Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices

SCOTT J. SHACKELFORD, JD, PHD*; ANDREW A. PROIA, JD**; BRENTON MARTELL, JD***; & AMANDA N. CRAIG, MSC, JD****

ABSTRACT

Even though U.S. congressional and multilateral efforts aimed at enhancing cybersecurity have thus far largely failed in their aims, courts and regulators are using existing common law doctrines and statutory enactments to hold companies accountable for cyber attacks. However, such judicial and regulatory actions have often been haphazard, due in part to confusion over what constitute reasonable standards of cybersecurity care. This Article analyzes the emerging cybersecurity duty of care and examines the potential impact of the 2014 National Institute of Standards and Technology (NIST) Cybersecurity Framework on shaping reasonable standards of cybersecurity. Given that cybersecurity best practices are not yet well defined, the NIST Framework has the potential to shape standards not only for critical infrastructure firms but also for the private sector writ large. Indeed, the Federal Communications Commission (FCC) in November 2013 wrote that it plans "to use an emerging framework of cybersecurity standards to assess and prioritize best practices . . . to address evolving cyber threats" in the telecommunications industry.[1] Moreover, the NIST Framework has the potential to shift the

* Assistant Professor of Business Law and Ethics, Indiana University; Senior Fellow, Center for Applied Cybersecurity Research; Distinguished Visiting Fellow, Notre Dame Institute for Advanced Study; Edward Teller National Fellow, Hoover Institution, Stanford University.

** JD, Indiana University Maurer School of Law; Postdoctoral Fellow, Indiana University Center for Applied Cybersecurity Research.

*** JD, Indiana University Maurer School of Law.

**** Senior Cybersecurity Strategist, Microsoft Corporation; MsC, University of Oxford; JD, Indiana University Maurer School of Law.

1. FCC, *Telecom Industry Plan to Map Current Best Practices to NIST Framework*, INSIDE CYBERSECURITY (Nov. 20, 2013), http://insidecybersecurity.com/index.php?option=com_user&view=login&return=aHR0cDovL2luc2lkZWN5YmVyc2VjdXJpdHkuY29tL0N5YmVyLURhaWx5LU5ld3MvRGFpbHktTmV3cy9mY2MtdGVsZWNvbS1pbmR1c3RyeS1wbGFuLXRvLW1hcC1jdXJyZW50LWJlc3QtcHJhY3RpY2VzLXRvLW5pc3QtZnJhbWV3b3JrL21lbnUtaWQtMTA3NS5odG1s [hereinafter FCC,

cybersecurity landscape internationally, especially in jurisdictions that largely favor a voluntary approach to enhancing cybersecurity, including the United Kingdom, India, and to a lesser extent, the European Union. The uptake of the NIST Framework beyond the United States could help to foster a global standard of cybersecurity care, promoting consistency, benefitting businesses active across jurisdictions, and contributing to cyber peace.

SUMMARY

Telecom Industry].

INTRODUCTION

> The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.
>
> – Executive Summary, NIST Cybersecurity Framework[2]

During the winter of 2013–2014, amidst the school delays and extreme weather conditions in much of the United States,[3] the federal Emergency Alert System issued a warning, but perhaps not the one people expected: "Civil authorities in your area have reported that the bodies of the dead are rising from their graves and attacking the living . . . . Do not attempt to approach or apprehend these bodies, as they are considered extremely dangerous."[4] Hackers had penetrated the System to issue a "bogus zombie alert" in yet another episode showcasing the myriad vulnerabilities buried in "critical systems throughout [U.S.] government."[5] Aside from being fodder for bored hackers, such weaknesses can be exploited by cyber criminals, terrorists, and nation States, which makes securing "critical infrastructure" a key test of effective cybersecurity policymaking.[6] Thus far, though, it is a test that many nations, including the United States, the United Kingdom, and India, are failing.

2. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1 (2014) [hereinafter NIST CYBERSECURITY FRAMEWORK].

3. *See National Overview—February 2013*, NOAA (Mar. 2013), http://www.ncdc.noaa.gov/sotc/national/2013/2 ("Three major winter storms impacted the nation during February, contributing to an above-average monthly snow cover . . . ."). Note that sections of this material are adapted from SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014) [hereinafter SHACKELFORD, MANAGING CYBER ATTACKS].

4. Craig Timberg & Lisa Rein, *Senate Cybersecurity Report Finds Agencies Often Fail to Take Basic Preventive Measures*, WASH. POST, Feb. 4, 2014, http://www.washingtonpost.com/business/technology/senate-cybersecurity-report-finds-agencies-often-fail-to-take-basic-preventive-measures/2014/02/03/493390c2-8ab6-11e3-833c-33098f9e5267_story.html (omission in original).

5. *Id.*

6. *E.g.*, Exec. Order No. 13636, 78 Fed. Reg. 11739, 11739 (Feb. 19, 2013) ("[C]ritical infrastructure

The growing danger posed by seemingly ever-more sophisticated and plentiful cyber attackers, especially as it relates to securing critical infrastructure, is not news. For example, former National Security Agency (NSA) and U.S. Cyber Command chief General Keith Alexander told a Senate committee in June 2013 that "'[o]n a scale of one to 10, with 10 being strongly defended, our critical infrastructure's preparedness to withstand a destructive cyber attack is about a three based on my experience.'"[7] Similarly, the lack of progress—not only in Congressional efforts, as seen in the debates surrounding the Cybersecurity Act of 2012,[8] but also in international efforts aimed at managing cyber attacks—is well documented.[9] This lack of regulatory engagement has often left judges in an uncertain position about what steps companies, including those operating critical infrastructure, should take to secure their data and systems.[10] A lack of definition regarding what constitutes a standard of care in the cybersecurity context has been the result. Enter the Obama Administration.

In February 2013, President Obama issued an executive order that, among other things, expanded public-private information sharing and tasked the NIST with establishing a voluntary "Cybersecurity Framework" comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure.[11] The Framework version 1.0, Framework for Improving Critical Infrastructure Cybersecurity, was released in February 2014.[12] The Cybersecurity Framework "harmonizes consensus standard and industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk."[13] The Framework provides a voluntary procedure to map cybersecurity best practices, determine the overall state of an organization's cyber

means 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.").

7. *NSA Chief Says U.S. Infrastructure Highly Vulnerable to Cyber Attack*, REUTERS, June 12, 2013, http://www.reuters.com/article/2013/06/12/us-usa-cybersecurity-idUSBRE95B10220130612.

8. *See*, *e.g.*, Scott J. Shackelford, Essay, *In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012*, 64 STAN. L. REV. ONLINE 106, 109–10 (2012) (discussing congressional efforts around the Cybersecurity Act of 2012). *But see U.S. Senators Push Ahead with Cybersecurity Legislation*, REUTERS, June 17, 2014, http://www.reuters.com/article/2014/06/17/us-usa-cybersecurity-congress-idUSKBN0ES29N20140617 (discussing the expectation of Congressional cybersecurity enactments).

9. *See*, *e.g.*, Tom Gjelten, *Seeing the Internet as an 'Information Weapon'*, NPR (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701 (discussing the fact that United Nations–sponsored cyber disarmament discussions have been ongoing since the late 1990s without much to show for it); Tony Romm, *Cybersecurity in Slow Lane One Year after Obama Order*, POLITICO, Feb. 9, 2014, http://www.politico.com/story/2014/02/cybersecurity-in-slow-lane-one-year-after-obama-order-103307.html?hp=f1 ("Nearly a year after President Barack Obama issued an executive order to improve the cybersecurity of the nation's vital assets, the administration doesn't have much to show: The government is about to produce only some basic standards, with little incentive for the private sector to participate.").

10. *See* Guin v. Brazos Higher Educ. Serv., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *4 (D. Minn. Feb. 7, 2006) (dealing with the difficulties associated with applying negligence to cases involving cyber security).

11. Exec. Order No. 13636, 78 Fed. Reg. at 11740–41.

12. NIST CYBERSECURITY FRAMEWORK, *supra* note 2.

13. Scott J. Shackelford & Andrew Proia, *Why Ignoring the NIST Framework Could Cost You*, HUFFINGTON POST (May 2, 2014), http://www.huffingtonpost.com/scott-j-shackelford/why-ignoring-the-nist-fra_b_5244112.html.

risk management practices, and structure roadmaps for organizations to mitigate those risks.[14]

To date, responses to the Framework have been mixed. Some, for instance, have argued that the Framework "represents the best efforts of the administration and . . . industry representatives from the 16 critical infrastructure sectors to work together to address a threat which President Obama has called one of the gravest national security dangers the United States faces."[15] Indeed, since its release, the Framework has garnered support from state and federal legislators, business executives, and public interest organizations.[16] However, praise has not been universal. Some, for example, have cautioned that the Framework does not go far enough in terms of its scope, influence, and impact.[17] One of the main questions surrounding the NIST Framework is how "voluntary" it will actually turn out to be—as well as how voluntary it should be.[18]

From its inception, the Framework has been developed with an aim toward creating a cost-effective method of addressing critical infrastructure cybersecurity vulnerabilities without enacting binding (and potentially cumbersome and inflexible) regulatory requirements.[19] Depending on the success of this and other similar programs, the Framework could help establish a baseline "standard of cybersecurity care" that could define legal liability for critical infrastructure organizations prior to

14. *See generally* NIST CYBERSECURITY FRAMEWORK, *supra* note 2.

15. Ian Wallace, *Introductory Remarks at the Brookings Institution's Panel Discussion, Improving Critical Infrastructure Cybersecurity: The Cybersecurity Framework and Beyond* (C-SPAN television broadcast Feb. 19, 2014), *available at* http://www.c-span.org/video/?317876-1/critical-infrastructure-cybersecurity-framework/.

16. *See generally* WHITE HOUSE, CYBERSECURITY FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE: WHAT OTHERS ARE SAYING (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/cybersecurity_framework_-_what_others_are_saying_2_27.pdf (providing statements of approval from various company executives, federal, state, and local governmental officials, and civil society and privacy groups).

17. *See*, *e.g.*, Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, CHRISTIAN SCI. MONITOR, Feb. 13, 2013, http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts (discussing shortcomings of the Executive Order, including that it failed to stress the importance of its recommendations); Romm, *supra* note 9 ("Nearly a year after President Barack Obama issued an executive order to improve the cybersecurity of the nation's vital assets, the administration doesn't have much to show: The government is about to produce only some basic standards, with little incentive for the private sector to participate.").

18. *See*, *e.g.*, *NIST's Voluntary Cybersecurity Framework May Be Regarded as De Facto Mandatory*, HOMELAND SECURITY NEWS WIRE (Mar. 3, 2014), http://www.homelandsecuritynewswire.com/dr20140303-nist-s-voluntary-cybersecurity-framework-may-be-regarded-as-de-facto-mandatory (stating that experts have warned that many of the recommendations in the framework "may be used by courts, regulators, and even consumers to hold institutions accountable for failures that could have been prevented if the cybersecurity framework had been fully implemented by the respective institution").

19. The Departments of Homeland Security, Treasury, and Commerce have proposed incentives that could encourage voluntary utilization of the Framework. Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, WHITE HOUSE BLOG (Aug. 6, 2013), http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework [hereinafter Daniel, *Incentives*]; *see also infra* note 240; Charlie Mitchell, *DHS Tightens Explanation of How Cyber Voluntary Program Will Help Industry*, INSIDE CYBERSECURITY (Feb. 24, 2014), http://insidecybersecurity.com/Cyber-General/Cyber-Public-Content/dhs-tightens-explanation-of-how-cyber-voluntary-program-will-help-industry/menu-id-1089.html (reporting on the promotion of the voluntary C-Cubed program for cybersecurity standards by the Department of Homeland Security).

and following cyber attacks. Currently, no baseline, comprehensive cybersecurity obligations are imposed across all of the U.S. critical infrastructure, but regulations do exist for certain sectors,[20] leaving the status quo a complex patchwork of oftentimes ambiguous state and federal regulations overlaying applicable common law doctrines.[21]

The NIST Framework not only has the potential to shape a standard of care for domestic critical infrastructure organizations but also could help to harmonize global cybersecurity best practices for the private sector writ large.[22] Existing legal literature has yet to delve deeply into shaping a standard of care in the cybersecurity context.[23] This Article fills that niche by analyzing to what extent cybersecurity standards of care are emerging organically and examining the potential impact of the NIST Framework on crystallizing best practices in the United States and beyond.[24] There is some evidence this may in fact already be occurring,[25] including in jurisdictions that favor a largely voluntary approach to enhancing cybersecurity such as the United Kingdom,[26] India,[27] and, to a lesser extent, the European Union (EU).[28]

20. EDWARD C. LIU ET AL., CONG. RESEARCH SERV., R42409, CYBERSECURITY: SELECTED LEGAL ISSUES 1–2 (2012).

21. *See* ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 52–61 (2013) (identifying over forty laws with provisions related to cybersecurity).

22. For example, some stakeholders have already argued that any time a "company's cybersecurity practices are [] questioned during a regulatory investigation and litigation, the baseline for what's considered commercially reasonable is likely to become the NIST Cybersecurity Framework." Gerald Ferguson, *NIST Cybersecurity Framework: Don't Underestimate It*, INFORMATIONWEEK (Dec. 9, 2013), http://www.informationweek.com/government/cybersecurity/nist-cybersecurity-framework-dont-underestimate-it/d/d-id/1112978.

23. *Cf.* Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11, 17–21 (2002) (arguing for adoption of traditional negligence law principles in the context of information security); Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 260 n.25 (2005) (investigating elements of an emerging duty of care in the identity theft context); Vincent R. Johnson, *Data Security and Tort Liability*, J. INTERNET L., Jan. 2008, at 22, 23–24 [hereinafter Johnson, *Data Security*] (discussing "voluntary assumption of a duty to protect data"); Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 301–03 (2013) (discussing recent legislative proposals addressing cybersecurity); Emily Kuwahara, Note, *Tort v. Contracts: Can Microsoft Be Held Liable to Home Consumers for Its Security Flaws?*, 80 S. CAL. L. REV. 997, 1014–15 (2007) (discussing policies behind the standard of care imposed); Kathryn E. Picanso, Note, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 377–80 (2006) (examining the duty of care in the information security context).

24. Our focus in this regard is primarily on negligence case law. However, other applicable areas of law including fiduciary duties and statutory compliance will also be examined. For instance, "chemical facilities are subject to chemical facility anti-terrorism standards (CFATS) promulgated by the Department of Homeland Security (DHS), which include provisions requiring chemical facilities to take measures to protect against cyber threats." LIU ET AL., *supra* note 20, at 1–2.

25. *FCC, Telecom Industry*, *supra* note 1, ("The telecommunications industry and the Federal Communications Commission plan to use an emerging framework of cybersecurity standards to assess and prioritize best practices for the sector as it works to address evolving cyber threats . . . .").

26. *E.g.*, Jane Jenkins, *The Network and Information Security Directive—What Role Can Regulation Play in Improving CyberSecurity: The Legal Perspective*, *in* CYBER SECURITY 2.0: REFLECTIONS ON UK/EU CYBER SECURITY CO-OPERATION 10, 11 (2014) ("The UK Government . . . advocates a policy of voluntary information sharing and has therefore set up the information sharing partnership (CISP) to encourage the sharing of information about attacks and the means to combat them.").

27. *FCC, Telecom Industry*, *supra* note 1.

28. *Proposal for a Directive of the European Parliament and of the Council concerning Measures to*

For businesses active across jurisdictions, and depending on the uptake of the NIST Framework by stakeholders, a global standard of cybersecurity care could eventually emerge that would promote consistency and contribute to "cyber peace" even absent regulatory action.[29]

In an effort to explore the past, present, and future development of a cybersecurity standard of care both domestically and globally, this Article is structured as follows: Part I sets the stage by analyzing the current state of U.S. law shaping a cybersecurity duty of care. Part II then lays out the NIST Framework, discussing its origins and evolution. Finally, Part III applies the findings from Part II to the legal doctrines revealed in Part I in an effort to hypothesize about what impact the NIST Framework might have on shaping a cybersecurity duty of care not only in the United States but also in the EU and India.[30] It should also be noted that this represents merely an initial attempt to frame some of the many topics coming out of the NIST process. Follow-up studies will be required, especially after (and assuming) more firms have begun adopting the Framework, to assess the long-term impact of the NIST Framework on managing the global cyber threat.

I. REVIEW OF EXISTING U.S. LAW SHAPING A CYBERSECURITY DUTY OF CARE

What constitutes the burgeoning field of "cybersecurity law and policy" is open to debate—but likely encompasses a wide array of topics from cyber-crime and privacy to data protection, contracts, torts, intellectual property, and even Internet governance.[31] For the present purposes, cybersecurity refers to the policy field

Ensure a High Common Level of Network and Information Security across the Union, at 3, COM (2013) 48 final (Feb. 7, 2013) (requesting legislative measures to improve on the current, voluntary approach to cybersecurity standards of care).

29. Efforts to date aimed at defining "cyber peace" have been minimal. The International Telecommunication Union (ITU), a U.N. agency specializing in information and communication technologies (ICTs) has likened "cyber peace" as being a necessary element in a "universal order of cyberspace" built on a "wholesome state of tranquility, the absence of disorder or disturbance and violence." Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 78 (2011), *available at* http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf. Although certainly desirable, such an outcome is politically unlikely and technically infeasible. *See* Joseph S. Nye, Jr., *Power and National Security in Cyberspace*, *in* 2 AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 5, 19–20 (Kristin M. Lord & Travis Sharp eds., 2011) (stating that many countries disagree about the scope or extent of enforcement of a future cyber treaty); *but see* Scott Shackelford, *The Meaning of Cyber Peace*, 2 NDIAS Q. 12, 13 (2013), *available at* http://www3.nd.edu/~gosborn/NDIAS-Quarterly_Fall-2013/FLASH/index.html (arguing that "[i]nstead of focusing on a single path to cyber peace," which is untenable due to the divergent ideas of what cybersecurity requires, global cyber peace should follow a "polycentric framework").

30. These jurisdictions were chosen as case studies since they have to date relied on a voluntary approach to enhancing national and regional cybersecurity similar to the United States. Moreover, especially in the case of the European Union (EU), U.S.–EU policymakers are in regular contact and the NIST Framework could do much to shape EU efforts in this space. *See generally Official: EU Eying NIST Framework With 'Great Interest'*, INSIDE CYBERSECURITY (Feb. 4, 2014), http://insidecybersecurity.com/index.php?option=com_user&view=login&return=aHR0cDovL2luc2lkZWN5YmVyc2VjdXJpdHkuY29tL0N5YmVyLURhaWx5LU5ld3MvRGFpbHktTmV3cy9vZmZpY2lhbC1ldS1leWluZy1uaXN0LWZyYW1ld29yay13aXRoLWdyZWF0LWludGVyZXN0L21lbnUtaWQtMTA3NS5odG1s (discussing official EU interest in the NIST framework).

31. *See* FISCHER, *supra* note 21, at summary, para. 3 ("More than 50 statutes address various aspects

concerned with managing cyber threats, including unauthorized access, disruption, and modification of electronically stored information, software, hardware, services, and networks.[32] The cyber threat matrix itself is always evolving; it consists of activities ranging from cyber economic-espionage that targets trade secrets and is carried out by transnational criminal organizations—sometimes at the behest of nation states—to "hacktivists" out to make a political point.[33] Many firms have begun to proactively invest in cybersecurity best practices to better protect themselves against increasingly sophisticated attackers,[34] but the ever-changing nature of the problem and sheer number of actors involved have made crafting a cybersecurity standard of care difficult.

Yet despite gaps in the legal framework and the ever-changing cyber threat, courts are increasingly willing to hold both organizations and firms liable for not protecting sensitive information. For example, the Michigan Court of Appeals held a union responsible for failing to safeguard the private information of members who became victims of identity theft.[35] Additionally, a federal court judge [BD1]in Michigan ruled that a local bank was at fault for not detecting earlier the losses its customers sustained through a phishing attack.[36]

There [BD2]have also been major class actions filed in invasion of information privacy lawsuits. Two such cases filed in 2003 against several of the largest information brokers in the United States also implicated the state of Florida for not protecting the privacy of its residents.[37][BD3] Damages sought were more than $2500 per violation, adding up to billions under the federal Driver Privacy Protection Act.[38] Ultimately, one of the defendant banks in the case was fined $50 million for purchasing data containing the personal information of hundreds of thousands of Florida residents for just $5656.[39] In 2006, ChoicePoint, a large data broker that maintains digital dossiers on many adults in the United States, was fined $10 million by the Federal Trade Commission (FTC)—at that point "the largest civil penalty in the agency's history."[40]

of cybersecurity either directly or indirectly, but there is no overarching framework legislation in place.").

32. *See* 44 U.S.C. § 3542(b)(1) (2012) (defining "information security" as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction").

33. *E.g.*, Alex Stark, *Review—Cybersecurity and Cyberwar*, E-INTERNATIONAL REL. (Jan. 6, 2014), http://www.e-ir.info/2014/01/06/review-cybersecurity-and-cyberwar/ (reviewing P.W. Singer & Allan Friedman, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW (2014)).

34. *See generally* FIN. INDUS. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES (2015).

35. Bell v. Mich. Council 25 of the Am. Fed'n of State, Cnty., & Mun. Emps., No. 246684, 2005 WL 356306, at *5 (Mich. Ct. App. Feb. 15, 2005).

36. *ACH Liability Up for Grabs as Court Finds against Bank in Second US Cyber-Heist Suit*, FINEXTRA (June 17, 2011), http://www.finextra.com/news/fullstory.aspx?newsitemid=22674.

37. DAVID H. HOLTZMAN, PRIVACY LOST: HOW TECHNOLOGY IS ENDANGERING YOUR PRIVACY 112 (2006) (quoting Dan Christensen, *Major Information Brokers Face Class Action for Invasion of Privacy*, LAW.COM, June 24, 2003, http://www.law.com/jsp/article.jsp?id=1056139884864&slreturn=1 (on file with author)).

38. *Id.*; 18 U.S.C. § 2724(a) (2000).

39. K.C. Jones, *Bank to Pay $50 Million for Buying Personal Data*, INFORMATIONWEEK (Aug. 29, 2006), http://www.informationweek.com/bank-to-pay-50-million-for-buying-person/192500171.

40. Gary Rivlin, *Keeping Your Enemies Close*, N.Y. TIMES, Nov. 12, 2006, http://www.nytimes.com/2006/11/12/business/yourmoney/12choice.html?_r=1. Likewise, in a similar instance the personal information of more than 540,000 New Yorkers was compromised when sensitive computer hardware went missing from a supposedly secure facility. *See*, *e.g.*, *540,000 New Yorkers at Risk of Identity Theft*, NBC NEWS

In all, [BD4]hundreds of millions of personal records have been exposed in thousands of incidents.[41] A single incident in 2006 involving the theft of a laptop owned by the Veterans Administration led to the loss of 26 million social security numbers of retired and active duty military personnel,[42] resulting in a class action lawsuit claiming more than $26.5 billion in damages.[43] Yet litigation is by no means universally successful. In late 2012, for example, a federal judge dismissed a case against Sony resulting from its massive data breach on the grounds that its users signed a privacy policy that contained "clear admonitory language that Sony's security was not 'perfect,'" and, therefore, "no reasonable consumer could have been deceived."[44]

Other courts have considered whether victims of identity theft may bring a claim against financial institutions that have carelessly handled their personal information, sometimes arriving at contradictory rulings.[45] Still other decisions have recognized a broad tort duty of confidentiality, which suggests that banks and other protectors of private information have a fundamental duty to keep their customers' personal information secure and confidential.[46] Some scholars are getting creative, advocating for an independent tort of "negligent enablement of cybercrime" based on principles of premises liability (requiring that landowners who open their land to the public must use reasonable care in ensuring safety for their guests), product liability (holding producers liable for defective products), and warranty.[47] Such a tort is meant to get around mass-market license agreements (the "accept" checkbox), which typically include liability waivers for negligent software design, and could help protect consumers against breaches caused by foreseeable software flaws, shifting the burden to the party best able to evaluate cybersecurity.[48] Other lawsuits have been

(July 24, 2006), http://www.msnbc.msn.com/id/14015598/ns/technology_and_science-security/t/new-yorkers-risk-identity. CS Stars, a Chicago-based insurance broker, was responsible for the system, which was ultimately recovered by the FBI. *Computer Holding Personal Data Found*, NBC NEWS (July 26, 2006), http://www.nbcnews.com/id/14047484/ns/technology_and_science-security/t/computer-holding-personal-data-found/#.VQ7r52TF_38.

41. *See*, *e.g.*, *Chronology of Data Breaches: Security Breaches 2005–Present*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach (last updated Dec. 31, 2013) (chronicling record breaches, with a running total approaching one billion total breaches).

42. Joris Evers, *Veterans Affairs Faulted in Data Theft*, ZDNET (July 12, 2006), http://www.zdnet.com/news/veterans-affairs-faulted-in-data-theft/148782.

43. Cindy Waxer, *The Hidden Cost of IT Security*, NETWORK SECURITY J. (Apr. 16, 2006), http://www.networksecurityjournal.com/features/hidden-cost-of-IT-security-041607/ (discussing the rise of IT costs in an attempt to avoid increasingly high financial damages from security breaches).

44. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 968 (S.D. Cal. 2012); *cf.* Schnall v. The Hertz Corp., 78 Cal. App. 4th 1144, 1163–69 (2000) (finding disclaimers do not give notice to the reasonable consumer when they are incomprehensible and needlessly complex).

45. *See*, *e.g.*, Brandon McKelvey, Comment, *Financial Institutions' Duty of Confidentiality to Keep Customer's Personal Information Secure from the Threat of Identity Theft*, 34 U.C. DAVIS L. REV. 1077, 1095–110 (2001) (describing consumers' reliance on causes of action against financial institutions for their failure to protect consumer information and indicating that courts do not universally recognize the causes of action).

46. *E.g.*, Peterson v. Idaho First Nat'l Bank, 367 P.2d 284, 290 (Idaho 1961) (holding that it is implicit in contracts between banks and consumers that banks have a duty to refrain from disclosing consumers' financial information).

47. *E.g.*, Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1607–10 (2005).

48. *See id.* at 1610–11 (suggesting that the tort of negligent enablement will protect software users by

brought under the theory of "negligent enablement of imposter fraud."[49] However, these have so far been unsuccessful because of an absence of the duty element required in a negligence suit.[50]

This Part builds from the foregoing discussion by assessing how common and statutory law are shaping a standard of cybersecurity care before considering what impact the NIST Framework might have on this regime. The Part begins by analyzing whether a standard of care might now be emerging in negligence cases. Then, it assesses the applicability of fiduciary duties. Finally, this Part considers some of the applicable statutory schemes related to critical infrastructure protection. Throughout, we argue that, at best, a cybersecurity standard of care in the U.S. context should be considered to be incomplete and immature, opening the door for the NIST Framework to have considerable impact on establishing such a standard.

A. Determining a Standard of Cybersecurity Care in Negligence Liability

Negligence, put simply, is conduct that "falls below the standard established by law for the protection of others against unreasonable risk of harm."[51] Avoiding liability for negligence generally requires conforming to a standard of conduct equivalent to that of another that would be considered "reasonable . . . under like circumstances."[52] A legislature or the courts may define this standard of conduct.[53] In all contexts, including cybersecurity, negligence might apply both to an action or omission—that is, failure to act when a duty was owed to do so.[54] In cybersecurity law, there is no explicit or overt "cybersecurity negligence" framework,[55] although attempts have been made to categorize cybersecurity negligence cases that highlight how each of the four negligence prongs have been met,[56] perhaps demonstrating that a standard may be slowly emerging.

The standard of care in negligence is not static but rather evolves over time along with technological advancements. A commonly utilized approach to

holding software producers, who currently waive their responsibility in "anti-warranty" licensing agreements, responsible for damages caused by software failures).

49. *E.g.*, Huggins v. Citibank, N.A., 585 S.E.2d 275, 276 (S.C. 2003).

50. *E.g.*, *id.* at 277; *see also* Chris Jay Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors*, *in* SECURING PRIVACY IN THE INTERNET AGE 207, 213–14 (Anupam Chander et al. eds., 2008) (describing the court's decision in *Huggins v. Citibank, N.A.*). Portions of this research first appeared in Scott J. Shackelford, *Should Your Firm Invest in Cyber Risk Insurance?*, 55 BUS. HORIZONS 349 (2012).

51. RESTATEMENT (SECOND) OF TORTS § 282 (1965).

52. *Id.* § 283.

53. *Id.* § 285.

54. *Id.* § 284.

55. *See supra* notes 22–28 and accompanying text.

56. *See* Picanso, *supra* note 23, at 376 (breaking down state-level cases by each negligence prong, examining findings of "liability for damages resulting from inadequate data security measures and obstacles to recovery"). These prongs include: duty of care and breach, *see*, *e.g.*, Bell v. Mich. Council 25 of the Am. Fed'n of State, Cnty., & Mun. Emps., No. 246684, 2005 WL 356306, at *1–2 (Mich. Ct. App. Feb. 15, 2005) (noting how to find the "special relationship" required to establish a duty); Remsberg v. Docusearch, Inc., 816 A.2d 1001, 1008 (N.H. 2003) ("[T]he risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client."), and causation and injury, *e.g.*, Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, WL 2465906, at *5 (D. Ariz. Sept. 6, 2005).

determining negligence has been the "risk/utility formula" famously articulated by Judge Learned Hand of the Second Circuit Court of Appeals.[57] Suggestions of the formula's use appeared in 1932, when a group of tugboats were hit by a storm and sank, resulting in the loss of its cargos of coal.[58] In the resulting lawsuit, the plaintiffs argued that the tug vessels were "unseaworthy" because they did not have radio receiving sets, which would have warned the tugboats of the storm and prevented the loss of the barges and cargo.[59] The tugboat companies defended themselves on the basis that they were following the prevailing standard practice of the industry: Radio receivers were expensive to purchase and maintain, so they were not typically found in tugboats. Therefore, the companies should not be liable.[60] However, Judge Learned Hand broke new ground, writing that even though having radios aboard was not yet an established industry custom, "[c]ourts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission."[61]

Judge Hand would be faced with a similar opportunity to articulate what should be required in *United States v. Carroll Towing Co.*[62] In this case, Judge Hand devised a formula for determining negligence, focusing on three primary elements: "(1) The probability that [injury will occur]; (2) the gravity of the resulting injury, if [it occurs]; and (3) the burden of adequate precautions."[63] Thus, "liability depends upon whether B [the burden of adequate precautions] is less than L [the gravity of the injury] multiplied by P [the probability of the harm]"—articulated in the algebraic formula $B < P*L$.[64] Though cybersecurity negligence case law is still in its infancy, a number of scholars have looked to Judge Hand's "risk/utility formula" as a means of determining liability for companies who suffer damage from lax cybersecurity.[65]

An open question extending from this case law, then, is whether judges should exercise similar discretion in requiring companies to better manage cyber attacks by boasting a given set of cybersecurity best practices. For example, firewalls and anti-virus software regularly rank as the security technologies most often used in cybersecurity surveys, but few companies regularly update such software.[66] After

57. *See*, *e.g.*, David G. Owen, *The Graying of Products Liability Law: Paths Taken and Untaken in the New* Restatement, 61 TENN. L. REV. 1241, 1251–52 (1994) (indicating that courts have often applied the risk-utility approach, which Learned Hand made famous, to determining negligence).

58. The T.J. Hooper (*In re* E. Transp. Co.) v. H. N. Hartwell & Son, Inc., 60 F.2d 737, 737 (2d Cir. 1932).

59. *Id.*

60. *Id.* at 740.

61. *Id.*

62. United States v. Carroll Towing Co., 159 F.2d 169 (2d Cir. 1947).

63. *Id.* at 173.

64. *Id.*

65. *E.g.*, Michael L. Rustad & Thomas H. Koenig, *Extending Learned Hand's Negligence Formula to Information Security Breaches*, 3 I/S J.L & POL'Y FOR INFO. SOC'Y 237, 244–53 (2007) [hereinafter Rustad & Koenig, *Extending Hand's Formula*] (explaining how Learned Hand's formula can be applied to cybersecurity); Robert Carolina, *The Reasonable Person in Cyber Security: When Did We Become Negligent?*, YOUTUBE (Feb. 24, 2014), http://www.youtube.com/watch?v=Di9aWQ4M8dk (explaining the reasonable person standard in cybersecurity).

66. *See, e.g.*, WADE BAKER ET AL., 2011 DATA BREACH INVESTIGATIONS REPORT 62–64 (2011), *available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf (showing inconsistent rates of using and updating firewalls and anti-virus software).

that, percentages drop off. Roughly 65% of companies used encryption for data in transit according to 2011 surveys conducted by Computer Science Institute and Verizon.[67] About half use intrusion prevention systems and encryption for data in storage, while approximately one-third use public-key encryption, specialized wireless security systems, or content-monitoring systems to prevent data loss.[68] However, these fractions are constantly changing,[69] which raises questions: For example, would a judge be justified in finding a firm negligent that suffered a data breach due to firewalls or spyware that had not been updated, even if many companies do not regularly update? What about not encrypting data at rest and in transit, or failing to do regular penetration testing?

Though the risk/utility formula has yet to be fully analyzed by a court within a cybersecurity context, courts have addressed what constitutes reasonable standards of cybersecuirty care through alternative rationales with varying outcomes. Some courts, for example, have looked to established practices to determine whether a trier of fact should be allowed to determine negligence; however, this approach is by no means consistent. Consider Sony, which in May 2011 was attacked with hackers reportedly compromising more than 100 million gamers' names, addresses, emails, user names, and passwords.[70]

In the ongoing case, *In re Sony Gaming Networks and Customer Data Security Breach Litigation*,[71] the court suggested that Sony's failure to employ industry cryptology standards was enough for plaintiffs to allege that Sony breached its duty to employ reasonable data security measures.[72] In their complaint, victims of the hack alleged that Sony had a duty "to design, implement, maintain, and test Sony's security system in order to ensure Plaintiffs' Personal Information was adequately secured and protected" and that "Sony breached this duty by failing to implement proper procedures to protect Plaintiffs' Personal Information."[73] Sony contested, arguing, among other things, that it had no legal duty to provide reasonable security.[74] Based on California and Massachusetts law,[75] the court in this case agreed with the plaintiffs, finding,

67. *Id.*

68. *Id.*

69. *See id.* at 63 (demonstrating the constantly changing number of companies using security technologies).

70. Ian Sherr & Amy Schatz, *Sony Deails Hacker Attack*, WALL ST. J., May 5, 2011, http://online.wsj.com/article/SB10001424052748703849204576302970153688918.html; Hayley Tsukayama, *Cyber Attack Was Large-Scale, Sony Says*, WASH. POST, May 4, 2011, http://www.washingtonpost.com/ blogs/faster-forward/post/cyber-attack-was-large-scale-sony-says/2011/05/04/AF78yDpF_blog.html; Nick Bilton, *Sony Explains PlayStation Attack to Congress*, N.Y. TIMES BITS BLOG (May 4, 2011), http://bits.blogs.nytimes.com/2011/05/04/sony-responds-to-lawmakers-citing-large-scale-cyberattack/.

71. *In re* Sony Gaming Networks and Consumer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014).

72. *Id.* at 966.

73. *Id.*

74. *Id.*

75. The complaint asserted negligence claims under California law, Florida law, Massachusetts law, Missouri law, and Ohio law. *Id.* at 963. The Florida, Missouri, and Ohio negligence claims' allegations of causation and harm, however, were "wholly conclusory, and therefore fail[ed] to put the Court or Sony on notice of the specific relief requested." *Id.* The court addressed the California and Massachusetts negligence claims separately.

> [B]ecause Plaintiffs allege that they provided their Personal Information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect their Personal Information, including the utilization of industry-standard encryption, the Court finds Plaintiffs have sufficiently alleged a legal duty and a corresponding breach.[76]

Beyond particular technologies, other courts have placed considerable weight on industry report recommendations, which may be considered similar to the NIST Framework, in determining whether a reasonable level of data security had been provided by an entity.[77] For instance, in *Shames–Yeakel v. Citizens Financial Bank*, the U.S. District Court for the Northern District of Illinois found that Citizens' failure to comply with security measures recommended in a report by the Federal Financial Institutions Examination Council (FFIEC) was enough to establish a triable issue of fact as to whether Citizens breached its duty of care.[78] Marsha Shames–Yeakel was the owner of a bookkeeping company, "Best Practices," which had a business checking account with Citizens Financial Bank.[79] According to the court, an "unknown person" gained access to Shames–Yeakel's credentials, stealing upwards of $26,500 on Shames–Yeakel's home equity credit line.[80] Shames–Yeakel argued that Citizens' online banking security "lagged behind industry standards,"[81] as Citizens Financial Bank only used "single-factor identification" as opposed to "multifactor identification."[82] Specifically, Shames–Yeakel cited the FFIEC's Report, Authentication in an Internet Banking Environment,[83] which "does not endorse any particular technology" but states that "agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties."[84] Citizens filed a motion for summary judgment, arguing, in part, that though it had a duty to protect its customer data, Shames–Yeakel had not produced sufficient evidence that Citizens had breached its duty of care.[85] The court denied Citizens' motion for summary judgment as to Shames–Yeakel's negligence claim.[86] While an expert retained by Citizens found the bank's use of single-factor

76. *Id.* *But see supra* note 44 and accompanying text.

77. *Cf.* Willingham v. Global Payment Inc., No. 1:12-CV-01157-RWS, 2013 WL 440702, at *19 (N.D. Ga. Feb. 5, 2013) (reflecting an alternative view in which courts are reluctant to rely on data security standards as a means of determining whether a duty was owed, let alone whether they should be used to determine reasonable standards of care).

78. 677 F. Supp. 2d 994, 1008–09 (N.D. Ill. 2009).

79. *Id.* at 997.

80. *Id.* at 998.

81. *Id.* at 1000.

82. *Id.* at 1000–01. Single-factor identification is the use of one authentication factor to satisfy validation (such as a "knowledge" factor like the use of a username and password). Multi-factor identification requires more than one authentication factor. *Cf. Azure Multi-factor Authentication*, MICROSOFT AZURE, http://azure.microsoft.com/en-us/services/multi-factor-authentication/ (last visited Mar. 23, 2015) (providing information on the benefits of multi-factor authentication services).

83. FED. FIN. INSTS. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT (2005), *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf.

84. *Id.* at 1; *accord Shames–Yeakel*, 677 F. Supp. 2d at 1001.

85. *Shames–Yeakel*, 677 F. Supp. 2d at 1008.

86. *Id.* at 1009.

authentication to be "reasonable," the court stated that Citizens' "delay" in complying with FFIEC security standards could lead "a reasonable finder of fact [to] conclude that the bank breached its duty to protect Plaintiffs' account against fraudulent access."[87]

The lacking judicial analysis of what constitutes reasonable standards of cybersecurity care stems in part from the numerous barriers that exist to pursuing tort claims related to cyber attacks. For example, Article III standing has been problematic in many negligent data security cases, as establishing the required "injury-in-fact" and "causation" can prove difficult.[88] Additionally, data breaches that "merely" result in pure economic losses have also prevented negligence cases from proceeding.[89] This "economic loss doctrine" holds that plaintiffs must suffer physical damage (either to the person or the person's property) beyond mere economic losses in order to establish injury under negligence.[90] Because most injuries resulting from a lack of data security are purely economic—such as fraudulent charges on a user's account—defendants have successfully avoided negligence liability by using the economic loss doctrine.[91] These alternative defenses, in turn, have often prevented in-depth judicial analysis on the standard of care issue in cybersecurity negligence cases, leading to a consideration of alternative doctrines—including fiduciary duties.

B. A Note on Leveraging Fiduciary Duties to Enhance Corporate Cybersecurity

In addition to suits for negligence, corporate officers and directors also may have liability stemming from their fiduciary duties to shareholders in the aftermath of a cyber attack.[92] Historically, the two types of fiduciary duties that apply to

87. *Id.*

88. *See*, *e.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (holding that plaintiff failed to state actual or impending injury under Article III "because she does not identify any incident in which her data has ever been accessed by an unauthorized person"); Reilly v. Ceridian Corp., 664 F.3d 38, 42, 44 (3d Cir. 2011) (finding no "actual or imminent" injury where "no identifiable taking occurred" and "all that [was] known [was] that a firewall was penetrated"). *But see*, *e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding injury in fact under Article III "[b]ecause the plaintiffs had alleged an act that increased their risk of future harm" after theft of a laptop containing personal data).

89. *See*, *e.g.*, Annett Holdings, Inc. v. Kum & Go, L.C., 801 N.W.2d 499, 503 (Iowa 2011) ("As a general proposition, the economic loss rule bars recovery in negligence when the plaintiff has suffered only economic loss.").

90. Ralph C. Anzivino, *The Economic Loss Doctrine: Distinguishing Economic Loss from Non-Economic Loss*, 91 MARQ. L. REV. 1081, 1082 (2008).

91. *E.g.*, *In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 498–99 (1st Cir. 2009); *In Re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 530–31 (N.D. Ill. 2011) ("Notably, other courts dealing with data breach cases have also held that the economic loss doctrine bars the plaintiff's tort claim because the plaintiff has not suffered personal injury or property damage."). *But see* Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc. 729 F.3d 421, 423–27 (5th Cir. 2013) (holding that the economic loss doctrine, under certain circumstances, did not bar plaintiff's negligence claim for allegedly unreasonable data security practices by defendant). However, in such situations, liability for purely economic losses may be sought under contract law. Anzivino, *supra* note 90, at 1081.

92. *See* Joseph P. McMenamin, *Pandemic Influenza: Is There a Corporate Duty to Prepare?*, 64 FOOD & DRUG L.J. 69, 85 (2009) ("Some courts considering derivative suits appear to be prepared in some instances to hold corporate directors to a simple negligence standard, which may expose directors to liability for failure to take reasonable, cost-effective steps to protect the company's interests.").

corporate officers and directors have been: (1) duty of loyalty; and (2) duty of care.[93] Directors have long enjoyed a great deal of discretion that immunizes them from many lawsuits alleging a breach of their fiduciary duties under a rule known as the "business judgment rule," which is a presumption that directors are acting in the best interests of the company.[94] However, this presumption has gradually become less of a silver bullet.[95] For example, some courts have extended the duty of care to encompass "a duty of oversight requiring directors and officers to act affirmatively to assure that adequate information and compliance systems are in place."[96] This puts the onus to make proactive investments in cybersecurity best practices squarely on directors that have perhaps grown accustomed to the benefits of immunity stemming from the business judgment rule.

Fiduciary duties thus may be relevant to managing cyber attacks and shaping a cybersecurity duty of care.[97] Related to the burgeoning duty of oversight, liability may be found on the basis of a lack of good faith under the duty of loyalty if "(a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[98] These standards speak to the importance of effective organization in managing the cyber threat. Yet many firms are still not making necessary organizational changes. When Sony was hacked in early 2011, it famously did not have a chief information security officer (CISO) or senior manager devoted wholly to information security.[99] It was not alone. In 2006, only 43% of respondents to a PricewaterhouseCoopers (PwC) survey said that they had a CISO or other similar security executive, though by 2009, that rate had increased to 85%.[100] This increase may in part be explained by the fact that companies with CISOs have been shown to save more than 20% on data breach costs over those that do not, according to one Symantec survey.[101]

93. Julian Velasco, *How Many Fiduciary Duties Are There in Corporate Law?*, 83 S. CAL. L. REV. 1231, 1232–33 (2010).

94. McMenamin, *supra* note 92, at 86–87.

95. *See id.* at 92 ("[E]xtensive factual analysis of corporate directors' business decisions suggest that courts may be growing increasingly willing to review in detail the substance, rather than merely the procedure, of business decisions. This change in application of the business judgment rule means that the overall defense may be weaker and more unpredictable than in the past." (footnote omitted)).

96. Bob Uda, *A Duty of Care in Cyberspace*, ICCTF (Mar. 3, 2011), http://www.icttf.org/blogs/927/42/a-duty-of-care-in-cyberspace (emphasis omitted).

97. *Cf.* J. Wylie Donald & Jennifer Black Strutt, *Cybersecurity: Moving Toward a Standard of Care for the Board*, BLOOMBERG L. (Nov. 4, 2013), http://about.bloomberglaw.com/practitioner-contributions/cybersecurity-moving-toward-a-standard-of-care-for-the-board/ (discussing how the fiduciary duties could affect board of directors in the cybersecurity context).

98. *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 123 (Del. Ch. 2009) (quoting Stone *ex rel.* AmSouth Bancorporation v. Ritter, 911 A.2d 362, 370 (Del. 2006)).

99. Dave Aitel, *Top Hacker Disasters of 2011: Five Critical Lessons for Businesses*, FOX BUS. (Dec. 5, 2011), http://www.foxbusiness.com/economy/2011/12/05/top-hacker-disasters-2011-five-critical-lessons-for-businesses.

100. Ralph DeFrangesco, *Chief Information Security Officer: A New Spin on an Old Job*, IT BUS. EDGE (Nov. 2, 2009), http://www.itbusinessedge.com/cm/blogs/defrangesco/chief-information-security-officer-a-new-spin-on-an-old-job/?cs=37172.

101. PONEMON INST., 2010 ANNUAL STUDY: U.S. COST OF A DATA BREACH 32 (2011), *available at* http://www.fbiic.gov/public/2011/mar/2010_Annual_Study_Data_Breach.pdf.

Shareholder lawsuits against companies and their executives for lax security measures have started to make headlines as well. In December 2013, Target disclosed that it was aware that hackers had gained "unauthorized access" to customer payment card data.[102] Later estimates would suggest that the breach affected some 70 million Target customers, one of the largest data breaches of a retail store in history.[103] Following disclosure of the breach, at least two shareholders have filed shareholder derivate lawsuits, alleging, among other claims, breach of fiduciary duty against dozens of Target executives.[104] One of the shareholders complaints claims that "[i]n violation of its express promise to do so, and contrary to reasonable customer expectations, Target failed to take reasonable steps to maintain its customers' personal and financial information in a secure manner."[105]

Executives at the hotelier Wyndham Worldwide Corporation are also at the center of a shareholder derivative lawsuit. The lawsuit alleges that Russian-based hackers were able to gain unauthorized access to Wyndham's corporate databases on three separate occasions, stealing the consumer information of more than 600.000 customers.[106] Similar to the Target complaint, shareholders claim that the Wyndham executives failed to take reasonable steps to maintain their customers' personal and financial information.[107] However, a federal judge dismissed the lawsuit with prejudice in October 2014. It will be some time before we know if similarly situated derivative lawsuits based on cybersecurity incidents, such as the Target lawsuit, will result in a similar outcome. Yet, as with negligence, the role of common law fiduciary duties in shaping a standard of cybersecurity care should not be ignored. Neither should the role of cybersecurity statutes relevant to safeguarding critical infrastructure, the topic we turn to next.

C. U.S. Statutory Law and Regulatory Requirements for Critical Infrastructure Cybersecurity

In addition to leveraging common law—including negligence and fiduciary duties—to help establish a standard of cybersecurity care, numerous state and federal statutes are also applicable. It is beyond the scope of this Article, though, to review all of these statutory regimes. Numerous secondary sources have ably done

102. Press Release, Target Corp., Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores (Dec. 19, 2013), http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores.

103. *See* 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://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html (describing the Target data breach as one of the worst ever).

104. Verified Shareholder Derivative Complaint, Collier v. Steinhafel (D. Minn. Jan. 29, 2014) (No. 0:2014cv00266), *available at* http://www.dandodiary.com/wp-content/uploads/sites/265/2014/02/targetsuit1.pdf; Verified Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets, Kulla v. Steinhafel (D. Minn. Jan. 21, 2014) (No. 0:14–cv–00203–SRN–JSM) [hereinafter Kulla], *available at* http://www.dandodiary.com/wp-content/uploads/sites/265/2014/02/firsttargetcomplaint.pdf.

105. Kulla, *supra* note 104, para. 3.

106. Verified Shareholder Derivative Complaint for Breach of Fiduciary Duty, Waste of Corporate Assets, and Unjust Enrichment, Palkon v. Holmes, para. 74, No. 2:14–cv–O1234–SRC–CLW (D.N.J. May 2, 2014) (redacted copy), *available at* http://www.dandodiary.com/wp-content/uploads/sites/265/2014/05/palcon1.pdf.

107. *Id.* para. 3.

this already.[108] However, it is worth summarizing several of the most applicable statutes and regulations related to establishing and shaping a cybersecurity standard of care for critical infrastructure organizations. This Subpart does so by analyzing select statutory and regulatory requirements associated with the case studies of finance, chemical, healthcare, and energy, facilities. Subsequently, state data breach statutes and their reasonable data security requirements are also considered. As this Subpart demonstrates, rather than establishing explicit best practices, these legal requirements rely heavily on company implementation of broader reasonable and appropriate security measures.

1. Financial Sector: Gramm-Leach-Bliley Act Safeguard Rules

While its information practices are governed by a variety of statues, regulations, and best practices, the financial sector's most significant data security regulations derive in part from the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA).[109] The GLBA was enacted, in part, to provide "a prudential framework for the affiliation of banks, securities firms, . . . and other financial service providers."[110] Under the GLBA, "financial institutions"[111] are required to "protect the security and confidentiality of those customers' nonpublic personal information."[112] Specifically, authorized agencies are required to establish appropriate administrative, technical, and physical safeguards for financial institutions:

> (1) [T]o insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[113]

Numerous agencies, including the FTC and the Securities and Exchange Commission (SEC), have since established certain rules and regulations to maintain

108. *E.g.*, FISCHER, *supra* note 21, at 52–61 (listing various federal laws identified as being related to cybersecurity).

109. Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

110. *Id.* pmbl.

111. A "financial institution" is broadly defined as any institution that is engaging in activities that are financial in nature. *See* 15 U.S.C. § 6809(3)(A) (2012) ("The term 'financial institution' means any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12."); 12 U.S.C. § 1843(k) (setting forth a number of activities which are financial in nature).

112. 15 U.S.C. § 6801(a); *see also* Guin v. Brazos Higher Educ. Serv., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *3–4 (D. Minn. Feb. 7, 2006) (stating that "[i]n some negligence cases [] a duty of care may be established by statute," and applying the Gramm-Leach-Bliley Act (GLBA) to establish the duty of care, but holding that there was not a breach of that duty in the case).

113. 15 U.S.C. § 6801(b).

and enforce data security safeguards. For instance, the FTC's "Safeguard Rule" requires covered financial institutions to "develop, implement, and maintain a comprehensive information security program that . . . contains administrative, technical, and physical safeguards that are appropriate to [an organization's] size and complexity, the nature and scope of [an organization's] activities, and the sensitivity of any customer information at issue."[114] This program must be "reasonably designed to achieve the objectives" of the GLBA.[115] The FTC Safeguard Rule additionally calls for the program to (1) designate an employee to coordinate the program; (2) "identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information"; (3) design safeguards to control the identified risks; (4) oversee financial service providers; and (5) provide continuous oversight for the program.[116] Financial entities under the authority of the SEC must follow similar safeguard standards. Under the SEC Safeguard Procedures, "[e]very broker, dealer, and investment company, and every investment adviser registered with the Commission" must adopt procedures "that address administrative, technical, and physical safeguards for the protection of customer records and information."[117]

2. Chemical Sector: Chemical Facility Anti-Terrorism Standards Regulation

In 2007, the U.S. Department of Homeland Security (DHS) promulgated the Final Rule of the Chemical Facility Anti-Terrorism Standards (CFATS).[118] These regulations are intended to "to enhance the security of our Nation by furthering the mission of the Department as provided in 6 U.S.C. §111(b)(1) and by lowering the risk posed by certain chemical facilities."[119] The CFATS requires certain high-risk chemical facilities to prepare "Security Vulnerability Assessment[s]" that "identify facility security vulnerabilities,"[120] and to implement "Site Security Plans" that

114. 16 C.F.R. § 314.3(a) (2014).

115. *Id*.

116. *Id.* § 314.4.

117. 17 C.F.R. § 248.30(a) (2009); *see also In re* J.P. Turner & Co., Exchange Act Release No. 3-13550, 98 SEC Docket 1729, 1741 (ALJ May 19, 2010) (initial decision) (ordering that J.P. Turner & Company cease committing violations of Rule 30(a)).

118. 6 C.F.R. § 27 (2007).

119. *Id.* § 27.100. "Chemical Facility" is defined within the Chemical Facility Anti-Terrorism Standards as

> any establishment that possesses or plans to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criteria identified by the Department. As used herein, the term chemical facility or facility shall also refer to the owner or operator of the chemical facility. Where multiple owners and/or operators function within a common infrastructure or within a single fenced area, the Assistant Secretary may determine that such owners and/or operators constitute a single chemical facility or multiple chemical facilities depending on the circumstances.

Id. § 27.105.

120. *Chemical Facility Anti-Terrorism Standards (CFATS)*, DEP'T HOMELAND SEC., http://www.dhs.gov/chemical-facility-anti-terrorism-standards (last updated Feb. 25, 2015); *accord* 6 C.F.R. § 27.215.

"include measures that satisfy the identified risk-based performance standards."[121] These Site Security Plans must include "appropriately risk-based measures," including efforts to "deter cyber sabotage, including by preventing unauthorized on-site or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems."[122]

Guidance on the application of the CFATS standards are issued by the DHS Assistant Secretary, but "the acceptable layering of measures used to meet these standards will vary by risk-based tier."[123] The DHS, in an effort to assist high-risk facilities in meeting the CFATS requirements, published Risk-Based Performance Standards Guidance.[124] The publication provides examples of risk-based measures to satisfy the cyber standards; however, the publication "does not establish legally enforceable requirements for facilities subject to CFATS" and states that "the specific security measures and practices discussed in this document are neither mandatory nor necessarily the 'preferred solution'" for compliance.[125]

3. Healthcare and Public Health Sector: Health Insurance Portability and Accountability Act's Security Rules

The Health Insurance Portability and Accountability Act (HIPAA) was adopted in 1996,[126] tasking the federal government with, among other requirements, creating security standards to protect "individually identifiable health information" with which various health-care entities are responsible for complying.[127] More specifically, HIPAA authorized the Department of Health and Human Services to adopt "national standards that protect the confidentiality and integrity of electronic protected health information," or "ePHI."[128] These national standards, published in 2003, have been referred to as the "HIPAA Security Rule."[129] Under the Security Rule, covered entities "must assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected."[130] HIPAA violations, including failing to comply with the standards or wrongfully disclosing personal information, may result in civil or

121. *Chemical Facility Anti-Terrorism Standards (CFATS)*, *supra* note 120.

122. 6 C.F.R. § 27.230(a)(8).

123. *Id.* § 27.230(a).

124. DEP'T OF HOMELAND SEC., RISK-BASED PERFORMANCE STANDARDS GUIDANCE: CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (2009), *available at* http://www.dhs.gov/xlibrary/assets/chemsec_cfats _riskbased_performance_standards.pdf.

125. *Id.* at 7.

126. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat 1936 (codified as amended at scattered sections of 18, 26, 29, and 42 U.S.C.).

127. FISCHER, *supra* note 21, at 58.

128. Jennifer Griffin & David Elliott, *HIPAA Security Rule Compliance Reviews on the Horizon*, 76 DEF. COUNSEL J. 261, 262 (2009).

129. *The Security Rule*, DEP'T OF HEALTH & HUMAN SERV., www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/ (last visited Mar. 25, 2015).

130. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8334 (Feb. 20, 2003). It should be noted that the Health Insurance Portability and Accountability Act (HIPAA) Security Rule does go into further detail about the cybersecurity requirements of covered entities than several other surveyed statutes.

criminal penalties;[131] the extent to which a private cause of action may exist under HIPAA is less clear.[132]

4. Energy Sector: North American Electric Reliability Corporation Standards

The North American Electric Reliability Corporation (NERC) is an international nonprofit regulatory body based in Atlanta, Georgia.[133] Under the Energy Policy Act of 2005, NERC is authorized to set mandatory standards in the operation of U.S. power systems, subject to financial penalties in the event of non-compliance.[134] The NERC "Reliability Standards" include nine critical infrastructure protection standards that mandate a variety of cybersecurity reporting, security identification, security implementation, and recovery requirements that are overseen by the Federal Energy Regulatory Commission (FERC).[135] The standards fit into a framework of protection, deterrence, prevention, limiting, and recovery.[136] Thus, in lieu of any actual overarching cybersecurity legislation, the authority given by Congress to the FERC stands in as a mechanism for creating mandatory cybersecurity standards in the critical infrastructure sphere.[137] The NERC also serves as a model of bottom-up governance in the form of industry best practices that were eventually sanctioned by the U.S. government after the 2003 northeast blackout.[138] Whether a similar pattern emerges regarding the NIST Framework remains to be seen.

5. State Data Security Regulations

In addition to federal regulatory requirements, state laws that call for "reasonable" security measures for certain types of personal information may also provide an opportunity for the NIST Framework to play a part in shaping what constitutes reasonable standards of cybersecurity care. Between 2002 and April

131. 42 U.S.C. § 1320d-5 (2012).

132. *See* Cory J. Fox, *HIPAA Violation Results in $1.44M Jury Verdict against Walgreens, Pharmacist*, BAKERHOSTETLER (Aug. 22, 2013), http://www.bakerlaw.com/health-law-update-august-22-2013#HIPAA ("Although HIPAA does not create a private cause of action, a recent Indiana Superior Court jury verdict demonstrates that HIPAA still could play an important role in private causes of action in state court based on negligence and professional liability . . . .").

133. *About NERC*, N. AM. ELECTRIC RELIABILITY CORP., http://www.nerc.com/AboutNERC/Pages/default.aspx (last visited Mar. 25, 2015).

134. *See* 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, 665 n.33 (2014) (discussing NERC's authority to establish and enforce mandatory reliability standards).

135. *CIP Compliance*, N. AM. ELECTRIC RELIABILITY CORP., http://www.nerc.com/pa/CI/Comp/Pages/default.aspx (last visited Mar. 25, 2015).

136. *Critical Infrastructure Protection Committee (CIPC)*, N. AM. ELECTRIC RELIABILITY CORP., http://www.nerc.com/comm/CIPC/Pages/default.aspx (last visited Mar. 25, 2015).

137. *See* Trope & Humes, *supra* note 134, at 665 n.33 (discussing the authority and the role of the Federal Energy Regulation Commission (FERC)).

138. *See* INTELLIGENCE & NAT'L SEC. ALLIANCE, ADDRESSING CYBER SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIP: AN ANALYSIS OF EXISTING MODELS 7 (2009), *available at* http://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx (describing the North American Electric Reliability Corporation origins as a voluntary standards setter that eventually was adopted by the FERC).

2014, 47 States passed data breach notification requirements, in some instances mandating government or private sector entities to provide notice to those whose "personally identifiable information" is lost.[139] Variations among States create a complex and sometimes contradictory regulatory environment for firms operating across jurisdictions;[140] for example, a handful of states have a "no-harm threshold law," meaning that it does not matter whether lost information was used in a way that harmed consumers or not—the mere fact that there has been a breach requires that notification be given.[141] States also have more-or-less-inclusive lists of personally identifiable information that must be lost for a breach to warrant disclosure.[142] Meanwhile, in the states that do not have any data breach notification laws as of 2014—Alabama, South Dakota, and New Mexico[143]—a company could knowingly have its customers' social security numbers breached but not inform those customers and still be legally compliant under state law.[144] The Obama Administration's mid-2009 Cyberspace Review laid out some proposals to address this issue.[145]

In addition to mandating requirements on entities responding to a data breach, many of these statutes include explicit requirements that covered entities holding certain types of sensitive information are required to implement and maintain "reasonable" security measures.[146] As with state data breach notification requirements, some state data security requirements are much more comprehensive than others. Massachusetts, considered to have one of the most wide-ranging state data security laws, not only requires organizations storing personal information of Massachusetts residents to have a written security plan to secure personal data, but also necessitates that the plan be regularly audited.[147] Others state statutes are more

139. *Security Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES (Jan. 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

140. *See id.* (listing the different breach notifications laws); *see also* Kevin J. O'Brien, *Europe Weighs Requiring Firms to Disclose Data Breaches*, N.Y. TIMES, Jan. 16, 2013, http://www.nytimes.com/2013/01/17/technology/17iht-data17.html (reporting that a proposed EU directive would require EU-wide data breach reporting for all firms that "run large databases, those used for Internet searches, social networks, e-commerce or cloud services").

141. Mike Tsikoudakis, *Patchwork of Data Breach Notification Laws Poses Challenge*, BUS. INS. (June 5, 2011), http://www.businessinsurance.com/apps/pbcs.dll/article?AID=/20110605/ISSUE03/306059998.

142. *See id.* (describing generally the types of state notification laws).

143. *Security Breach Notification Laws*, *supra* note 139.

144. *See* Jacqueline May Tom, *A Simple Compromise: The Need for a Federal Data Breach Notification Law*, 84 ST. JOHN'S L. REV. 1569, 1569–70 (2010) (discussing the effect of breach law on a state's duties).

145. *See* WHITE HOUSE OFFICE OF THE PRESS SEC'Y, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE vi (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [hereinafter CYBERSPACE POLICY REVIEW] (listing ten summary points of a near-term action plan for reforms in U.S. cybersecurity policies).

146. *E.g.*, ARK. CODE ANN. § 4-110-104(b) (2011); CAL. CIV. CODE § 1798.81.5(b) (West Supp. 2015); MD. CODE ANN. COM. LAW § 14-3503(a) (LexisNexis 2013); NEV. REV. STAT. § 603A.210.1 (2013); OR. REV. STAT. § 646A.622(1) (2013); R.I. GEN. LAWS § 11-49.2-2(2) (West 2013); TEX. BUS. & COM. CODE ANN. § 521.052 (West 2015).

147. Bart Lazar, *States Ramp Up Data Security Laws*, PCWORLD (Nov. 9, 2008), http://www.pcworld.com/article/153553/data_security-law.html.

general and do not specifically define what constitutes "reasonable" cybersecurity under the law.[148]

D. Summary

This Part has examined various existing and developing cybersecurity standards and frameworks under common and statutory law at the state and federal levels. As has been shown, there is not yet a comprehensive cybersecurity standard of care crystallizing across sectors, but we do see the beginnings of one with regards to negligence, the duty of oversight, and various statutory schemes to protect critical infrastructure. The situation is ripe for clarification. Whether the NIST Framework is an appropriate vehicle for addressing existing regulatory ambiguity is the subject we turn to next—after introducing its recent evolution and scope.[149]

II. INTRODUCING AND EXAMINING THE NIST CYBERSECURITY FRAMEWORK

Prior to President Obama's 2013 State of the Union Address and Executive Order 13636, efforts to update the regulatory provisions addressing critical infrastructure insecurity had largely stalled. In 2011, for instance, the Obama Administration released for consideration a comprehensive cybersecurity legislative proposal that intended to improve critical infrastructure protection.[150] Portions of the Administration's 2011 proposal had been introduced in both the House and the Senate,[151] but largely to no avail.[152] The Cybersecurity Act of 2012 would have tasked a new National Cybersecurity Counsel to work with private sector critical infrastructure owners and operators to identify critical cyber infrastructure, conduct sector-by-sector cyber risk assessments, and establish a voluntary, outcome-based cybersecurity program for critical infrastructure.[153] However, the bill faced

148. *See* John Black, *Developments in Data Security Breach Liability*, 69 BUS. LAW 199, 206 (2013) ("Although several states have data security laws that require businesses to adopt reasonable security measures to protect personal information . . . those statutes do not define what constitutes reasonable data security."); *see also* Johnson, *Data Security*, *supra* note 23, at 22 (stating that the California Security Breach Information Act "leaves no doubt that businesses owe a duty under California law to protect customers' personal information and that customers may recover damages if businesses breach that duty," yet "makes no attempt to define what constitutes 'reasonable security procedures and practices'").

149. *See* SHACKELFORD, MANAGING CYBER ATTACKS, *supra* note 3, at 244–45 (noting firms' concerns with regulatory intervention in cybersecurity).

150. Letter from Jacob J. Lew, Dir., Office of Mgmt. & Budget, to John Boehner, Speaker, U.S. House of Representatives (May 12, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/ letters/Cybersecurity-letters-to-congress-house-signed.pdf ("The proposal would improve critical infrastructure protection by bolstering public-private partnerships with improved authority for the Federal government to provide voluntary assistance to companies and increase information sharing."); *see also* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, LEGISLATIVE LANGUAGE: LAW ENFORCEMENT PROVISION RELATED TO COMPUTER SECURITY (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf (detailing the legislative language proposed by the Office of Management and Budget to the U.S. Congress).

151. FISCHER, *supra* note 21, at 5.

152. *See*, *e.g.*, *U.S. Senators Push Ahead with Cyber Security Legislation*, *supra* note 8 ("[S]pats over liability and privacy protections have thwarted passage of comprehensive cyber security bills thus far.").

153. Cybersecurity Act of 2012, S. 3414, 112th Cong. § 101 (2012). Senate Bill 3414 is not to be

opposition from the private sector[154] and failed to pass the Senate.[155] The recommendations issued by the House of Representatives House Republicans Cybersecurity Task Force[156] have also failed to result in legislation as of March 2015.[157] This legislative inertia prompted executive action by the Obama Administration.

A. Executive Order 13636 and the Objectives of the NIST Framework

Executive Order 13636, effective in February 2013, intended to balance effective critical infrastructure security measures with the maintenance of a cyber-environment that encourages efficiency, innovation, and economic prosperity.[158] The major directives of the Order included enhancing the scope and efficiency of cybersecurity information sharing programs,[159] assessing and coordinating privacy and civil liberties protections in cybersecurity activities,[160] and implementing a baseline framework and voluntary program to reduce cyber risk to critical infrastructure.[161] The Order itself provided a number of overarching objectives for the Cybersecurity Framework to fulfill. For example, it placed the Director of NIST in charge of developing a voluntary Framework that "include[s] a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[162] The Framework would use cybersecurity best practices, at both a national and international level, in order to provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" that could help critical infrastructure manage cybersecurity risks.[163] The Framework's creators were tasked with developing an approach that could adapt well to future, unknown technologies while also allowing the Framework to be used

confused with Senate Bill 2105, an earlier bill of the same name, which would have tasked the Department of Homeland Security to identify "covered critical infrastructures" sectors and require owners of covered entities to remediate or mitigate identified cyber risks. Cybersecurity Act of 2012, S. 2105, 112th Cong. §§ 101–104 (2012).

154. *See*, *e.g.*, Letter from R. Bruce Josten, Exec. Vice President of Gov't Affairs, Chamber of Commerce, to the Members of the U.S. Senate (July 30, 2012), http://www.uschamber.com/ letter/key-vote-letter-s-3414-cybersecurity-act-2012%E2%80%9D (expressing that "[t]he [U.S. Chamber of Commerce] strongly opposes S. 3414").

155. Eric Engleman, *Cybersecurtity Bill Killed, Paving Way for Executive Order*, BLOOMBERG (Nov. 15, 2012), http://www.bloomberg.com/news/articles/2012-11-15/cybersecurity-bill-killed-paving-way-for-executive-order.

156. *See* HOUSE REPUBLICAN CYBERSECURITY TASK FORCE, 113TH CONG., RECOMMENDATIONS OF THE HOUSE REPUBLICAN CYBERSECURITY TASK FORCE 5 (2011) (providing recommendations on "how House Republicans should approach four issue areas within cybersecurity").

157. However, as of this writing there is movement on various cybersecurity measures hastened by major data breaches, such as Anthem. *See* Andy Greenberg, *Privacy Critics Go 0-2 with Congress Cybersecurity Bills*, WIRED (Mar. 26, 2015), http://www.wired.com/2015/03/privacy-critics-go-0-2-congress-cybersecurity-bills/ (reporting on the most recent bills in the House and Senate, which are expected to reach a vote on each floor by late April).

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

159. *Id.* at 11739–40.

160. *Id.* at 11740.

161. *Id.* at 11740–42.

162. *Id.* at 11741.

163. *Id*.

across industries.[164] The Framework was also intended to mature over time, allowing areas of improvement to be recognized and accounted for in future Framework variations.[165]

Privacy and civil liberties protections are also specifically emphasized within the Framework. The Order called for the Cybersecurity Framework and its associated information security measures to identify, assess, and mitigate the impact that security practices within the Framework may have on business confidentiality, individual privacy, and civil liberties.[166] It also requested agencies to coordinate and ensure that privacy and civil liberties protections are incorporated into all activities mandated by the Order generally. Specifically, "[P]rotections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities."[167]

Executive Order 13636 provided NIST one year to develop the Cybersecurity Framework.[168] To help with this process, NIST held five framework workshops throughout 2013, bringing together a large and diverse contingent of stakeholders, including academics, government officials, and private sector industry members.[169] Meetings were held, webinars were presented, and informal sessions were scheduled to provide feedback throughout the course of the Framework's development.[170]

These efforts resulted in the release of a preliminary draft of the Framework on October 22, 2013,[171] just prior to the fifth workshop, which was held in November 2013.[172] The preliminary Framework would undergo relatively few adjustments before it was released in its final version in early 2014.[173] Among the more significant

164. *See* Exec. Order No. 13636, 78 Fed. Reg. at 11741 ("The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations.").

165. *Id.*

166. *Id.*

167. *Id.* For an understanding of the Fair Information Practice Principles, see generally ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY VERSION 2.13 (2015), *available at* http://www. bobgellman.com/rg-docs/rg-FIPShistory.pdf.

168. Exec. Order No. 13636, 78 Fed. Reg. at 11741.

169. For workshop recordings and slides, see *Cybersecurity Framework—Workshops and Events*, NIST, http://www.nist.gov/cyberframework/cybersecurity-framework-events.cfm (last visited Mar. 31, 2015).

170. For the materials and resources that were produced and circulated throughout the creation of the NIST Cybersecurity Framework, see *Cybersecurity Framework—Archived Documents*, NIST, http://www.nist.gov/cyberframework/cybersecurity-framework-archived-documents.cfm (last updated Feb. 12, 2014).

171. NAT'L INST. OF STANDARDS & TECH., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK (2013), *available at* http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf [hereinafter NIST PRELIMINARY CYBERSECURITY FRAMEWORK]; Press Release, NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments (Oct. 22, 2013), http://www.nist.gov/itl/cybersecurity-102213.cfm.

172. *Cybersecurity Framework—Workshops and Events*, *supra* note 169.

173. Some of the minor adjustments included amending the Framework Core. For example, some of the Subcategories found in the "Identify" Function's "Risk Assessment" Category were restructured and included additional Informative References. *Compare* NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 22 ("ID.RA-3: Threats, both internal and external, are identified and documented."), *with* NIST PRELIMINARY CYBERSECURITY FRAMEWORK, *supra* note 171, at 15–16 ("ID.RA-3: Threats to organizational assets are identified and documented.").

revisions was the removal of verbiage designed to signal whether an organization has successfully implemented the Framework, stressing the "voluntary" nature of the Framework.[174] Certain terms, such as "adoption," were removed,[175] and greater emphasis was placed on the Framework's focus on critical infrastructure.[176] The most significant change came from the removal of the preliminary Framework's "Privacy Methodology," a detailed approach designed to address privacy and civil liberties considerations surrounding the deployment of cybersecurity activities.[177] Reflecting a concern among stakeholders that "the methodology did not reflect consensus private sector practices and therefore might limit use of the Framework,"[178] NIST incorporated an alternative privacy methodology developed by Hogan Lovells's partner Harriet Pearson.[179] The new privacy methodology, contained within the final version of the Framework, removes the organizational chart that would have corresponded to the Framework Core and instead provides a "general set of considerations and processes since privacy and civil liberties implications may differ by sector or over time and organizations may address these considerations and processes with a range of technical implementations."[180] Overall, the preliminary Framework provided the foundation for what would become version 1.0 of the final Framework.

B. Breakdown of the NIST Cybersecurity Framework

The Cybersecurity Framework takes a risk-based approach for organizations to detect, mitigate, and respond to cyber threats.[181] Rather than developing new

174. *See* NAT'L INST. OF STANDARDS & TECH, UPDATE ON THE DEVELOPMENT OF THE CYBERSECURITY FRAMEWORK 2 (2014) [hereinafter DEVELOPMENT OF THE CYBERSECURITY FRAMEWORK], *available at* http://www.nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-Update-011514-2.pdf ("A significant number of commenters stated that the Framework should reinforce throughout the document that it is intended to be voluntary.").

175. *See id.* ("While many commenters suggested incorporating the definition of 'adoption' previously identified by NIST, this was not an area of consensus as alternative definitions were proposed, and several commenters preferred that detail around adoption be reflected in use of the Framework or in supporting material.").

176. *See id.* ("NIST received comments recommending that the Framework state clearly that its focus is on the nation's critical infrastructure, while acknowledging that the document has broader utility and can be helpful to many parts of the economy.").

177. NIST PRELIMINARY CYBERSECURITY FRAMEWORK, *supra* note 171, at 28–35.

178. DEVELOPMENT OF THE CYBERSECURITY FRAMEWORK, *supra* note 174.

179. Letter from Harriet Pearson, Partner, Hogan Lovells, to Adam Sedgewick, Nat'l Inst. of Standards & Tech. (Dec. 5, 2013), http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf.

180. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 15.

181. Risk assessment and management is a complex process that has developed into its own, distinct area of expertise. "Risk," generally, refers to the "effect of uncertainty on objectives." International Organization for Standardization, *ISO 31000 2009: Plain English Introduction,* PRAXIOM RESEARCH GRP. LTD., http://www.praxiom.com/iso-31000-intro.htm (last visited Apr. 22, 2015). As the International Organization for Standardization's has further described:

> Whenever you try to achieve an objective, there's always the chance that things will not go according to plan. There's always the chance that you will not achieve what you expect to achieve. Every step you take to achieve an objective involves uncertainty. Every step has an

cybersecurity standards and risk management processes, the Cybersecurity Framework "relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience," which allows the Framework to "scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements."[182] The Cybersecurity Framework provides a "common language" for entities to evaluate their current cybersecurity posture, determine their targeted state for cybersecurity, prioritize opportunities for improvement, assess progress toward their targeted state, and establish sufficient methods of communication among internal and external stakeholders about cybersecurity risk.[183] The substance of the Cybersecurity Framework is composed of three parts: (1) The Framework Core, (2) The Framework Implementation Tiers, and (3) The Framework Profile. We investigate each element in turn.

1. Framework Core

The Cybersecurity Framework begins by laying out the Framework Core, which "provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes."[184] Neither an exhaustive list nor a checklist, the Framework Core is an organizational map of industry-recognized cybersecurity practices that are helpful in managing cybersecurity risk, and it provides unified terminology for organizations to understand successful cybersecurity practice outcomes.[185] The Framework Core is broken down into four elements—Functions, Categories, Subcategories, and Informative References—that assist in mapping applicable cybersecurity standards, guidelines, and best practices.[186]

The Core begins by delineating essential cybersecurity activities "at their highest level," referred to as Functions.[187] The Framework recognizes five Functions—Identify, Protect, Detect, Respond, and Recover[188]—that are intended to

> element of risk that needs to be managed . . . . [R]isk is the chance that there will be a positive or negative deviation from the objectives you expect to achieve.

Id. The process of identifying, assessing, and responding to risk is referred to as "risk management," and while the Framework itself is not a risk management process, it "uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity." NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 5.

182. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 4.

183. *Id.* at 1.

184. *Id.* at 7.

185. *See id.* ("The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk.").

186. *Id.* at 7–8. For a complete list of the applicable cybersecurity standards, guidelines, and best practices in the Framework Core, see *id.* app. A.

187. *Id.* at 7.

188. These Framework Core Functions are defined as follows:

> Identify-Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.. . . .
>
> Protect-Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.. . . .

assist an organization in expressing its management of cybersecurity risk by organizing practices into these key areas.[189] Each Function contains more detailed subsets of overarching practices, referred to as Categories, which are "groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities."[190] Each Category assists an organization's approach to mapping the key Functions underlying the Cybersecurity Framework.[191] Each Category provides a brief description to more efficiently place it within the context of its corresponding Function, as well as to guide further categorization within the remaining Core elements. For example, the "Identify" Function contains within it the "Asset Management" Category, which articulates practice outcomes to identify and manage the "data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes . . . consistent with their relative importance to business objectives and the organization's risk strategy."[192]

> Detect-Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. . . .
>
> Respond-Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. . . .
>
> Recover—Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 8–9.

189. *See id.* (explaining the categories within each Function and how they address cybersecurity risk).

190. *Id.* at 7.

191. *Cf. id.* app A at 19, tbl. 1 (listing Category Unique Identifiers for each Function).

192. *Id.* app. A at 20, tbl. 2.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CCS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8

Fig. 1: NIST Framework Core Example[193]

Further subdividing the Framework Core are "specific outcomes of technical and/or management activities" referred to within the Framework as Subcategories.[194] These subcategories provide further detail for organizations to address each overarching Category. Building off of our previous example, one Subcategory of the "Identify" Function's "Asset Management" Category is the practice of keeping inventory of all organization devices and systems, articulated in the above example as ID.AM-1.[195] Each of these Subcategories receives a reference to the corresponding "standards, guidelines, and practices common among critical infrastructure sectors" that would provide methods for accomplishing the stated Subcategory practice, referred to as "Informative Reference[s]."[196] An organization, for example, looking for an established standard or guideline for device inventory related to federal systems and organizations could look to the Framework's suggested NIST Special Publication 800-53.[197] Specifically, the Framework directs an entity to the publication's "Configuration Management-8: Information System Component Inventory" within the publication's security controls.[198] It is within this document that an organization can review the specific control requirements, supplemental

193. *Id.* at 8.

194. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 8.

195. *See supra* fig.1; *see also* NIST CYBERSECURITY FRAMEWORK, *supra* note 2, app. A at 20 tbl.2 ("Physical devices and systems within the organization are inventoried").

196. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, app. B at 38.

197. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NIST SPECIAL PUB. 800-53, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS (2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

198. *See id.* app. F-CM at F-73 to 75 (stating that an organization satisfies this control if the organization, among other requirements, "[d]evelops and documents an inventory of information system components that . . . [a]ccurately reflects the current information system . . . [i]ncludes all components within the authorization boundary of the information system . . . [i]s at the level of granularity deemed necessary for tracking and reporting; and . . . [r]eviews and updates the information system component inventory").

guidance to the control, and stated "control enhancements."[199] The Framework's Informative References are not intended to be an exhaustive list, and companies are encouraged to continue to identify new or revised standards, guidelines, or practices as the cybersecurity landscape evolves.[200]

2. The Framework Implementation Tiers

After mapping common cybersecurity activities and the various standards and practices employed to conduct these activities, the Framework provides a method for an organization to understand the degree to which its cybersecurity risk management practices match the characteristics described within the Framework, known as the Framework Implementation Tiers.[201] The Tiers provide a measurement for how organizations view and manage cybersecurity risk, taking into consideration an organization's current practices, the cyber threat environment, legal and regulatory requirements, business objectives, and organizational constraints, among other considerations.[202] Based upon an organization's evaluation of its practices, the organization can identify to which Tier it belongs. The Implementation Tiers consist of a range of four Tiers: Partial, Risk Informed, Repeatable, and Adaptive.[203]

Each Tier definition is broken down into three general subsections: (1) Risk Management Process; (2) Integrated Risk Management Program; and (3) External Participation.[204] These subsection definitions assist an organization in selecting its appropriate Tier.[205] The Risk Management Process subsection addresses the extent to which an organization's cybersecurity risk management practices are formalized, the breadth of these formalized practices, and the extent to which the practices actively adjust to the changing cybersecurity landscape.[206] The Integrated Risk Management Program subsection evaluates the level of awareness that managers and employees have of an organization's risk management practices, the level of involvement that managers and employees have in mitigating cybersecurity risks, and

199. *Id.*

200. The Privacy Methodology found within the NIST Cybersecurity Framework plays a role within the Framework Core as well. The Methodology calls on organizations, as they assess the Framework Core outlined in Appendix A of the Cybersecurity Framework, to consider a number of processes and activities that may be considered to address privacy and civil liberties implications. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 16–17. The categories of these processes and activities include: "Governance of cybersecurity risk"; "Approaches to identifying and authorizing individuals to access organizational assets and systems"; "Awareness and training measures"; "Anomalous activity detection and system and assets monitoring"; and "Response activities, including information sharing or other mitigation efforts." *Id.*

201. *Id.* at 5.

202. *Id.* at 9. It is important to note that the "Tiers do not represent maturity levels," but that advancing to a higher tier "is encouraged when such a change would reduce cybersecurity risk and be cost effective." *Id.*

203. *Id.* at 10–11.

204. *Id.*

205. *See id.* ("Tiers . . . provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. [Tiers] . . . describe an increasing degree of rigor and sophistication in cybersecurity risk management practices . . . .").

206. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 10–11 (describing each of these factors for each Tier).

the level of cybersecurity information sharing that occurs within the organization.[207] Finally, the External Participation subsection evaluates the extent to which organizations coordinate and collaborate with other external entities to share threat information.[208]

3. The Framework Profile

While the Framework's Implementation Tiers gauge the degree and sophistication of an organization's overall cybersecurity risk management practices, the Framework Profiles are meant to align the particular Framework Core Functions, Categories, and Subcategories with an organization's own implementation scenarios.[209] For example, an organization could create a "Current Profile" that would indicate "the cybersecurity outcomes that are currently being achieved" and a "Target Profile" that would specify "the outcomes needed to achieve the desired cybersecurity risk management goals."[210] Comparing these Profiles would allow an organization to reveal "gaps" that should be addressed to meet the organization's cybersecurity risk management objectives and assist the organization in establishing a roadmap for achieving its Target Profile.[211] Overall, the drafters expressed that "successful implementation" of the Framework is based on an organization's ability to achieve its Targeted Profiles.[212]

207. *Id.*

208. *Id.*

209. *Id.* at 5.

210. *Id.* at 11.

211. *Id.* (stating that that the Target Profiles should be "well aligned with organizational and sector goals, consider[] legal/regulatory requirements and industry best practices, and reflect[] risk management priorities").

212. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 9 ("Successful implementation of the Framework is based upon achievement of the outcomes described in the organization's Target Profile(s).").

	Risk Management Process	Integrated Program	External Participation
Tier 1: Partial	Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/ mission requirements.	There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.	An organization may not have the processes in place to participate in coordination or collaboration with other entities.
Tier 2: Risk-Informed	Risk management practices are approved by management but may not be established as organizational-wide policy. . . .	There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.	The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.
Tier 3: Risk-Informed and Repeatable	The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to . . . a changing threat and technology landscape.	There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.	The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.
Tier 4: Adaptive	The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous . . . cybersecurity activities. Through a process of continuous improvement . . . the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.	There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.	The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

Fig. 2: NIST Framework Implementation Tiers Definitions[213]

213. *Id.* at 10–11.

C. Implementing the NIST Cybersecurity Framework

Articulating the basic components is only a portion of the Framework. Even more critical is how an organization implements the Framework. Understanding that organizations and industries vary significantly, and that cyber threats evolve rapidly, the Framework was developed in such a way as to allow implementation throughout myriad critical infrastructure settings.[214] First, the Framework was developed to be organizationally comprehensive, emphasizing coordination of the Framework throughout every level of an organization.[215] Second, the Framework was created to be flexible, allowing it to supplement an organization's already existing cybersecurity risk management program or to guide an organization in implementing such a risk management program for the first time.[216] Third, the Framework was organized to be adaptable to changing circumstances and environments so that future versions of the Framework could be created as the cybersecurity landscape evolves.[217]

The Framework stresses the coordination of risk management activities within every level of an organization.[218] Early on in the Framework's development, stakeholders emphasized the importance of the Framework's implementation into all levels of an organization—from senior leadership to employees, partners, and customers.[219] Thus, the Framework explains how the executive level, the business and process level, and the implementation and operations level of an organization can contribute to the implementation of the Framework.[220] Additionally, the Framework's flexibility is intended to allow its approach to address cybersecurity risks regardless of the organization, industry, or country.[221] As the Framework stresses, it is "not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure."[222] Instead, it assembles effective national and international cybersecurity practices, giving organizations the autonomy to adopt the Framework in a manner that fits the organization's business requirements and current risk management practices.

Further, because the NIST Framework "references globally recognized standards for cybersecurity, the Framework can also be used by organizations located outside the United States and can serve as a model for international

214. *See id.* at 4 (discussing the various considerations that went into the Framework, including making it adaptable for numerous different industries and businesses in various countries).

215. *Id.*

216. *Id.* at 6.

217. *See supra* text accompanying note 182.

218. *See* NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 12 & fig.2 (diagramming and discussing how executives, business/process level, and implementation/operations level personnel can simultaneously work toward improving cybersecurity).

219. *See* NAT'L INST. FOR STANDARDS & TECH., UPDATE ON THE DEVELOPMENT OF THE CYBERSECURITY FRAMEWORK (2013) (finding that the Cybersecurity Framework's Request for Information period stressed "the importance of senior leadership's engagement in the cybersecurity risk management process," and "[a]s a foundation, all users, including employees, partners, and customers, have a need for general cybersecurity awareness").

220. *See* NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 12 (describing a "common flow of information" and decision-making within an organization that includes all levels of an organization).

221. The Framework was importantly not intended to be United States-specific, and the Framework stresses that "the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity." *Id.* at 4.

222. *Id.* at 2.

cooperation on strengthening critical infrastructure cybersecurity."[223] One region of significance is Europe. In 2013, a EU cybersecurity directive was proposed; it would require that companies harden their security policies to meet EU-developed standards—a development that could cause any firm providing online services in Europe to "fundamentally have to change the way its business operates."[224] Moreover, U.S.-EU policymakers are in regular discussions, meaning that the NIST Framework could be influential in shaping EU efforts in this space[225] and could even help shape a global duty of cybersecurity care—as is explored further in Part III.

The Framework provides a seven-step implementation process and may be used either as a reference guide to create a new risk management program or to supplement an already existing program.[226] For instance, AT&T has stated that it will begin assessing how the Framework "best complements [its] existing cyber-risk management program."[227] At the same time, IBM announced the creation of the IBM Industrial Controls Cybersecurity Consulting service that will assist companies in utilizing the Framework by "educat[ing] clients on details and mechanics of the NIST Cybersecurity Framework and perform[ing] a comprehensive assessment of a client's security maturity relative to the guidelines, best practices and international standards referenced in the Framework."[228]

Finally, the Framework's adaptability to changing circumstances allows it to evolve as the cybersecurity landscape continues to mature. The Framework is a "living document" that will be amended, updated, and improved as companies begin implementing the Framework and feedback begins to surface.[229] On the day the Framework was released, a "roadmap" was issued that discussed the Framework's "next steps" and identified "key areas of development, alignment, and collaboration."[230] NIST plans to relinquish its role as "convener and coordinator" to private industry, but it plans to continue its current leadership into at least version 2.0.[231]

223. *Id.* at 1–2.

224. *See* Warwick Ashford, *How Will EU Cyber Security Directive Affect Business?*, COMPUTERWEEKLY (Feb. 19, 2013), http://www.computerweekly.com/news/2240178256/How-will-EU-cybersecurity-directive-affect-business (citing Stewart Room, a partner at Field Fisher Waterhouse, who argues that this directive will mean that other firms beyond telecom companies will face regulatory burdens related to cybersecurity, including "e-commerce platforms; [I]nternet payment gateways; social networks; search engines; cloud computing services; and app stores").

225. *See generally EU Eying NIST Framework With 'Great Interest'*, *supra* note 30.

226. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 13–15.

227. Ed Amoroso, *Protecting Our Nation's Critical Infrastructure*, AT&T PUB. POL'Y BLOG (Feb. 12, 2014), http://www.attpublicpolicy.com/cybersecurity/protecting-our-nations-critical-infrastructure/.

228. Press Release, IBM, IBM to Help Companies Utilize New Cybersecurity Framework Aimed at Protecting Nation's Critical Infrastructure (Feb. 13, 2014), http://www-03.ibm.com/press/us/en/pressrelease/43207.wss.

229. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 2.

230. NAT'L INST. OF STANDARDS & TECH., NIST ROADMAP FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1 (2014), http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

231. *Id.* at 1–2.

D. Framework Incentives and C-Cubed Voluntary Program

A difficulty with any voluntary program is encouraging participation. While advocated as a "cost-effective" approach,[232] implementing the Framework's practices will inevitably require time, money, and resources on the part of critical infrastructure organizations, especially those organizations that are currently without a cybersecurity risk management program. At the outset, increasing organizational participation in the Framework was approached in two ways: (1) reviewing current regulatory authorities to determine if establishing requirements based upon the Cybersecurity Framework would be permissible under current authority; and (2) researching a set of implementation incentives and developing a voluntary program to support the adoption of the Framework.[233]

First, Executive Order 13636 called on agencies with "responsibility for regulating the security of critical infrastructure [to] engage in a consultative process with [the] DHS, [the Office of Management and Budget], and the National Security Staff to review the . . . Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks."[234] These agencies are instructed to report to the President "whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required."[235]

However, not every organization that may fall within the ambit of "critical infrastructure" has clear regulatory requirements related to cybersecurity. To maintain the voluntary nature of the Framework, Executive Order 13636 tasked the Secretary of Homeland Security, "in coordination with Sector-Specific Agencies," to develop a "voluntary program" to support adoption of the Framework by critical infrastructure organizations and other interested entities.[236] Coinciding with the release of the Cybersecurity Framework, the DHS announced the Critical Infrastructure Cyber Community C³ Voluntary Program (C-Cubed Program).[237] The C-Cubed Program aims to "assist stakeholders with understanding use of the

232. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 1.

233. Exec. Order No. 13636, 78 Fed. Reg. 11739, 11742–43 (Feb. 19, 2013).

234. *Id.* at 11742.

235. *Id.* at 11743. If current regulatory requirements were deemed "insufficient," agencies with responsibility for regulating the security of critical infrastructure are required to "propose prioritized, risk-based, efficient, and coordinated actions . . . to mitigate cyber risk." *Id.*

236. *Id.* at 11742–43. The Presidential Policy Directive 21 outlined the sixteen sectors of "critical infrastructure," as well as the "[s]ector-[s]pecific agency" that has "institutional knowledge and specialized expertise about the sector." Press Release, White House, Presidential Policy Directive—Critical Infrastructure Security and Resilience (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. The critical infrastructure sectors established by the Directive, and their respective sector specific agencies, include: Chemical (DHS); Commercial Facilities (DHS); Communications (DHS); Critical Manufacturing (DHS); Dams (DHS); Defense Industrial Base (DoD); Emergency Services (DHS); Energy (Department of Energy); Financial Services (Department of Treasury); Food and Agriculture (Department of Agriculture and Department of Health and Human Services (DHHS)); Government Facilities (DHS and General Services Administration); Healthcare and Public Health (DHHS); Information Technology (DHS); Nuclear Reactors, Materials, and Waste (DHS); Transportation Systems (DHS and Department of Transportation); and Water and Wastewater Systems (Environmental Protection Agency). *Id.*

237. *Critical Infrastructure Cyber Community Voluntary Program*, US–CERT, http://www.us-cert.gov/ccubedvp (last visited Apr. 1, 2015).

Framework and other cyber risk management efforts, and support development of general and sector-specific guidance for Framework implementation."[238]

In addition to creating a voluntary program, Executive Order 13636 tasked the Secretary of Homeland Security, the Secretary of the Treasury, and the Secretary of Commerce with establishing "a set of incentives designed to promote participation in the Program."[239] The Departments' recommendations provided overlapping suggestions on how best to encourage the Framework's adoption[240] as well as consensus on eight recommendations: cybersecurity insurance, grant funds, government service process preferences, liability limitations, streamlining and unifying regulations, public recognition of voluntary participation, rate recovery for price regulated industries, and increased cybersecurity research.[241] Comments from the Obama Administration suggest it believes that market-based incentives and encouragement through the C-Cubed Voluntary Program will be the most successful drivers for organizations to adopt the Cybersecurity Framework. One senior Administration official stated:

> [W]e believe that the best drivers for adoption or use of the framework will ultimately be market based. Don't get me wrong, I think the government-based incentives are really important for us to pursue. But at the end of the day, it's the market that's got to drive the business case for the Cybersecurity Framework. The federal government is going to do its best to make the costs of using the framework lower, and the benefits of the framework higher, but it's the market that's going to ultimately make this work.[242]

As we will explore in Part III, however, market-driven incentives may be eclipsed not only by up-front costs but also by uncertainty—for instance, by creating incentives to avoid potential liability that may arise from failing to implement the Framework.

238. *Id.*

239. Exec. Order No. 13636, 78 Fed. Reg. at 11742.

240. *See* DEP'T OF COMMERCE, DISCUSSION ON RECOMMENDATIONS TO THE PRESIDENT ON INCENTIVES FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS TO JOIN A VOLUNTARY CYBERSECURITY PROGRAM 1–3 (2013) [hereinafter DEP'T OF COMMERCE RECOMMENDATIONS], *available at* http://www.ntia.doc.gov/files/ntia/ Commerce_Incentives_Discussion_Final.pdf (listing proposed government incentives to encourage adoption of the cybersecurity framework); DEP'T OF HOMELAND SEC., EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 3 (2013) [hereinafter DHS STUDY], *available at* https://www.dhs.gov/ sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf ("Securing critical infrastructure against growing and evolving cyber threats requires a layered approach."); TREASURY DEP'T, SUMMARY REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636, at 3–6 (2013) [hereinafter TREASURY DEP'T REPORT], *available at* http://www.treasury.gov/press-center/Documents/Treasury%20Report%20%28Summary%29%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf (detailing numerous government incentives that could encourage the adoption of the cybersecurity framework).

241. Daniel, *Incentives*, *supra* note 19.

242. Press Release, White House, Background Briefing on the Launch of the Cybersecurity Framework (Feb. 12, 2014), http://www.whitehouse.gov/the-press-office/2014/02/12/background-briefing-launch-cybersecurity-framework.

E. Summary

This Part has explored the evolution and scope of the NIST Framework, investigating the reasons for its creation (namely Congressional inaction coupled with mounting cyber insecurity) and exploring its initial reception and uptake by critical infrastructure providers. The next task is linking this investigation to the legal analysis of Part I to begin exploring what impact the NIST Framework might have on delineating a global cybersecurity standard of care, which we conclude with next.

III. POTENTIAL FOR NIST CYBERSECURITY FRAMEWORK TO DEFINE NATIONAL AND INTERNATIONAL STANDARDS OF CYBERSECURITY CARE

As Part I demonstrated, legal compliance with current U.S. cybersecurity law relies heavily on interpreting and implementing "reasonable" and "appropriate" cybersecurity measures. Negligence law relies on oftentimes amorphous reasonable standards of care, while statutes like the GLBA require covered financial institutions to provide reasonable security safeguards. High-risk chemical facilities under the CFATS need to implement appropriate risk-based measures to mitigate cyber attacks in order to be compliant, while state breach notification statutes such as that of Massachusetts include clauses requiring governmental and private entities to implement reasonable data security measures. Given that what constitutes "reasonable" cybersecurty practices is not yet well defined, the NIST Cybersecurity Framework has the potential to be influential in shaping reasonable cybersecurity standards in the United States and further afield.

Like the United States, other nations and regions, including the United Kingdom, EU, and India, are in the midst of reshaping their own cybersecurity policies.[243] All of these jurisdictions have to date favored, to a greater or lesser degree, a more voluntary approach to enhancing cybersecurity, including for critical infrastructure companies, which could enhance the impact of the NIST Framework.[244] Indeed, because the NIST Framework "references globally recognized standards for cybersecurity," the drafters of the Framework created the instrument such that it may "also be used by organizations located outside the United States and can serve

243. *See*, *e.g.*, *EU Eying NIST Framework With 'Great Interest'*, *supra* note 30 (stating that the EU is trying to set up a cybersecurity framework and is considering the U.S. framework with great interest); Press Release, Cabinet Office & Francis Maude, Member of Parliament, Government Mandates New Cyber Security Standard for Suppliers (Sept. 26, 2014), http://www.gov.uk/government/news/ government-mandates-new-cyber-security-standard-for-suppliers (announcing that contractors bidding for some U.K. government contracts must comply with new "Cyber Essentials" controls); *NIST to Discuss Cybersecurity Framework with Officials from India*, INSIDE CYBERSECURITY (Sept. 16, 2014), http://insidecybersecurity.com/index.php?option=com_user&view=login&return=aHR0cDovL2luc21kZWN5YmVyc2VjdXJpdHkuY29tL0N5YmVyLURhaWx5LU5ld3MvRGFpbHktQnJpZWZzL25pc3QtdG8tZGlzY3Vzcy1jeWJlcnNlY3VyaXR5LWZyYW1ld29yay13aXRoLW9mZmljaWFscy1mcm9tLWluZGlhL21lbnUtaWQtMTA3NS5odG1s (reporting that the NIST is hosting Indian officials at a cybersecurity workshop to foster information exchanges about cybersecurity policies between the United States and India).

244. For more information on comparative critical infrastructure regulation, see generally Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014).

as a model for international cooperation on strengthening critical infrastructure cybersecurity."[245]

Although the time is not yet ripe to tell a definitive story of the national, to say nothing of the global, impact of the NIST Framework given how recently the Framework was announced prior to this writing, it is important to begin a conversation—especially given the centrality of due diligence standards in building out norms that would contribute to a law of cyber peace applicable below the armed attack threshold.[246] Although norms may not bind states in the same manner as formalized treaties, as Jim Lewis of the Center for Strategic and International Studies has noted, "[N]on-binding norms [can] exercise a powerful influence on state behaviour."[247] Indeed, the importance of norms to enhancing cybersecurity has been referenced in numerous international conferences[248] and in academia.[249] In particular, due diligence standards, which may be considered to be a core area of cybersecurity that the NIST Framework is designed to strengthen, have been touted as a vital cyber norm to better define.[250] To that end, this Part examines three case studies—the United Kingdom, the EU, and India—to begin the analysis of how the NIST Framework may help shape a regional, if not global, cybersecurity standard of care for critical infrastructure firms. Finally, it assesses the role that the private sector might play in promoting the Framework globally.

A. The NIST Cybersecurity Framework and Shaping a Reasonable Standard of Care

The NIST Framework could have a particularly significant impact on shaping a reasonable standard of cybersecurity care in common law negligence claims. What exactly is "reasonable" is itself open to interpretation. Courts, however, have found that it does not necessarily infer "state of the art" facilities, technologies, or business

245. NIST CYBERSECURITY FRAMEWORK, *supra* note 2, at 1–2.

246. *See* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 229–32 (2009) (introducing the international law applicable above and below the armed attack threshold, which is the point above which the law of war is activated).

247. James Andrew Lewis, *Confidence-Building and International Agreement in Cybersecurity*, *in* DISARMAMENT FORUM: CONFRONTING CYBERCONFLICT 51, 53 (2011).

248. *E.g.*, Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 65th Sess., Sept. 14, 2010–Sept. 12, 2011, para. 18, U.N. Doc. A/65/201 (July 30, 2010). For example, in 2007, the International Telecommunications Union (ITC) held a cybersecurity workshop to bring together West African stakeholders "to discuss, share information, and collaborate on the elaboration and implementation of national policy, regulatory and enforcement frameworks for cybersecurity and CIIP," also known as critical information infrastructure protection. *ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP)*, INT'L TELECOMM. UNION, http://www.itu.int/ITU-D/cyb/events/2007/praia/ (last visited Apr. 2, 2015).

249. *See*, *e.g.*, ROGER HURWITZ, AN AUGMENTED SUMMARY OF THE HARVARD, MIT AND U. OF TORONTO CYBER NORMS WORKSHOP 8–10 (2012) (outlining the difficulty of building consensus around international cybersecurity norms at a large academic workshop).

250. *See*, *e.g.*, Andreas Zimmermann, *International Law and 'Cyber Space'*, ESIL REFLECTIONS, Jan. 2014, at 1, 4, *available at* http://www.esil-sedi.eu/sites/default/files/ESIL%20Reflections%20-%20Andreas%20Zimmermann_0.pdf (noting that there are many unanswered legal questions related to the specific content of due diligence obligations in cyber space).

practices.[251] Because of the ambiguity that can surround reasonableness, reliance on industry standards has been used "as a guidepost for assessing reasonable conduct."[252] As has been stated, "Company practices and procedures should be rooted in concepts of reasonableness. Adherence to industry practice, in turn, may be viewed as reasonable and provide a defense in some cases in the event of litigation."[253]

When viewed through the lens of Judge Hand's risk/utility formula discussed in Part I,[254] the Cybersecurity Framework could provide a new basis on which courts utilize the formula, particularly in determining how "adequate" the Framework might have been to prevent alleged harm and the "burden" on an organization to implement the Framework. The Framework, again, is not a new set of standards or best practices for critical infrastructure organizations but instead provides a way for companies to determine which standards and practices are worth implementing and whether an organization is adequately doing so through its current risk management process. The Framework's approach to applying common cybersecurity practices could be an "adequate precaution" to mitigate cybersecurity threats that, if successful, could result in harm to the nation's security, the economy, or the public's safety. Courts could also look at what the "burden" on an organization might have been to use the Framework to determine which cybersecurity practices were best suited for their particular industry. Overall, a critical infrastructure organization could be found to have acted negligently if it is determined that (1) the critical infrastructure organization suffered a cyber attack that resulted in damage or injury; (2) the organization failed to utilize the Framework to address and manage its cybersecurity risks; (3) the Framework is deemed an adequate precaution that, if implemented, would have prevented the harm; and (4) the burden on an organization to utilize the Framework was less than the probability that the cybersecurity incident would occur multiplied by the significance of the incident.

Outside of a risk/utility analysis, reliance on industry standards to determine what constitutes reasonable cybersecurity practices leaves ample room for utilization of the NIST Framework. Similar to the FFIEC report in *Shames–Yeakel*,[255] the NIST Cybersecurity Framework could be utilized to argue the appropriate standard of care. Failing to comply with the NIST Framework, similar to Citizens Financial Bank's delayed compliance with the recommended multi-factor authentication in the FFIEC report or Sony's failure to employ industry encryption standards,[256] could be enough to establish a triable issue of fact as to whether reasonable standards of cybersecurity have been met by a company (meaning that courts would not be able to establish as a matter of law that a company adhered to a reasonable standard of care). Overall, cases like *Shames–Yeakel* and the many cases deriving from the 2011 Sony breach demonstrate just how fertile the ground is for defining a reasonable

251. *See*, *e.g.*, Ross v. RJM Acquisitions Funding LLC, 480 F.3d 493, 496–99 (7th Cir. 2007) (analyzing the term "reasonable" under the Fair Debt Collection Practices Act). *Ross* is not a security case and thus is limited in its authoritative value. However, the Fair Debt Collection Practice Act, which the court is interpreting, may be used as persuasive authority in the context of technological safeguards. ANDREW B. SERWIN, INFORMATION SECURITY AND PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE § 24:96 (2014).

252. IAN BALLON, E-COMMERCE AND INTERNET LAW: TREATISE WITH FORMS § 2.05 (2014).

253. *Id.*

254. *See supra* notes 58–65 and accompanying text.

255. *See supra* notes 84–87 and accompanying text.

256. *See supra* notes 71–76 and accompanying text.

standard of cybersecurity care—and just how cogently the Cybersecurity Framework could fulfill that role depending on industry uptake and ultimate judicial interpretation.

Attempts to utilize the Framework under a negligence theory would still need to overcome the other hurdles plaguing data security cases. Hurdles—such as establishing Article III standing and overcoming the economic loss doctrine—have often prevented in-depth judicial analysis of the standard of care issue in data security negligence cases.[257] That being said, if the consequences of lax security measures go beyond breach of sensitive data and produce kinetic effects impacting the health, safety, and welfare of individuals, then plaintiffs attempting to recover from mere data breaches will likely be able to overcome some of these hurdles.[258] As a result, courts would have the opportunity to grapple more directly with the standard of care issue.

In addition to its impact on common law, the Cybersecurity Framework could shape statutorily enumerated requirements on organizations to implement reasonable cybersecurity requirements. As Part I demonstrated, many statutory and regulatory requirements do not mandate specific practices, but instead provide space for an organization to assess its own cyber risks and implement reasonable safeguards.[259] Similar to negligence and fiduciary law, the NIST Framework's collection of industry practices to identify, protect, detect, respond, and recover from cybersecurity risks could thus set the standard for what constitutes reasonable cybersecurity practices within these statutory regimes.

To date, the Administration has continued to push for a voluntary approach to the Framework's adoption,[260] thus making it unlikely that regulators will use their enforcement authority against covered entities that fail to voluntarily utilize the NIST Framework. After assessing the sufficiency of existing regulatory authority to establish requirements based on the Cybersecurity Framework, as ordered by Executive Order 13636, the President's Cybersecurity Coordinator, Michael Daniel, announced that "existing regulatory requirements, when complemented with strong voluntary partnerships, are capable of mitigating cyber risks to our critical systems and information."[261] Reviews conducted by the Environmental Protection Agency,[262]

257. *See supra* notes 88–91 and accompanying text.

258. *See*, *e.g.*, Fahmida Y. Rashid, *Chinese Hackers Attacked FEC During Government Shutdown*, PC MAG. SECURITY WATCH (Dec. 17, 2013), http://securitywatch.pcmag.com/hacking/318975-chinese-hackers-attacked-fec-during-government-shutdown (reporting on a massive hack on the Federal Election Commission (FEC) that "crashed several FEC computer systems" while IT personnel were furloughed during the 2013 government shutdown); *see also* WATER SECTOR COORDINATING COUNCIL CYBER SEC. WORKING GRP., ROADMAP TO SECURE CONTROL SYSTEMS IN THE WATER SECTOR 16 (2008) (listing "real cyber events" that resulted in kinetic consequences involving water sector organizations).

259. *See supra* Part I.C.

260. *See supra* Part II.

261. Michael Daniel, *Assessing Cybersecurity Regulations*, WHITE HOUSE BLOG (May 22, 2014), http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations.

262. *See*, *e.g.*, Letter from Peter C. Grevatt, Dir., U.S. Envt'l Prot. Agency Office of Ground Water & Drinking Water, to Michael Daniel, http://water.epa.gov/infrastructure/watersecurity/upload/EO_13696_10-b-_EPA_response.pdf ("[T]he EPA believes that a voluntary partnership model is a proven approach that will be effective for managing cybersecurity risks . . . .").

the Department of Health and Human Services,[263] and the DHS[264] all generally supported the voluntary approach to addressing and mitigating cyber risks. However, the voluntary approach could very well shift to a more mandatory approach if the current implementation policies are found to be ineffective.[265] Some critical infrastructure organizations, recognizing the consistency between the Cybersecurity Framework and existing regulatory requirements like the GLBA, HIPAA, and CFATS, are proactively reviewing their cybersecurity risk management practices to reflect both the Framework and their existing regulatory requirements.[266] Although potentially beneficial, such an extra level of due diligence also increases the time and resources these organizations must take to ensure compliance, as is discussed further below.[267]

Beyond regulatory enforcement, however, federal requirements on organizations to implement cybersecurity requirements could be used to impose liability through the legal doctrine of negligence per se. Negligence per se is a "theory of negligence in which the fact that an entity's conduct has violated some applicable statute is *prima facie* evidence that the entity has acted negligently."[268] In other words, conduct that violates a statute satisfies the "duty" and "breach" elements of a plaintiff's negligence claim. "In the context of cyber threats to critical infrastructure," a Congressional Research Service report on critical infrastructure liability has stated, "a regulated entity that fails to adequately secure its information infrastructure as required under a federal regulatory scheme [may be] liable for a cyber incident that causes harm to customers or other third parties."[269] If the NIST Framework is utilized as a benchmark for the various sector-specific cybersecurity requirements, an organization may not only face penalties from a federal regulator but also may be open to negligence per se–based lawsuits. However, the utilization

263. *See*, *e.g.*, Press Release, Dep't of Health and Human Servs., HHS Activities to Enhance Cybersecurity: Executive Order 13636, Section 10(b)—HHS Assessment (May 12, 2014), http://www.phe.gov/Preparedness/planning/cip/Pages/eo13636.aspx ("Through these programs, HHS works in voluntarypartnership with public and private sector entities . . . to enhance their security and resilience with respect to all hazards, including cyber threats.").

264. *See*, *e.g.*, DEP'T OF HOMELAND SEC., EXECUTIVE ORDER 13636—IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY SECTION 10(B) REPORT ON THE DEPARTMENT OF HOMELAND SECURITY'S CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (2014), *available at* http://www.dhs.gov/sites/default/files/publications/EO%2013636%20Section%2010%28b%29%20Report%20for%20CFATS%20%28May%202014%29%20Final_0.pdf (discussing various proposals that "have value as part of an overall approach to risk management," which led DHS to "encourag[e] high-risk chemical facilities to consider the voluntary adoption" of NIST Framework protocols).

265. *Cf. Cyber Regulatory Landscape Could Be More Nuanced than Acknowledged*, INSIDE CYBERSECURITY (May 19, 2014), http://insidecybersecurity.com/Cyber-General/Cyber-Public-Content/cyber-regulatory-landscape-could-be-more-nuanced-than-acknowledged/menu-id-1089.html ("[T]he White House is broadly asserting, without disclosing details, that federal regulators are confident their existing authority is adequate to implement the president's cybersecurity executive order.").

266. *See*, *e.g.*, Joe Adler, *Why Obama's "Voluntary" Cybersecurity Plan May Prove Mandatory*, AM. BANKER, Feb. 14, 2014, http://www.americanbanker.com/issues/179_32/why-obamas-voluntary-cybersecurity-plan-may-prove-mandatory-1065651-1.html (finding that the financial sector expects regulators to incorporate the cybersecurity framework in their requirements for financial institutions, likely by cross-referencing it to the privacy and security obligations under the GLBA).

267. *See infra* notes 316–325 and accompanying text.

268. LIU ET AL., *supra* note 20, at 6 (citing Makas v. Hillhaven, Inc., 589 F. Supp. 736, 741 (M.D.N.C. 1984)).

269. LIU ET AL., *supra* note 20, at 6.

of the negligence per se standard still falls prey to the other negligence hurdles the plaintiff must satisfy, including satisfying standing requirements, making it somewhat difficult to employ negligence per se in a cybersecurity context.[270]

Beyond federal regulatory requirements, state laws that call for "reasonable" security measures for certain types of personal information may also provide an opportunity for the Cybersecurity Framework to play a part in shaping what constitutes reasonable standards of cybersecurity care. Organizations operating within a particular state—especially those that use or store personal information as defined under state law—need to also be aware of the potential for liability that state statutes might create. This also reflects general security requirements that supplement state breach notification laws. Organizations that fail to utilize the Framework and suffer a breach that compromises a particular state's citizens' personal information may be open to regulatory action by the appropriate state authorities under an argument that the company has failed to implement "reasonable" security measures. In addition, some states are looking to explicitly require through legislation utilization of the Cybersecurity Framework now that the Framework has been released.[271]

Regardless of the Framework's eventual impact on a reasonable standard of cybersecurity care, the uncertainty of legal consequences may be enough to hinder private-sector voluntary participation in the Framework.[272] Legal compliance issues have typically dominated business approaches to cyber threats. A 2013 survey by AIG and Penn Schoen Berland, for instance, found that 75% of executives and brokers said that "legal compliance issues are making companies think more about cyber risks."[273]

This focus on legal compliance has prompted a push for congressional action that could limit the liability of organizations that implement the Framework. The incentive reports issued by the DHS, the Department of Commerce, and the Department of the Treasury all included discussion on some form of limited liability for companies who voluntarily adopt the Framework.[274] The Commerce Department, for instance, suggested that the Framework should:

> include a review of tort cases against critical infrastructure owners and operators and an assessment of mechanisms . . . that have the potential to

270. *See* Rustad & Koenig, *Extending Hand's Formula*, *supra* note 65, at 241 (stating that, at the time of the article's publication, "[n]o plaintiff has successfully employed a *negligence per se* argument in a computer security case").

271. *See*, *e.g.*, H.B. 804, 434th Gen. Assemb., Reg. Sess. (Md. 2014) (proposing to require Maryland to include a cybersecurity framework within its information technology master plan, and for that framework to consider materials developed by the NIST).

272. Lauren Larson, *NIST, DHS Push for More Engagement Around Cyber Framework*, FEDERAL NEWS RADIO (Mar. 27, 2014), http://www.federalnewsradio.com/473/3591100/NIST-DHS-push-for-more-engagement-around-cyber-framework- (reporting statements of Wisconsin Senator Ron Johnson that "fear of legal entanglements may be hindering participation" in the NIST framework).

273. Press Release, Am. Int'l Grp., Inc., AIG Survey Finds More Insurance Decision Makers Concerned about Cyber Threat than Other Major Risks (Feb. 6, 2013), http://phx.corporate-ir.net/phoenix.zhtml?c=76115&p=irol-newsArticle&ID=1782195&highlight=.

274. DEP'T OF COMMERCE RECOMMENDATIONS, *supra* note 240, at 14–15; DHS STUDY, *supra* note 240, at 62–63; TREASURY DEP'T REPORT, *supra* note 240, at 3.

> reduce or transfer their tort liability if a cyber incident causes damage despite the owner or operator's adoption and implementation of some or all of the standards, procedures, and other measures that comprise the Framework.[275]

Fear of liability is also a reason why many recent cybersecurity legislative proposals have included limits on legal liability for organizations that implemented the proposed framework.[276] Until these legal uncertainties are addressed, the Administration's aspirational goals of widespread utilization of the Framework may prove futile.

Of course, a different outcome is also conceivable. The legal uncertainty surrounding the Framework's impact on legal liability could be an incentive for organizations to begin implementing the Cybersecurity Framework. Given the ambiguity as to how exactly a reasonable standard of cybersecurity care may be taking form, implementation of the Framework could be viewed by companies as the most efficient way to mitigate risk to legal liability. So while some fear that the Framework may be used as a sword by plaintiffs,[277] companies may look to the Framework for its use as a liability shield, arguing that, despite the occurrence of cyber attacks resulting in harm, an organization's utilization of the Framework translated into reasonable security measures under the circumstances and could therefore mitigate liability. Companies though may still look to government to make this "safe harbor" concept explicit through congressional action given the absence of comprehensive U.S. cybersecurity legislation.

B. Voluntary Cybersecurity Frameworks in Global Context

The lack of clarity regarding what constitutes a standard of cybersecurity care in the United States is further muddled when comparing the situation in the U.S. with that of other jurisdictions. Still, analyzing national regulation in cyberspace is important for at least three reasons: (1) national control of cyberspace is increasing and is a critical aspect of its status as a "pseudo commons,"[278] (2) enclosure through

275. DEP'T OF COMMERCE RECOMMENDATIONS, *supra* note 240, at 2.

276. *E.g.*, Cybersecurity Act of 2012, S. 3414, 112th Cong. § 706 (2012).

277. *See*, *e.g.*, Chris Strohm, *US Unveils Cyber Security Guidelines for Industry*, HYDROCARBON PROCESSING (Feb. 14, 2014), http://www.hydrocarbonprocessing.com/Article/3309410/Latest-News/US-unveils-cyber-security-guidelines-for-industry.html (quoting a lawyer who sees the potential for a company's non-adoption of the framework leading to a "presumption of negligence" against the company).

278. The pseudo commons represents a compromise position between competing models of cyber regulation, namely those espousing Internet sovereignty and Internet freedom, i.e., considering cyberspace as an extension of national territory or a global networked commons. *See*, *e.g.*, David R. Johnson & David G. Post, *Law and Borders–The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375 (1996) ("The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign."); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 519 (1999) ("The limitations on the scope of intellectual property law serve to fuel the intellectual commons—to generate a resource upon which others can draw."); *see also* JOSEPH S. NYE, JR., THE FUTURE OF POWER 143 (2011) (referring to cyberspace as an "imperfect commons"); Press Release, Ind. U., London Conference Reveals 'Fault Lines' in Global Cyberspace and Cybersecurity Governance (Nov. 7, 2011), *available at* http://newsinfo.iu.edu/news/page/normal/20236.html (highlighting the tension between civil liberties and regulations online).

nationalization is one of the classic solutions to the tragedy of the commons,[279] and (3) national regulations form an important component of polycentric governance—a useful vehicle for conceptualizing cybersecurity law and policy—even though states do not enjoy a "general regulatory monopoly" in cyberspace.[280] The importance of investigating national regulation comes into sharp relief in the context of the NIST Framework, especially given the extent to which it could catalyze positive network effects, enhancing cybersecurity across sectors and borders.[281]

1. U.K. Cybersecurity Frameworks

In the United Kingdom, as in the United States, the emphasis to date has been on voluntary standards to enhance Critical National Infrastructure protection. For example, the 2011 U.K. Cyber Security Strategy, which focuses on government contractors, states that the British government "will work with industry to develop rigorous cyber security . . . standards."[282] In addition, the United Kingdom's Centre for the Protection of National Infrastructure (CPNI) published "a baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."[283] However, the Strategy neglects to explain how the largely voluntary approach represents a significant change to the status quo sufficient to effectively meet this threat to British national security,[284] and the information security controls are labeled specifically as "guidance."[285] The Strategy also does not offer specifics about how the British government will help enhance cybersecurity for the "wider group of companies not currently deemed part of the critical infrastructure" but which are nevertheless essential to Britain's long-term economic competitiveness.[286] However, the United Kingdom has announced plans for a new strike force capable of protecting public and private sector assets against cyber attacks.[287]

279. *See*, *e.g.*, Antonio Lambino, *Impending Tragedy of the Digital Commons?*, WORLD BANK (Oct. 25, 2010), http://blogs.worldbank.org/publicsphere/node/5562 (discussing the tendency of governments to intervene in computer networks in the interest of national security).

280. ANDREW D. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 47 (2007). For more on the role that polycentric governance can play in enhancing cybersecurity, see Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance*, 62 AM. U. L. REV. 1273 (2013).

281. *Cf.* Neal K. Katyal, *The Dark Side of Private Ordering: The Network/Community Harm of Crime*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 193, 193–94 (Mark F. Grady & Francesco Parisi eds., 2006) ("The Internet is the paradigmatic sphere in which the positive advantage of 'network effects' is central—that the greater the size of the network, the greater the benefits.").

282. U.K. CABINET OFFICE, THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 27 (2011), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (emphasis omitted).

283. *Critical Security Controls Guidance*, CTR. FOR PROTECTION OF NAT'L INFRASTRUCTURE, http://www. cpni.gov.uk/advice/cyber/Critical-controls/ (last visited Apr. 2, 2015).

284. *See generally* U.K. CABINET OFFICE, *supra* note 282.

285. *Critical Security Controls Guidance*, *supra* note 283.

286. U.K. CABINET OFFICE, *supra* note 282, at 28.

287. Rob Waugh, *New British Cyber Defense Force Will Protect Industry—And "If Needed, Strike in Cyberspace"*, WELIVESECURITY (Sept. 29, 2013), http://www.welivesecurity.com/2013/09/29/new-british-cyber-defense-force-will-protect-industry-and-if-needed-strike-in-cyberspace/.

How might the NIST Framework impact the current state of the United Kingdom's cybersecurity policymaking? Given the common legal origins of U.S. and U.K. law, the analysis of negligence jurisprudence in the United States should be informative, if not dispositive, to British firms in weighing whether to invest in considering their compliance with measures or controls advanced by the CPNI or resulting from the Cyber Security Strategy. If such controls are recognized as establishing some grounds for a negligence case, CPNI or another government agency might also be encouraged to develop more detailed cybersecurity standards like those included in the NIST Framework, in which case the Framework may be considered a useful starting point. This outcome may even be more likely in the United Kingdom than in the United States given the lower barriers to standing prevalent in British common law.[288] This might potentially open up the courts to negligence lawsuits, for example, to a greater degree than what has been witnessed to date in the United States. Likewise, the role that U.S. executive agencies are playing in potentially expanding the scope of industries affected by the Framework's standards might demonstrate how the British government could move beyond developing standards relevant only to critical infrastructure. But the biggest looming change for British cybersecurtity policymaking might not be coming from across the Atlantic but from across the English Channel.

2. EU Cybersecurity and NIST

In 2013 an EU cybersecurity directive was proposed requiring companies to harden their cybersecurity to meet EU-developed standards—a development that could cause any firm providing online services in Europe to "fundamentally have to change the way its business operates."[289] Among much else, this regime would require many firms with some nexus to e-commerce to invest in cybersecurity technologies, develop procedures to prove compliance to national and EU regulators, and undertake enhanced cyber risk mitigation measures to better manage attacks.[290] It could also help define a Europe-wide cybersecurity duty of care for covered industry. Given that the size of the EU's economy is comparable, if not larger, than that of the United States,[291] this new EU regime could have substantive

288. *See*, *e.g.*, Jon Owens, *Comparative Law and Standing to Sue: A Petition for Redress for the Environment*, 7 ENVNTL. L. 321, 325–26 (2001) (comparing the "overseas trend in favor of broader standing" with the United State's more restrictive standing doctrine).

289. Ashford, *supra* note 224.

290. *Id.*; *see also Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, at 2–6, JOIN (2013) 1 final (Feb. 7, 2013) (espousing an Internet freedom agenda including universal access, democratic and "efficient multi-stakeholder governance," and setting out goals to achieve "cyber resilience"; to achieve this, the Communication sets out a number of goals, including setting national-level cybersecurity standards, setting up national and regional CERTs, sharing private-sector best practices, and regularly assessing cyber risk—especially for firms operating critical infrastructure—so as to build a "cybersecurity culture"). *But see* Stephen Gardner, *Member States Reportedly Unconvinced on Need for EU Cybersecurity Directive*, BLOOMBERG BNA (June 3, 2013), http://www.bna.com/member-states-reportedly-n17179874317/ (reporting on questions from ministers arising from a mandate approach and noting that "other parts of the world, such as the USA, appear to opt for a more voluntary and flexible approach with regard to cybersecurity standards" and worrying about creating "inconsistencies for companies whose operations span several jurisdictions" (internal quotations omitted)).

291. *See The Economy*, EUR. UNION, http://europa.eu/about-eu/facts-figures/economy/index_en.htm

network effects extending to the many global businesses that operate in EU nations.[292]

What has been less appreciated to date is the impact that the NIST Framework could have on this burgeoning EU cybersecurity policy. According to Francois Rivasseau, the Deputy Head of the EU delegation to the United States, "European officials are considering the [NIST] framework . . . with 'great interest.'"[293] Indeed, Rivasseau went on to note: "The EU is is [sic] trying to set up a European system that 'would basically provide us with the same capabilities or possibilities,'" further mentioning that the NIST Framework should be a "catalyst[]" that "lead[s] to the creation of [cybersecurity] norms."[294] Though formal European endorsement of the NIST Framework has not yet occurred as of writing, there are ongoing discussions about how best to translate the NIST Framework for use by global audiences.[295] Most importantly, many of the Framework's guidelines can be mapped to International Organization for Standardization (ISO) standards (like ISO/IEC 27001:2013 at 32)[296] or Control Objectives for Information and Related Technology 5 (COBIT 5) standards, which were developed by a global industry association.[297] Such standards represent global best practices,[298] meaning that EU adoption can be framed as compliance with international standards that protect global business. As such, these European efforts could be deemed to reinforce the NIST Framework and help to bolster its global impact.

(last visited Apr. 2, 2015) (noting that the EU's economy is larger than the United States's economy in terms of the goods and services that it produces).

292. *See*, *e.g.*, Agustino Fontevecchia, *The Largest U.S. Companies with Big European Exposure*, FORBES (Nov. 9, 2011), http://www.forbes.com/sites/afontevecchia/2011/11/09/defensive-stocks-like-coke-and-ge-far-from-immune-to-europe/ (noting that the EU's slowing economy "will affect U.S. companies with substantial sales exposure to the Old Continent").

293. *EU Eying NIST Framework With 'Great Interest'*, *supra* note 30.

294. *Id.*

295. *See id.* (acknowledging that the EU was considering the NIST Framework, although expressing uncertainty as to whether formal adoption of the Framework would be forthcoming); *see also* Dan Verton, *Global Security Association Helps Translate NIST Framework*, FEDSCOOP (Sept. 15, 2014, 4:41 PM), http://fedscoop.com/global-security-association-helps-explain-nist-framework/ (noting that the Information Security Forum, a U.K. based association, has released a mapping document to help companies understand where their level of compliance with the NIST network falls).

296. The ISO has also developed guidance "to help various industry sectors use the organization's recently updated standards for information technology security." *International Group Drafts Guidance to Encourage Cross-Sector Use of New Security Standards*, INSIDE CYBERSECURITY (Feb. 3, 2014), http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/international-group-drafts-guidance-to-encourage-cross-sector-use-of-new-security-standards/menu-id-1075.html.

297. *See* Press Release, ISACA, New US Cybersecurity Framework Developed by NIST Features COBIT 5 in the Core (Feb. 14, 2014), http://www.isaca.org/About-ISACA/Press-room/News-Releases/2014/Pages/New-US-Cybersecurity-Framework-Developed-by-NIST-Features-COBIT-5-in-the-Core.aspx (noting that the ISACA helped in the development of the NIST Framework, which can be mapped back to "COBIT due to its global relevance and proven industry use").

298. *See*, *e.g.*, Gary Hardy, *Guidance on Aligning CobiT, ITIL, and ISO 17799*, 1 INFO. SYSTEMS CONTROL J. 1, 1–2 (2006), http://www.isaca.org/Journal/archives/2006/Volume-1/Documents/jpdf0601-Guidance-on-Aligning.pdf (stating that ISO and COBIT apply generally to all IT best practices).

3. Voluntary Cybersecurity Frameworks in India

Similar to the EU, and also in 2013, India published its first policy explicitly devoted to protecting critical information infrastructure: the National Cyber Security Policy 2013 (NCSP).[299] The 2013 policy calls for the creation of a National Critical Information Infrastructure Protection Centre (NCIIPC) to protect critical infrastructure,[300] while section IV.A in particular "encourage[s]" all organizations to designate a chief information security officer and "to develop information security policies duly integrated with their business plans and implement such policies as per international best practices."[301] Section IV.B further promotes the adoption of global best practices "in information security and compliance" and "in formal risk assessment and risk management processes."[302] While the 2013 NCSP is mostly devoted to explaining the role that the Indian government should play in protecting critical information infrastructure, the NCIIPC in June 2013 also published Guidelines for the Protection of National Critical Information Infrastructure, which are more targeted to India's private sector but similarly reference the importance of adhering to global standards.[303] However, the NCIIPC lacks a "public face," and its "exact functions" are in doubt,[304] rendering dubious its potential to encourage private sector adoption of its Guidelines.

The NCSP and Guidelines for the Protection of National Critical Information Infrastructure, then, are reminiscent of U.S. and U.K. efforts at establishing voluntary cybersecurity best practices—rather than the more heavy-handed EU approach. But both documents' explicit and numerous references to global standards and best practices create an opportunity for government officials and businesses promoting the NIST Framework to refer to its ISO and COBIT 5 standards references. Moreover, if Europe develops an approach that strengthens the Framework abroad, and given India's common law roots with U.K. jurisprudence, then Indian firms may be more strongly encouraged to implement the NIST Framework or the global standards that it references. In addition, the United States may be encouraging adoption of the Framework or such standards more directly; in December 2013, India's Ministry of Home Affairs conducted its first "homeland security dialogue" with the U.S. government, during which the countries discussed the need to build secure cyber infrastructure and "synchronize" domestic laws with

299. MINISTRY OF COMMC'N & INFO. TECH., NOTIFICATION ON NATIONAL CYBER SECURITY POLICY—2013, FILE NO. 2(35)/2011-CERT-IN (2013) (India) [hereinafter 2013 NCSP]; *Government Releases National Cyber Security Policy 2013*, TIMES OF INDIA, July 2, 2013, http://articles.timesofindia.indiatimes.com/2013-07-02/security/40328016_1_national-cyber-security-policy-power-infrastructure-air-defence-system; *National Cyber Security Policy: An Analysis*, CALIBRE (July 3, 2013), http://thecalibre.in/in-depth-current-affairs/national-cyber-security-policy-an-analysis/072013/?p=3853 [hereinafter Calibre Analysis].

300. Calibre Analysis, *supra* note 299.

301. 2013 NCSP, *supra* note 299, § IV.A(3).

302. *Id.* § IV.B(1), (3).

303. *See* Muktesh Chander, *Protection of National Critical Information Infrastructure*, DEF. & SECURITY ALERT, Oct. 2013, at 54, 55–56, *available at* http://www.dsalert.org/images/web/intro/October_2013_Issue_Intro.pdf (providing general information about CII, detailing international efforts and NCIIPC's efforts to protect CII).

304. *NTRO Would Protect the Critical ICT Infrastructures of India*, CTR. OF EXCELLENCE FOR CYBER SECURITY RESEARCH & DEV. INDIA (Jan. 13, 2014) (on file with author).

global standards.[305] However, it is not only national policymakers who are paying attention to the roll out of the NIST Framework. Perhaps even more involved to date have been companies,[306] both in the drafting and now the global push to establish a global cybersecurity duty of care and contribute to the process of cyber norm creation. It is to that story that we turn to next.

C. How (and Why) the Private Sector is Pushing the NIST Framework Globally

Since its publication in February 2014, the NIST Framework has been heralded by both U.S. industry and government officials as an example of leveraging public-private partnerships to achieve effective cybersecurity policy.[307] Indeed, while drafting the Framework, NIST requested and incorporated feedback from more than 3000 security professionals.[308] Because some U.S. technology companies and industry associations have "invested considerable time and energy toward developing the [F]ramework"—and already believe themselves to be in compliance with the Framework—they are motivated not only to demonstrate their "commitment to using the [F]ramework" but also to promote the Framework.[309] Broader adoption of the Framework may not only lead to greater resilience, enabling continued wide use of companies' information security products, but also enable them to demonstrate a competitive advantage.

Industry association ISACA, which represents 110,000 cybersecurity, governance, and assurance professionals, assisted NIST in the development of the Framework and gave NIST a platform to present at ISACA's North American Computer Audit, Control and Security Conference in April.[310] Likewise, numerous

305. Press Release, Press Info. Bureau, Gov't of India, Ministry of Home Affairs, India-US Homeland Security Dialogue Two Day Conference of Police Chiefs Concludes (Dec. 5, 2013), http://pib.nic.in/newsite/PrintRelease.aspx?relid=101040. Notably, though, what government agency might best develop and implement critical infrastructure best practices remains unclear. In India, the Department of Electronics and Information Technology, Department of Telecom, Ministry of Defense, Ministry of Home Affairs, and National Security Advisor (Prime Minister's Office) are all important stakeholders.

306. *E.g.*, Press Release, IBM, *supra* note 228 (introducing and discussing NIST's new Cybersecurity Framework, in relation to IBM's cybersecurity consulting service).

307. *E.g.*, INFO. TECH. INDUS. COUNCIL, ITI RECOMMENDATIONS TO THE DEPARTMENT OF HOMELAND SECURITY REGARDING ITS WORK DEVELOPING A VOLUNTARY PROGRAM UNDER EXECUTIVE ORDER 13636, "IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY" (2014), *available at* http://www.itic.org/dotAsset/3ed86a62-b229-4d43-a12b-766012da4b1f.pdf; *see also* Ann M. Beauchesne, *Administration Sends Cybersecurity Stakeholders a Positive Message: The NIST Framework Should be Voluntary, Flexible, and Collaborative*, U.S. CHAMBER OF COM. (June 11, 2014), http://www.uschamber.com/administration-sends-cybersecurity-stakeholders-positive-message-nist-framework-should-be-voluntary (discussing industry support for NIST Framework and making sure that pre-existing regulations comply); Matt Thomlinson, *The NIST Cybersecurity Framework: A Significant Milestone towards Critical Infrastructure Resiliency*, MICROSOFT CYBER TRUST BLOG (Feb. 13, 2014), http://blogs.technet.com/b/security/archive/2014/02/13/the-nist-cybersecurity-framework-a-significant-milestone-towards-critical-infrastructure-resiliency.aspx (commending NIST for its work on the Framework and confirming Microsoft's compliance with the NIST Framework).

308. PWC, WHY YOU SHOULD ADOPT THE NIST CYBERSECURITY FRAMEWORK 1 (2014), *available at* http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

309. *See* Beauchesne, *supra* note 307 (noting the measures industry members have done to promote cybersecurity since the Framework's issuing).

310. Press Release, ISACA, *supra* note 297.

industry associations, representing energy, information technology, manufacturing, retailing, and other sectors, joined together in June 2014 to applaud the Framework and demonstrate their continued investment in promoting the Framework.[311] For example, industry association Information Technology Industry Council (ITI) explained that it has recently visited Japan and South Korea, sharing with both countries' governments and business leaders "the benefits of a public-private partnership-based approach to developing globally workable cybersecurity policies."[312] Moreover, "ITI highlighted the [F]ramework as an example of an effective policy developed in this manner, reflecting global standards and industry-driven practices."[313]

As an especially global industry—with significant incentives to drive governments toward adopting and implementing global standards, which would ease their compliance and liability fears—information technology leaders may promote the Framework both via industry associations and more directly, with governments themselves. In addition, the insurance industry may also be incentivized to promote the Framework; AIG in the United States has developed a policy that "supports" NIST's Framework, and in the United Kingdom AIG is working with the U.K. government "to see how it can recognise commitments to meet data hygiene standards and enforce cyber security standards."[314] AIG is seeking to support companies by seeking "accord" with government priorities—and like any global industry, the more those government priorities align, the more straightforward such support to industry customers or compliance with government guidelines.[315]

Looking ahead, the legal standards on which U.S. and other lawmakers settle will be important in shaping firms' cybersecurity investments. According to McAfee, "For many companies, security and risk managementdecisions [sic] are based on strict adherence to compliance standards, not on protecting their intellectual capital."[316] Indeed, another McAfee survey found that compliance with regulation is the "key motivator" for security decisions "in Dubai, Germany, Japan, the U.K., and the U.S.;" only in India and China did surveyed companies more often base security decisions on gaining or maintaining competitive advantages.[317] These surveys point to a trend showing that regulations are critical to firms' security investment decisions, even if businesses at times balk at additional regulatory compliance burdens. Consequently, regulatory intervention can play a vital role in enhancing the public good of cybersecurity. But how much is too much?

Survey data from PwC indicate that since 2008, many firms around the world are increasingly unhappy with cybersecurity regulations. As many as 57% of Indian, 58% of U.S., and 72% of Chinese companies agreed that their regulatory

311. *See* Beauchesne, *supra* note 307 (discussing industry support for NIST Framework and making sure that pre-existing regulations comply).

312. *Id.*

313. *Id.*

314. Jamie Bouloux, *A Broader View*, INSIDER Q., Summer 2014, at 38.

315. *Id.*

316. MCAFEE, UNDERGROUND ECONOMIES: INTELLECTUAL CAPITAL AND SENSITIVE CORPORATE DATA NOW THE LATEST CYBERCRIME CURRENCY 16 (2011) [hereinafter MCAFEE, INTELLECTUAL CAPITAL], *available at* http://www.ndia.org/Divisions/Divisions/Cyber/Documents/rp-underground-economies.pdf.

317. MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 6 (2009), *available at* http://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf.

environments were becoming "more complex and burdensome."[318] A Symantec report argued that "enterprises are buried with [information technology] compliance efforts," ranging from HIPAA to Sarbanes-Oxley,[319] which, among other things,[320] impose severe fines on companies that are found negligent.[321] Some worry that well-meaning regulations may force companies to focus more on compliance than security,[322] and others disagree about the effectiveness of existing regulations and argue that the onus should be on proponents of greater regulation.[323] In a 2007 Computer Security Institute survey, 25% of respondents "strongly disagree[d]" that Sarbanes-Oxley, for example, has improved their organization's information security, and just 12% "strongly agree[d]" that the regulation had positive effects.[324] Similarly, only a third of respondents to a 2011 McAfee survey said that they "feel that compliance regulations imposed by their home country are very useful and aim at the heart of the problem to protect their corporation's intellectual capital."[325] These findings point to the fact that more needs to be done to fashion effective cybersecurity interventions where needed and to streamline compliance so that the focus is on enhancing cybersecurity and not checking boxes—not only in the United States, but also around the world.

318. PRICEWATERHOUSECOOPERS, TRIAL BY FIRE*: WHAT GLOBAL EXECUTIVES EXPECT OF INFORMATION SECURITY—IN THE MIDDLE OF THE WORLD'S WORST ECONOMIC DOWNTURN IN THIRTY YEARS 36 (2010), *available at* http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey 2010_report.pdf.

319. SYMANTEC, STATE OF ENTERPRISE SECURITY: 2010, at 12 (2010), *available at* http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf.

320. *See*, *e.g.*, Health Insurance Portability and Accountability Act of 1996, 18 U.S.C. §§ 669(a), 1347(2) (2012) (imposing penalties for individuals who knowingly and willfully convert to use assets of a health care benefit program or carries or attempts to carry out a plan aimed at defrauding a health care benefit program or otherwise fraudulently obtaining money or property belonging to the health care benefit program in connection with the delivery of benefits); *HIPAA Compliance*, PATIENT PROMPT, http://patientprompt.com/our-technology/compliance-hipaa-pipeda/ (last visited Apr. 3, 2015) (reporting that HIPAA fines can range "up to $250K and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information").

321. *See*, *e.g.*, Michelle DeBarge & Jody Erdfarb, *US State Supreme Court Expands Potential Negligence Liability for HIPAA Violations*, TERRALEX (Mar. 16, 2015), http://www.terralex.org/publication/ p6cc362bb94/us-state-supreme-court-expands-potential-negligence-liability-for-hipaa-violations (addressing a Connecticut Supreme Court decision that allows plaintiffs on state law negligence claims to use HIPAA as setting the applicable standard of care).

322. *See*, *e.g.*, Chandra McMahon, *Is Compliance Security? 5 Tips for Balancing the Two*, LOCKHEED MARTIN (Feb. 18, 2015), http://lockheedmartin.com/us/news/features/2015/is-compliance-security.html (noting that in a recent survey of information technology security leaders, the top priority overall was compliance, not security).

323. *See*, *e.g.*, Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT'L SECURITY J. 39, 82–83 (2011) ("[T]he burden is on proponents of regulation to explain how they determine what is the appropriate level of cybersecurity . . . .").

324. ROBERT RICHARDSON, CSI SURVEY 2007: THE 12TH ANNUAL COMPUTER CRIME AND SECURITY SURVEY 24–25 (2007), http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf; *cf. Enhancing and Implementing the Cybersecurity Elements of the Sector-Specific Plans: Joint Hearing before the Subcomm. on Emerging Threats, Cybersecurity & Sci. & Tech. and the Subcomm. on Transp. Sec. & Infrastructure Prot. of the H. Comm. on Homeland Sec.*, 110th Cong. 87 (2007) (statement of Lawrence A. Gordon, Professor, Robert H. Smith School of Business, University of Maryland) (making the empirical case that Sarbanes-Oxley has actually "created a strong incentive for organizations to increase their cybersecurity investments").

325. MCAFEE, INTELLECTUAL CAPITAL, *supra* note 316, at 8.

CONCLUSION

In February 2013, President Obama issued Executive Order 13636: Improving Critical Infrastructure Cybersecurity, which, among other things, called for public-private partnerships with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop approaches to mitigating cyber threats. Specifically, the Executive Order called on the NIST Director "to lead the development of a framework to reduce cyber risks to critical infrastructure."[326] One commentator has argued that the Framework "represents the best efforts of the administration and . . . industry representatives from the 16 critical infrastructure sectors to work together to address a threat which President Obama has called one of the gravest national security dangers the United States faces."[327] But praise has not been universal. Some have cautioned that the Framework does not go far enough in terms of its scope, influence, and initial impact.[328]

Among the less discussed aspects of the Framework is its potential to shape a cybersecurity standard of care for both domestic critical infrastructure firms and potentially the private sector writ globally. Over time, common law liability, coupled with preferential regulatory treatment to organizations that have implemented the Framework, could pressure companies to conform their cybersecurity practices to this "voluntary" Cybersecurity Framework. Whether this development turns out to be beneficial to individual firms in particular and national and international security generally depends on one's views of the seriousness of the cyber threat, the value of the NIST approach, and the ability of the competitive market to identify and implement cybersecurity best practices absent regulatory intervention. This Article begins this conversation by undertaking an introductory examination of the NIST Cybersecurity Framework, focusing on the Framework's evolution, scope, and potential to shape a reasonable standard of cybersecurity care.

Ultimately, we have argued that, while the final impact that the Cybersecurity Framework may have on shaping a standard of cybersecurity care will not be known for some time to come, the Framework could have a significant impact on common law in the United States as well as on what constitutes a cybersecurity standard of care in other jurisdictions, including the United Kingdom, the EU, and India. However, significant barriers in the United States, such as standing concerns, must be overcome for this to take place. Still, business managers, policymakers, and scholars would do well to note the potential impact of the 2014 NIST Framework as cases referencing it begin to move through the courts.

The NIST Framework begins from a very simple, three-step premise: "Determine if your organization even has a formal security program and understand your security posture. Determine what is protected, whether security practices are adaptable and repeatable, and whether they meet your organization's business and mission needs. Identify gaps and develop a road map for improvement."[329] But,

326. Exec. Order No. 13636, 78 Fed. Reg. 33, 11739, 11740–01 (Feb. 19, 2013).

327. Wallace, *supra* note 15, at 2.

328. *See id.* at 16 (indicating that there are gaps in the cybersecurity framework).

329. William Jackson, *Protecting Critical Infrastructure: A New Approach*, INFORMATIONWEEK (Apr. 21, 2014), http://www.informationweek.com/government/cybersecurity/protecting-critical-infrastructure-a-new-approach/d/d-id/1204577?page_number=2.

while the Framework may in many ways read as "common sense,"[330] it is perhaps its simplicity that is also at the heart of its strength since it, even if it accomplishes nothing else, could create a common matrix for managing cyber risk. The NIST Framework is not the whole answer to the multifaceted cybersecurity problem—nor will it alone fashion international due diligence cyber norms. Government regulators can and will also continue efforts to enhance cybersecurity, including for critical infrastructure, through incentivizing the use of such tools as cyber risk insurance, and the market will similarly continue innovating to better manage cyber risk. However, the era of the "voluntary" cybersecurity framework has begun, and its impact will likely be felt in boardrooms and courtrooms across the United States, and perhaps even the world, for many years to come.

330. *Id.*