework would probably result in better, less-generalized standards for those sectors that produce a framework." Palmer, *supra* note 109, at 364.

192. Letter from Josten, *supra* note 85, at 2.

193. *Id.* at 3.

194. *Id.* at 3.

collaboration between industry and government partners and that foster mutually agreed-upon solutions targeted at increasing collective security."[195]

Other laws passed by Congress should only be used to addresses across-the-board challenges, such as information sharing, privacy, and liability, leaving the agencies to tackle sector-specific needs. The private sector supports "legislation . . . that would address the need of businesses to receive timely and actionable information from government analysts to protect their enterprises by improving detection, prevention, mitigation, and response through enhanced situational awareness."[196]

CONCLUSION

The critical infrastructure sectors that provide essential services to Americans are under a constant barrage of cyberattacks from sophisticated hackers. A successful attack with severe consequences is on the horizon. While the private sector controls the vast majority of critical infrastructure in the United States, the government has a national security interest in protecting those assets from cyberthreats. There is a gap between the government's interest in protecting against unlikely, but destructive, APTs and the private sector's interest in utilizing a cost-effective, risk-based approach to protect against cyberthreats. To ensure that the private sector addresses all cyberthreats, additional legislation and regulations are not just inevitable, they are necessary.

The government and private sector should work together to develop laws and regulations that will ensure a high level of protection against APTs before a successful attack occurs. These measures should be developed to address the concerns and interests of both the private and public sectors, and they should be no broader than necessary to address the different perspectives of both sectors. Specifically, they should ensure that critical infrastructure companies of all sizes can protect against APTs. Such measures should also be thoughtfully developed now to prevent reactive measures in the future. An industry-led public-private partnership approach will ensure that the measures are effective, and benefit from the government's resources. Placing the regulatory authority under sector-specific agencies will prevent the creation of an ineffective cross-sector solution. This approach will result in a framework that ensures American critical infrastructure is protected from evolving cybersecurity threats.

195. *Id.* at 3.
196. *Id.* at 5.