2023

A Cybersecurity "Standard of Care" for Critical Infrastructure

John Klaczany

I. INTRODUCTION

The USA PATRIOT Act of 2001[1] defined "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Subsequently, in 2013, President Barack Obama issued Presidential Policy Directive-21 ("PPD-21") which identified sixteen critical infrastructure sectors which included, among others, defense industrial base, commercial facilities, communications, emergency services, financial services, healthcare and public health, information technology, transportation systems, and water and wastewater systems.[2]

We, as Americans, often take critical infrastructure for granted. Stated differently, we generally expect our lights to turn on, water to flow, banking services to work properly, transportation systems to run predictability, etc.[3] When such services fail to work as expected, most of us express frustration amid the inconvenience.[4] However, extreme failures of critical infrastructure could result in much more grave consequences, including severe injury and death.[5] Therefore, it is imperative that critical infrastructure entities take measures to ensure both the physical and cyber security of their systems and processes.[6]

---

[1] 42 U.S.C. § 5195(c)(e), https://www.congress.gov/bill/107th-congress/house-bill/3162.

[2] *Presidential Policy Directive – Critical Infrastructure Security and Resilience*, The White House (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[3] Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 44 FLA. ST. U. L. Rev. 515, 516 (2017).

[4] *Id.*

[5] *Id.*

[6] *Id.*

Over the years, organizations have increasingly relied on digital programs, such as Supervisory Control and Data Acquisition (SCADA), to detect faults, identify inefficiencies, and control their processes.[7] However, such reliance has exposed many entities, especially those in critical infrastructure, to increased risks in the cyber domain.

The Department of Homeland Security ("DHS") has identified cyberattacks on critical infrastructure as "one of the most significant strategic risks for the United States."[8] Moreover, the United States Government Accountability Office ("GAO") has identified cyberthreats to critical infrastructure as a "high-risk area."[9] The reasons for these characterizations are multifold. Critical infrastructure entities are particularly attractive targets for malicious actors due to their prevalence, interdependence, and potential psychological effects on end users.[10]

In fact, the DHS has noted that hostile nation-states, as well as transnational criminal organizations, frequently launch cyberattacks seeking to gain access to control systems in the energy, water, and nuclear sectors.[11] The scope of such attacks is not limited to these areas, however, evidenced by the fact that 83% of critical infrastructure entities reported a cyberattack in 2021.[12] Moreover, for that same year, the Federal Bureau of Investigation's ("FBI") Internet Crime Complaint Center received 649 complaints of ransomware attacks on critical

---

[7] *Id.* at 517.

[8] *Secure Cyberspace and Critical Infrastructure*, U.S. Dep't of Homeland Sec. (last visited Oct. 29, 2022), https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure.

[9] U.S. Gov't Accountability Off., GAO-22-105103, *Critical Infrastructure Protection*, (Feb. 9, 2022), at 7, https://www.gao.gov/assets/720/718988.pdf.

[10] Haber & Zarsky, *supra* note 3, at 521 (particularly noting that hostile actors have a "publicity incentive" to attack critical infrastructure to "enhance their visibility and prestige").

[11] *Secure Cyberspace and Critical Infrastructure*, *supra* note 8.

[12] Mike Burgard, *The Critical Infrastructure Act of 2022 – Cyber Incident Reporting*, Marco (Apr. 4, 2022), https://www.marconet.com/blog/the-critical-infrastructure-act-of-2022-cyber-incident-reporting.

infrastructure organizations.[13] The scope of these ransomware attacks was also widespread, as fourteen of the sixteen critical infrastructure sectors reported that "at least one member" was affected by an attack.[14] These statistics, however, likely reflect the lower bounds of the true numbers. In 2016, the FBI estimated that only ten to twelve percent of cybercrimes are actually reported.[15]

One does not need to scour the news for long to learn about the most recent cyberattack on critical infrastructure. For example, a recent attack on Colonial Pipeline led President Joe Biden to declare a "State of Emergency" amid shortages and soaring gas prices.[16] The pipeline, which transports roughly 2.5 million barrels of oil per day[17], was shut down for days after malicious actors infected its billing and accounting systems with ransomware.[18] The pipeline returned to operation only after the operator paid a seventy-five Bitcoin ransom.[19]

With few exceptions, there has been minimal regulatory intervention requiring private critical infrastructure organizations to adopt cybersecurity practices.[20] In my view, such a regime should persist, as a workable cybersecurity "standard of care" can be formulated sans binding and

---

[13] Federal Bureau of Investigation, *Internet Crime Report 2021*, at 15, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
[14] *Id.*
[15] Tucker Bailey et al., *Cybersecurity legislation: Preparing for increased reporting and transparency*, McKinsey & Company (June 17, 2022), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-legislation-preparing-for-increased-reporting-and-transparency.
[16] Sean Michael Kerner, *Colonial Pipeline hack explained: Everything you need to know*, TechTarget (Apr. 26, 2022), https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.
[17] Kristin L. Bryan, *Federal Court Dismisses Colonial Pipeline Cybersecurity Litigation*, National Law Review (July 13, 2022), https://www.natlawreview.com/article/federal-court-dismisses-colonial-pipeline-cybersecurity-litigation.
[18] Kerner, *supra* note 16.
[19] *Id.*
[20] *See* Haber & Zarsky, *supra* note 3, at 534.

cumbersome regulatory enactments which inhibit competition and expend finite administrative resources.[21]

Thus, below, I propose several theories which could define a cybersecurity "standard of care" for critical infrastructure entities. Firstly, I evaluate whether the threat of fiduciary duty claims against board members is sufficient to define a cybersecurity "standard of care." Secondly, I consider whether negligence liability is an appropriate mechanism to define such a "standard of care," and delve into the workability of defining an entity's cybersecurity "duty of care" by Judge Hand's cost-benefit analysis and the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework. Lastly, I assess whether the recently enacted Cyber Incident Reporting for Critical Infrastructure Act of 2022 could itself define a cybersecurity "standard of care" or, at a minimum, supplement the NIST Cybersecurity Framework for use under the negligence liability theory.

II. PROPOSED THEORIES FOR A CYBERSECURITY "STANDARD OF CARE"

A. Fiduciary Duties

A cybersecurity "standard of care" for critical infrastructure entities can be defined by a director's fiduciary duties to shareholders.[22] Directors owe stockholders a duty of loyalty to act in the best interests of the corporation. Encompassed within this duty of loyalty is the duty of oversight, which requires directors to monitor the corporation's business and verify that acceptable compliance practices are in place.[23] A board may be liable for breach of the duty of

[21] *See* Scott Shackelford, *Why Ignoring the NIST Framework Could Cost You*, HuffPost (May 2, 2014), https://www.huffpost.com/entry/why-ignoring-the-nist-fra_b_5244112; Haber & Zarsky, *supra* note 3, at 542.
[22] Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 318 (2015).
[23] *Id.* at 319.

oversight when either "(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 them from being informed of risks or problems requiring their attention."[24] In the seminal case of *In re Caremark Int'l Inc. Derivative Litigation*[25], the court held that a board must "attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists…"[26] In other words, "a showing of bad faith is a *necessary condition* to director oversight liability."[27]

In *Marchand*, the court held that a board's oversight function must be more aggressively exercised for an organization's "most central consumer safety and legal compliance issues."[28] In that case, the court concluded that the stockholder-plaintiff particularly pled, to survive a motion to dismiss, that the board of Blue Bell Creameries breached its duty of oversight by failing to implement a reasonable food safety monitoring and reporting system.[29] The shareholder's allegations arose after a deadly *listeria* outbreak killed three customers.[30] Specifically, the plaintiff adequately pled that prior to the deadly outbreak, there existed "no board committee that addressed food safety" nor any "schedule for the board to consider on a regular basis … any key food safety risks."[31] The court further noted that enhanced oversight was required as food safety

[24] *Stone v. Ritter*, 911 A.3d 362, 370 (Del. 2006).
[25] 698 A.2d 959 (Del. Ch. 1996).
[26] *Id.* at 970.
[27] *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d 106, 123 (Del. Ch. 2009).
[28] *Marchand v. Barnhill*, 212 A.3d 805, 824 (Del. 2018)
[29] *Id.*
[30] *Id.* at 807.
[31] *Id.* at 822.

was an "essential and mission critical" aspect of the ice cream manufacturer's business.[32] Moreover, the court determined that it was "one of the most central issues at the company."[33]

More recently, in *In re Boeing Co. Derivative Litig.*[34], the court denied the airplane manufacturer's motion to dismiss, concluding that the shareholders had particularly pled that a majority of Boeing's board had breached their duty of oversight.[35] The derivative suit stemmed from the crashes of Lion Air Flight 610 and Ethiopian Airline Flight 302, which occurred in October 2018 and March 2019, respectively, and resulted in the death of all onboard.[36] Upon investigation, the official cause of the crashes was determined to be a faulty external sensor located on the 737 MAX aircraft.[37]

Boeing's shareholders alleged that the board failed to monitor airplane safety risks and take appropriate actions to mitigate those risks.[38] Although noting, citing *Caremark*, that claiming a breach of the duty of oversight is "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment," the court held that shareholders had satisfied their high burden.[39] Specifically, the court determined that the shareholders alleged particularized facts such as that the board did not "regularly allocate meeting time or devote discussion to airplane safety" nor did it employ a committee "charged with direct responsibility to monitor airplane safety."[40] Moreover, the stockholders sufficiently alleged that the board consciously failed to monitor its operations when, upon learning of the crash of Lion Air Flight

---

[32] *Id.* at 824.
[33] *Id*. at 822.
[34] 2021 WL 4059934 (Del. Ch. 2021).
[35] *Id.* at *1.
[36] *Id.* at *2.
[37] *Id.* at *1.
[38] *Id*.
[39] *Id.* at *24 (quoting *In re Caremark Int'l Inc. Derivative Litigation*, 698 A.2d 959, 967 (Del. Ch. 1996)).
[40] *Id.* at *26-27.

610, it failed to immediately "request any information about it from management."[41] Therefore, like in *Marchand*, the Boeing shareholders alleged sufficient factual claims to survive a motion to dismiss. The board failed to properly oversee a "mission critical" aspect of the organization's business, airplane safety.[42]

However, in *Sorenson*, the court held that a stockholder's allegation of breach of the duty of oversight was insufficient to survive a motion to dismiss.[43] In that case, Marriott International, a worldwide lodging provider, was subject to a data breach which exposed the personal information of five-hundred million of its patrons.[44] The cyberattack was committed through the guest reservation database of Starwood Hotels and Resorts, which Marriott had acquired years prior.[45] Principally, plaintiff argued that Marriott's board faced liability for their "conscious and bad faith decision not to remedy Starwood's severely deficient information protection systems post-acquisition."[46] However, the court concluded that although "cybersecurity has increasingly become a central compliance risk deserving of board level monitoring" and that the harms stemming from cyberattacks "increasingly call upon directors to ensure that … appropriate oversight systems [are] in place," the complaint did not meet the "high bar" required to plead a breach of the duty of oversight claim.[47] Specifically, the plaintiff failed to adequately allege bad faith conduct on the part of Marriott's directors for utterly failing to undertake their monitoring and reporting duties or that they "deliberately disregarded" known "red flags."[48] In fact, the

[41] *Id.* at *34.
[42] *Id.* at *26.
[43] *Firemen's Ret. Sys. v. Sorenson*, 2021 WL 4593777 (Del. Ch. 2021).
[44] *Id.* at *1.
[45] *Id.*
[46] *Id.* at *11.
[47] *Id.* at *1-12.
[48] *Id.* at *1-36.

stockholder acknowledged that the board was regularly made aware of cybersecurity risks and mitigation and "engaged outside consultants to improve and auditors to audit corporate cybersecurity practices."[49]

Taking all into account, liability stemming from a breach of a director's duty of oversight could facilitate a cybersecurity "standard of care" for critical infrastructure facilities. As previously noted, critical infrastructure entities are increasingly attractive targets for malicious actors who seek to disrupt operations, reap financial bounties, and sow panic. Thus, as observed in *Marchand* and *In re Boeing*, cybersecurity measures at critical infrastructure facilities can likely be characterized as "essential and mission critical" aspects of the organization. Although the primary function of critical infrastructure entities is to supply their patrons with services, the adequate protection of such processes is of paramount importance so as to ensure efficient and continuous operation. Classifying cybersecurity as a "mission critical" aspect of critical infrastructure entities would thus heighten a board's duty of oversight with respect to the implementation of reasonable cybersecurity measures.

Moreover, the potential for personal liability will likely prompt directors to adopt more robust processes to address cybersecurity. For example, directors would likely ensure that baseline cybersecurity measures exist and that committees or specialized employees, such as a chief security officer, are employed to monitor such systems. Additionally, directors would likely make certain that reports are made to the board when cybersecurity shortcomings are discovered, or potential infrastructure improvements are identified.

[49] *Id.* at *13.

However, defining a cybersecurity "standard of care" by director fiduciary duties is not likely the optimal solution. Firstly, not every critical infrastructure entity has a board of directors or shareholders. Because critical infrastructure sectors are defined broadly by PPD-21[50], many bodies, especially those in healthcare, are generally smaller in size. Requiring these entities to incorporate would arguably be impractical and may pose administrative challenges for the States. Moreover, the economic costs associated with employing cybersecurity professionals may be prohibitively expensive for such smaller firms.

Secondly, as noted in *In re Boeing*, it is quite challenging for shareholders to successfully plead a breach of the duty of oversight. To survive a motion to dismiss, shareholders must show that the directors acted in bad faith which, as observed in *Sorenson*, is challenging. Thus, directors, probably cognizant of these difficulties, might be content in rolling the proverbial dice in electing to retain their entity's deficient cybersecurity reporting structure. Moreover, the difficulty of pleading a breach of the duty of oversight is buttressed by the business judgment rule, which presumes that directors, when making a business decision, act on an informed basis, in good faith, and in the honest belief that the action taken was in the best interests of the company.[51] Thus, when faced with questions surrounding the inadequacy of the critical infrastructure entities' cybersecurity measures, directors could claim that they were instead focused on the organization's profitability. This, in turn, could have the effect of granting directors a form of "immunity" against stockholder fiduciary duty claims.

Lastly, defining the cybersecurity "standard of care" by fiduciary duties effectively sets a cybersecurity "minimum." As previously defined in *Stone*, a board may be liable for breach of

[50] *See Presidential Policy Directive – Critical Infrastructure Security and Resilience*, *supra* note 2.
[51] *Aronson v. Lewis*, 473 A.2d 805, 812 (Del. 1984).

the duty of oversight when directors "utterly failed" to implement any reporting or information systems, or "consciously failed" to oversee its operations. Thus, to satisfy their duty, directors need only demonstrate that *some* reporting systems exist and that they have taken *some* steps to monitor its operations. Defining the "standard of care" in such a way contravenes public policy, as it does not incentivize entities to implement particularly robust cybersecurity regimes.

B. Negligence Liability

A critical infrastructure entity's potential for liability under a theory of negligence can also form a cybersecurity "standard of care." This possibility of suit, in turn, can incentive critical infrastructure organizations to enact, at minimum, "reasonable" cybersecurity measures to protect their systems and processes.

Negligence is conduct that "falls below the standard established by law for the protection of others against unreasonable risk of harm."[52] A *prima facie* case of negligence consists of four elements: (1) plaintiff's sufferance of an injury, (2) the existence of a duty that defendant owed to plaintiff, (3) defendant's breach of that duty, and (4) proof that defendant's breach was an actual and proximate cause of plaintiff's injury.[53] To avoid negligence liability, entities are typically required to adhere to a duty of care that is "reasonable."[54]

Below, I will outline two formulations that can be utilized to define a "reasonable" standard of conduct with respect to an entity's implementation of cybersecurity measures to combat cyberthreats. I will contend that an entity's failure to implement such "reasonable" cybersecurity measures constitutes a breach of their cybersecurity duty. Specifically, I will evaluate whether

[52] Restatement (Second) of Torts § 282 (1965).
[53] *Negligence*, Legal Information Institute (last visited Oct. 30, 2022), https://www.law.cornell.edu/wex/negligence.
[54] Restatement (Second) of Torts § 283 (1965).

the "Hand Formulation" or the NIST Cybersecurity Framework can be effectively employed to define a "reasonable" duty of care. Then, I will discuss the potential challenges of utilizing a negligence theory to define a cybersecurity "standard of care," and argue that its use in the critical infrastructure entity context fundamentally differs from its role in establishing liability against organizations for data breaches.

i. The "Hand Formulation"

Courts, cognizant of the vast array of cyber threats surrounding critical infrastructure organizations, can employ the "Hand Formulation" to establish negligence liability for an entity's failure to implement "reasonable" cybersecurity practices. The "Hand Formulation," a type of cost-benefit analysis, was first outlined by Judge Learned Hand in *United States v. Carroll Towing Co*.[55]

In *Carroll Towing*, the court found the owner of the Anna C, a barge, negligent for failing to employ a bargee during the time of the boat's sinking in New York Harbor.[56] In reaching this conclusion, Judge Hand articulated a blueprint for determining liability in circumstances where risks were foreseeable:

> Since there are occasions when every vessel will break from her moorings, and since, if she does, she becomes a menace to those about her; the owner's duty, as in other similar situations, to provide against resulting injuries is a function of three variables: (1) The probability that she will break away; (2) the gravity of the resulting injury, if she does; (3) the burden of adequate precautions. Possibly it serves to bring this notion into relief to state it in algebraic terms: if the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether B less than PL.[57]

[55] 159 F.2d 169 (2d Cir. 1947).
[56] *Id.* at 174.
[57] *Id.* at 173.

Employing this formulation, the court concluded that the burden of having a bargee aboard the vessel was less than the gravity of injury resulting from a runaway barge multiplied by the probability that the barge would break free unattended.[58]

Although based on sound logic, I am skeptical that the "Hand Formulation" can be effectively utilized to determine whether a critical infrastructure entity is liable for failing to implement "reasonable" cybersecurity measures. Principally, the major shortcoming of Judge Hand's formula stems from its imprecision. Stated differently, the "Hand Formulation" seeks to quantify that which is unquantifiable.

In theory, algebraic expressions are desirable as their use yields transparent and uncontroversial results. Individuals who question the solution generated by an expression need only to identify the unknown variables, determine their explicit values, and perform the calculations, to arrive at a similar result. This self-check function, intrinsic to mathematics, eliminates the opaqueness and oftentimes ambiguous explanations that are associated with subjective reasoning. Mathematical expressions are desired, as the cliché goes, because the proof is in the pudding. However, the "Hand Formulation" strips away this most attractive feature, thereby yielding arbitrary and imprecise results.[59]

Cyberattacks, which seek to disrupt business operations or gain unauthorized access, are foreseeable risks to critical infrastructure entities. However, determining whether an entity was negligent for failing to implement "reasonable" cybersecurity measures, through the "Hand Formulation," is practically an impossible task for courts. Specifically, the inherent arbitrariness

[58] *Id.* at 173-74.

[59] *See U.S. Fid. & Guar. Co. v. Jadranska Slobodna Plovidba*, 683 F.2d 1022, 1026 (7th Cir. 1982) (stating that "though mathematical in form, the Hand formula does not yield mathematically precise results in practice; that would require that B, P, and L all be quantified, which so far as we know has never been done in an actual lawsuit").

associated with assigning numerical values to the formula's variables makes its application unworkable.[60]

In the "Hand Formulation," "B" is characterized as the burden of adequate precautions. In this context, "B" is defined as an entity's burden of implementing cybersecurity measures which would have combated a particular cyberthreat. However, equating a numerical value for "B" is quite complicated. Unlike in *Carroll*, where the court could determine the cost of employing a bargee on the Anna C, it is difficult to quantify the cost of implementing cybersecurity measures that would have prevented a particular cybersecurity breach. This is due, in part, to the varying sophistication of cyberthreats that critical infrastructure entities encounter.[61] Furthermore, the varying technical abilities of the malicious cyber actors and fluid landscape of cyberthreats is unpredictable.[62] Thus, the true value of the cost of implementing an adequate cybersecurity process, which would have prevented the unauthorized access, may be incalculable.

Moreover, assigning a value to "P" requires just as much guesswork. "P" is defined as the probability of the harm. In these circumstances, "P" is specified as the probability that a cyberattack will occur against a particular body. Because of the attractiveness of critical infrastructure entities as targets of cyberattacks, and their interconnectivity to one another, it is fair to assume that "P" will always hover around one.[63] However, an exact determination is

---

[60] *See McCarty v. Pheasant Run, Inc.*, 826 F.2d 1554, 1557 (7th Cir. 1987) (noting that typically "parties do not give the jury the information required to quantify the variables of the Hand Formula," and therefore, "juries may be forced to make rough judgments of reasonableness, intuiting rather than measuring the factors in the Hand Formula"); John C.P. Goldberg, *Twentieth-Century Tort Theory*, 91 GEO. L.J. 513, 551-52 (2003) (contending that the likelihood of an erroneous liability determination is high when the information given for use in the Hand Formula is often "partial and indeterminate" and evaluated by jurors and judges "with no particular expertise").
[61] *See* Haber & Zarsky, *supra* note 3, at 522-23 (noting that the sophistication of cyberattacks range from those like Stuxnet, "which required substantial manpower and expertise to create," to those that "can be deployed by exploiting unsophisticated technological vulnerabilities without using substantive human or economic resources").
[62] *Id*. at 520-23 (noting that the actors behind cyberattacks can take several forms including that of nation-states, terrorists, and teenagers).
[63] Haber & Zarsky, *supra* note 3, at 521.

impossible as only a hostile actor knows of his intentions. Moreover, the calculus may be complicated further when one considers that the likelihood of a cyberattack could vary by critical infrastructure sector.

Lastly, characterizing "L" numerically is complicated. "L" is defined as the severity of the resulting harm. In this analysis, "L" can be characterized as the harm potentially suffered by a critical infrastructure organization due to a cyberattack. Quantifying the harms faced by critical infrastructure entities is difficult, as the variable encompasses a potentially wide range of injuries, varying in severity. For example, consider that a breach of an entity's cybersecurity protocols could lead to an organizational shutdown, thereby halting that entity's operations for hours, days, or indefinitely.[64] Furthermore, the severity of the resulting harm depends on the sophistication of the cyberattack and its orchestrators. Moreover, because critical infrastructure organizations are "so vital" to the United States, the value of "L" must be determined by also considering the harms suffered by the entity's end users.[65] However, these harms may be unquantifiable as a cyberattack can affect a large class of unidentified individuals, each suffering a distinct injury.

In sum, the "Hand Formulation" is, as the phrase goes, just a shot in the dark. An alternative framework is necessary to define a critical infrastructure entity's "reasonable" duty of care.

ii. The NIST Cybersecurity Framework

On February 12, 2013, President Obama issued Executive Order 13636 which established that "it is the policy of the United States to enhance the security and resilience of the Nation's

[64] *See* Kerner, *supra* note 16 (noting that the Colonial pipeline was shut down for days following the ransomware attack).
[65] *See* 42 U.S.C. § 5195(c)(e), *supra* note 1.

critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."[66] Within this document, President Obama called on the Director of the National Institute of Standards and Technology ("NIST"), an agency within the Department of Commerce, to formulate a Cybersecurity Framework to "reduce cyber risks to critical infrastructure."[67] Moreover, the Cybersecurity Framework was to be voluntary and include "consensus standards and industry best practices to the fullest extent possible."[68] Executive Order 13636 did not qualify "best practices," but noted that the phrase encompassed both domestic and international cybersecurity standards.[69] Additionally, Executive Order 13636 noted that the Cybersecurity Framework was designed to be "technology neutral" and provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to assist critical infrastructure entities identify and manage cyber threats.[70] President Obama's declaration noted, however, that the Cybersecurity Framework was not designed to be rigid. Rather, it was to be a living document, where improvements are "addressed through future collaboration" to keep pace with evolving cyberthreats and newfound understanding of those threats.[71] In the Cybersecurity Enhancement Act of 2014[72], Congress formalized NIST's role in facilitating the development of future Cybersecurity Frameworks.

---

[66] *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11,739, 11,739 (Feb. 12, 2013).
[67] *Id.* at 11,741.
[68] *Id*.
[69] *Id*.
[70] *Id*.
[71] *Id*.
[72] *See* 15 U.S.C. § 272(e)(1)(A)(i), https://www.congress.gov/bill/113th-congress/senatebill/1353/text.

Version 1.0 of the Cybersecurity Framework was developed in 2014 after NIST consulted with private sector industry leaders, academics, and government stakeholders.[73] The most recent revisions to the Cybersecurity Framework were outlined in Version 1.1, which was released in April 2018.[74] Presently, NIST is hosting webinars and workshops to gather stakeholder feedback in anticipation of the release of Version 2.0, which is slated to issue sometime within the next few years.[75]

The Cybersecurity Framework is a "risk-based" approach that consists of three primary components: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles.[76] In short, the Framework Core provides a set of actions to reach key cybersecurity outcomes "identified by stakeholders as helpful in managing cybersecurity risk."[77] The Framework Core consists of four interworking parts: Functions, Categories, Subcategories, and Informative References.[78] Broadly speaking, the five "Functions," "Identify," "Protect," "Detect," "Respond," and "Recover," serve to provide an overview of an entity's management of cybersecurity threats.[79] "Categories" and "Subcategories" expand on "Functions" by defining cybersecurity outcomes based on specified activities.[80] Lastly, "Informative References" are "standards, guidelines, and practices" which steer entities to reach their desired outcomes.[81]

---

[73] *Questions and Answers*, National Institute of Standards and Technology (last visited Nov. 4, 2022), https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#proposed.
[74] *Updating the NIST Cybersecurity Framework – Journey to CSF 2.0*, National Institute of Standards and Technology (last visited Nov. 4, 2022), https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20.
[75] *Id*.
[76] Nat'l Inst. of Standards and Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1 2018), at 3, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[77] *Id*. at 6.
[78] *Id*.
[79] *Id.* at 6-8.
[80] *Id.* at 7.
[81] *Id*.

The Framework Implementation Tiers "provide context on how an organization views cybersecurity risk and the processes in place to manage that risk."[82] An entity's sophistication in risk management methods is characterized over four tiers, from lowest to highest: (1) Partial, (2) Risk Informed, (3) Repeatable, and (4) Adaptive.[83] An entity's initial tier selection takes into account several factors including the entity's current risk management practices, the threat environment surrounding the organization, and business constraints.[84] Although organizations are encouraged to improve their standing, "tiers do not represent maturity levels."[85] Rather, tiers are designed to "support organizational decision making about how to manage cybersecurity risk" and set an entity's cybersecurity "tone."[86] When deciding whether to move to a higher tier, management should perform a cost-benefit analysis.[87]

Framework Profiles empower entities "to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities."[88] It is common for organizations to employ a "Current Profile," which describes the outcomes presently being realized, and a "Target Profile," which outlines the outcomes required to meet an entity's risk management objectives.[89] If gaps exist between the profiles, organizations should strive to eliminate them.

---

[82] *Id.* at 8.
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.* at 8-9.
[87] *Id.* at 8.
[88] *Id.* at 11.
[89] *Id.*

The Cybersecurity Framework can be utilized to define "reasonable" cybersecurity measures for critical infrastructure entities.[90] One way to determine "reasonableness" through the Cybersecurity Framework is to require entities to conform to a specified profile tier, such as "repeatable," to be eligible for government contracts related to critical infrastructure jobs. Because of the allure of critical infrastructure entities as targets of cyberattacks, such a scheme ensures that robust cybersecurity measures are in-place and is relatively clear-cut to administer. For jobs which do not require government contracts, for instance, an entity's compliance with the "partial" tier can be characterized as "reasonable." However, as a cost-benefit analysis, defining "reasonableness" in such a way may be contrary to the Cybersecurity Framework's risk-based goals and may also preclude some entities from competing for contracts. An additional way to establish "reasonableness" via the Cybersecurity Framework is through the "Hand Formulation."[91] In other words, an entity could be found negligent if the burden of implementing the Framework, or relevant parts of it, is less than the severity of the resulting harm multiplied by the incident's likelihood of occurring.[92]

Defining "reasonableness" through a critical infrastructure entity's implementation of the Cybersecurity Framework can offer several advantages. Firstly, defining a "reasonable" duty of care by the Cybersecurity Framework is the most favorable from a public policy perspective. Stated differently, characterizing a "reasonable" duty of care by the Cybersecurity Framework raises the overall cybersecurity posture of entities, as the Framework incorporates modern best practices and cybersecurity expertise.[93] This, in turn, ensures that critical infrastructure entities

[90] Shackelford et. al, *supra* note 22, at 340.
[91] *Id.* at 342.
[92] *Id.*
[93] *Id.* at 327.

employ defensive mechanisms which are on par with the most novel cyberthreats. Secondly, expressing "reasonableness" through usage of the Cybersecurity Framework may promulgate an international cybersecurity duty of care.[94] This international implementation, in turn, will strengthen the Framework by including within it foreign best practices and risk mitigation strategies after feedback from international entities is obtained.[95] Thirdly, the Cybersecurity Framework is flexible, and thus, if desired, can complement an entity's existing cybersecurity practices.[96]

However, defining a "reasonable" duty of care by the Cybersecurity Framework may be problematic for a couple of reasons. Principally, for most entities, use of the Cybersecurity Framework is voluntary.[97] Secondarily, entities may be hesitant to utilize the Cybersecurity Framework for financial reasons. In fact, a 2016 study found that despite being characterized as a "best practice" by a vast majority of the surveyed security professionals, more than half of those individuals felt that level of investment required to fully comply with the Cybersecurity Framework was "high."[98] Moreover, the report noted that of the entities utilizing the Cybersecurity Framework, 64% do not comply with its recommendations completely, due in part to its high financial burden.[99] Additionally, entities may be wary of incurring the costs associated

[94] *Id.* at 336-37.
[95] GAO-22-105103, *supra* note 9, at 13 (noting that as of October 2021, the Framework has been downloaded roughly 1.6 million times and translated into Arabic, Bulgarian, Indonesian, and Polish, to name a few).
[96] *See* Shackelford et. al, *supra* note 22, at 336.
[97] *But See Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 Fed. Reg. 22,391, 22,392 (May 11, 2017) (making the NIST Cybersecurity Framework mandatory for Federal Agencies).
[98] *NIST Cybersecurity Framework Adoption Linked to Higher Security Confidence According to New Research from Tenable Network Security*, Tenable (Mar. 29, 2016), https://www.tenable.com/press-releases/nist-cybersecurity-framework-adoption-linked-to-higher-security-confidence-according.
[99] *Id.*

with employing cybersecurity professionals, who would assist will the roll-out and ensure continuing compliance with the Cybersecurity Framework.[100]

However, the benefits derived from an entity's implementation of the Cybersecurity Framework likely outweigh these concerns. With respect to the Framework's voluntariness, defining a "reasonable" duty of care by the Framework makes it *de facto* mandatory. In other words, a critical infrastructure entity's failure to adopt the Framework could be found "unreasonable." Thus, entities would be well advised to implement the Framework as a sort of "liability shield."[101] Moreover, the additional expenses incurred by entities in utilizing the Framework can be rationalized. Firstly, implementation of the Framework could be "less expensive" than the damages an entity may be liable for if it is found negligent. Secondly, an entity's use of the Cybersecurity Framework may prevent costly downtime in the event of a serious cyberattack.

iii. The Potential Challenges of Defining a "Standard of Care" by Negligence

Defining a cybersecurity "standard of care" by negligence, however, may be difficult due to the potential challenges that plaintiffs may encounter when bringing a negligence claim against an entity. To start, plaintiffs will need to demonstrate that they suffered an injury. In the data breach context, demonstrating injury has proven to be a challenge for plaintiffs due to the economic loss doctrine, which prevents recovery for purely economic harms.[102] Therefore, to succeed on the merits of their negligence claim, plaintiffs must show that they suffered a physical injury to their person or property.[103] However, unlike the data breach context,

[100] GAO-22-105103, *supra* note 9, at 27.
[101] Haber & Zarsky, *supra* note 3, at 536.
[102] Scott J. Shackelford et al., *supra* note 22, at 318.
[103] *Id.*

demonstrating physical harm stemming from a critical infrastructure entity's lack of cybersecurity measures may be manageable.[104] Consider, for instance, a cyberattack on a critical infrastructure entity that provides individuals with drinking water. Suppose further that this attack shuts down the organization's operations for days. In this scenario, the affected populations' inability to obtain drinking water from the organization could attribute to serious physical injuries, thereby satisfying the "injury prong."[105] Furthermore, in addition to "injury," plaintiffs will need to demonstrate that an entity's failure to implement cybersecurity measures caused her injury. Although this determination would be fact-specific, plaintiffs could likely meet this requirement. In all, however, the uncertainty of a plaintiff establishing a *prima facie* case may enable entities to escape negligence liability.

C. The Cyber Incident Reporting for Critical Infrastructure Act of 2022

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCA") was signed into law by President Biden as part of the Consolidated Appropriations Act of 2022.[106] The purpose of the Act is to provide the Cybersecurity and Infrastructure Agency ("CISA") with a greater understanding of the cyberthreats facing critical infrastructure entities in the United States. With such information, CISA can "rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly

[104] *Id*. at 343 (noting that one may overcome the economic loss doctrine with a showing that an entity's "lax security measures" produced "kinetic effects impacting the health, safety, and welfare of individuals").
[105] Dana Sparks, *Can dehydration lead to serious complications?*, Mayo Clinic (Sept. 12, 2015), https://newsnetwork.mayoclinic.org/discussion/dehydration-can-lead-to-serious-complications/ (noting that the complications stemming from severe dehydration can include swelling of the brain, seizure, kidney failure, or death).
[106] H.R.2471 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2022, H.R.2471, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

share that information with network defenders to warn other potential victims."[107] CIRCA's enactment will drastically alter the cyber reporting landscape, as prior reporting was voluntary.[108]

CIRCA will require "covered entities" to report "covered cyber incidents" to CISA within 72 hours of such an incident.[109] To qualify as a "covered cyber incident," the event must be "substantial" and generally attribute to either a loss of system integrity or confidentiality, be disruptive to industrial operations, or have a serious impact on the safety and resiliency of such processes.[110] The reports provided to CISA must, at a minimum, contain a description of the cyber incident as well as the name and contact information of the entity affected by such incident.[111] Where applicable, the reports must also include a description of the vulnerabilities exploited, the cybersecurity measures that were in place at the time of the incident, identifying information of the actors that the entity reasonably believes to be responsible for the incident, and a description of the category of information that was accessed by the unauthorized individuals.[112] Critical infrastructure entities will also be required to submit supplemental reports to CISA if "substantial new or different information becomes available."[113]

---

[107] *Statement From CISA Director Easterly On the Passage of Cyber Incident Reporting Legislation*, Cybersecurity & Infrastructure Security Agency (Mar. 11, 2022), https://www.cisa.gov/news/2022/03/11/statement-cisa-director-easterly-passage-cyber-incident-reporting-legislation.

[108] *Congress Passes Cyber Incident Reporting for Critical Infrastructure Act of 2022*, Sidley (Mar. 21, 2022), https://www.sidley.com/en/insights/newsupdates/2022/03/congress-passes-cyber-incident-reporting-for-critical-infrastructure-act-of-2022.

[109] Pub. L. 107–296, title XXII, § 2242, as added Pub. L. 117–103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1042.

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] *Id.*

The Act will also obligate "covered entities" to report ransomware payments within 24 hours of such transactions.[114] The requirements for reports pertaining to ransomware payments are like those described above.[115]

However, critical infrastructure entities who will be obligated to report cyber incidents and ransomware payments to CISA are not without protections. For example, the information obtained by the agency will be unavailable for use in a regulatory action against any covered entity.[116] Moreover, CISA will redact the identifying information from reports when apprising other critical infrastructure entities of the recent cyber incident, which may continue to pose risks to other organizations.[117] The reports will also be exempt from Freedom of Information Act disclosure.[118]

Although CIRCA was signed into law on March 15, 2022, the incident reporting requirements will require time to take effect. Specifically, CIRCA sets forth that CISA's Director must publish a notice of proposed rulemaking within 24 months of the Act's enactment.[119] Subsequently, a final rule must be promulgated no later than 18 months after publication of the proposed rule.[120] The pending rulemaking will provide clarity on several aspects of CIRCA, including the definition of "covered entities" and "covered cyber incidents," as well as the precise form the reports should take.[121]

---

[114] *Id.*
[115] *See id.*
[116] Pub. L. 107–296, title XXII, § 2245, as added Pub. L. 117–103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1051.
[117] *Id.*
[118] *Id.*
[119] Pub. L. 107–296, title XXII, § 2242, as added Pub. L. 117–103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1042.
[120] *Id.*
[121] *Id.*

In the context of data breaches, commentators have argued that state data breach notification laws, which require data custodians to notify customers affected by a breach, establish a data security "standard of care."[122] The reasons that such statutes establish a "standard of care" are twofold. Firstly, the costs associated with notifying affected customers of a breach are great.[123] For example, data custodians who were the targets of a cyberattack must expend significant time and economic resources to retain legal counsel and communicate with affected individuals.[124] Moreover, entities may elect to provide affected customers with remedies such as identify theft insurance. Thus, to minimize the effect that these potential expenditures would likely have on an entity's "bottom line," data custodians enact proactive data security mechanisms. Secondly, the threat of reputational damage stemming from data breach notification laws has likely attributed to data custodians implementing more robust data security measures.[125] After receiving a notification that their personally identifiable information had been comprised, affected customers likely express their displeasure to friends, family, and others. Such negative publicity may, in turn, cause consumers to look elsewhere for their needs.[126]

I am skeptical that CIRCA, by itself, can establish a cybersecurity "standard of care" for critical infrastructure entities. Firstly, the costs associated with notification are minimal. As compared to data breach notification statutes, where entities are required to report breaches to potentially thousands of individuals, CIRCA requires only that notification be given to CISA. Secondly, critical infrastructure entities face minimal reputational concerns stemming from the notification of a cyber incident or ransomware payment to CISA. Although CISA is aware of the

[122] William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1152-53 (2019).
[123] *Id.* at 1152.
[124] *Id*.
[125] *Id.* at 1153.
[126] *Id*.

identity of the critical infrastructure entity reporting the cyber incident, information given to third parties regarding the cyberattack does not contain this identifying information. Rather, the "useful information" forwarded to other parties will likely contain only the information required to enact pressing cybersecurity patches or identify novel threats. Thus, the reputational damage stemming from reporting cyberattacks will be minimized, as the public will likely be unable to identify the subject of the cyberattack. However, in the age of whistleblowers, investigative journalism, and leaks, it may be entirely possible for the public to identify the victim of the cyberattack. Thus, the threat of reputational harm to critical infrastructure entities cannot be categorically ruled out. In turn, developing a "standard of care" from CIRCA may be possible.

Lastly, defining a cybersecurity "standard of care" by CIRCA would not promote uniformity. Even if a "standard of care" could be deduced by CIRCA, not every critical infrastructure entity has the same level of reservations with respect to costs or reputational concerns. One can argue that competition in some critical infrastructure sectors, particularly when considering geography, is lacking. Thus, some entities in critical infrastructure may not fear the ramifications of reputational harm, as their consumers lack alternative sources for vital goods or services. Therefore, a cybersecurity "standard of care" developed from CIRCA would vary between critical infrastructure sectors and geography, which does not promote the benefits derived from a national regime.

CIRCA may, however, be useful in defining a cybersecurity "standard of care" in conjunction with, or as a supplement to, the NIST Cybersecurity Framework.[127] Because CIRCA

[127] *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 317 (2014) (arguing for a "hybrid form of regulation" which incorporates "directive regulation" with "management-based regulatory delegation"). The above proposal for defining a cybersecurity "standard of care," roughly mimics Thaw's hybrid form of regulation by combining CIRCA, a quasi-form of directive regulation, with the NIST Cybersecurity Framework, a type of management-based regulatory delegation.

will compel critical infrastructure entities, who were the subject of a cyberattack, to report to CISA, the available information relating to novel cyberthreats will grow. This, in turn, will facilitate real-time information sharing between CISA and the sixteen critical infrastructure sectors, and will catalyze the development of robust cybersecurity defenses to combat the most unique cyberthreats. Since cyber incident reporting was voluntary prior to CIRCA, CISA and critical infrastructure entities will now be able to utilize this "new" information to track the recent trends and mechanisms utilized by malicious actors. This information gathered from the Act's required disclosure can then be used to strengthen future versions of the Cybersecurity Framework. A dynamic Framework is highly desired, considering the ever-evolving battleground that is cyberspace. The development of cybersecurity defenses must outpace the evolution of cyberthreats.

III. CONCLUSION

Society's reliance on the efficient and continuous operation of critical infrastructure entities cannot be understated. Because of ever-increasing cyber threats, critical infrastructure organizations must be held accountable for their use of inadequate cybersecurity mechanisms. *Ex post* liability is the superior method for holding these entities accountable, as traditional regulatory enactments are onerous, costly, and disincentive competition. Therefore, clearly defining a cybersecurity "standard of care" is crucial to ensure that entities enact preemptive cybersecurity measures.

Fiduciary duties are not likely the best mechanism for defining a cybersecurity "standard of care" since not all critical infrastructure entities employ a board of directors. Moreover, successfully pleading a breach of a director's duty of oversight is extremely difficult. Furthermore, even if one assumes that cybersecurity measures are "mission critical" aspects of

critical infrastructure entities, a "standard of care" developed from fiduciary duties contravenes public policy, as such a standard does not incentive the implementation of particularly robust cybersecurity practices.

Additionally, negligence theory can be utilized to define a cybersecurity "standard of care." Although the "Hand Formulation" is a mechanism by which to define an entity's liability for failing to employ "reasonable" cybersecurity measures, it is not the optimal one. The variables encompassing Judge Hand's cost-benefit formula are incapable of precise numerical characterization, which thus, attributes to arbitrary liability determinations. Therefore, a critical infrastructure entity's implementation of the NIST Cybersecurity Framework is the preferred mechanism by which to define a "reasonable" duty of care. Defining "reasonableness" by the Cybersecurity Framework offers several advantages including the formulation of a robust "standard of care," potential for international use, and flexibility. However, defining a "reasonable" duty of care by the Cybersecurity Framework poses challenges to entities because of its voluntariness and cost. Lastly, the common barriers that exist for plaintiffs pursuing negligence claims, specifically "injury in fact" and "causation," can likely be adequately addressed in the critical infrastructure entity context.

Lastly, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 is likely not the optimal framework for developing a cybersecurity "standard of care" as the financial and reputational concerns intrinsic to notice requirements are not present in an entity's report to CISA. However, the Act may have use in supplementing the NIST Cybersecurity Framework.