YALE LAW & POLICY REVIEW

Locking Down "Reasonable" Cybersecurity Duty

*Charlotte A. Tschider**

Following a data breach or other cyberattack, the concept of "reasonable" duty, broadly construed, is essential to a plaintiff's potential causes of action, such as negligence, negligence per se, breach of contract, breach of fiduciary duty, and any number of statutory claims. The impact of an organization's discretionary choices, such as whether to take specific security steps for a system, may result in potential risk to an individual, another organization, or the organization itself. Although organizations regularly engage in cybersecurity risk analysis, they may not understand what practices will be considered reasonable in a court of law and are therefore unable to anticipate downstream legal issues. Attorneys are likewise unable to confidently advise their clients on how to best avoid liability. This Article examines, in detail, potential sources for reasonably defining duty, and how organizations and attorneys might consider legal duty through the lens of cybersecurity risk management.

Specifically, I call for a two-part cybersecurity duty analytic model: static, or objective duty informed by industry practices, and dynamic, or subjective duty informed by situational risk. For some doctrinal areas, this may work primarily as an analytic model, while for others, such as negligence, this could be formalized as a test. By offering a model for analyzing what cybersecurity duty ought to be, organizations can adequately understand how potential legal risk might be evaluated in order to implement practices that protect

* Charlotte A. Tschider is an Assistant Professor at the Loyola University Chicago School of Law. I would like to thank the many people who have shaped the creation of this Article, offering guidance and draft reviews along the way, including Gus Hurwitz, David Thaw, Derek Bambauer, William McGeveran, Lauren Scholz, Blake E. Reid, and Sharon K. Sandeen. I would like to especially thank Steven M. Bellovin and participants of the 2020 Privacy Law Scholars Conference for their thoughts on the topic, my exceptionally talented research assistant, Annalisa Kolb, for her analysis of cases that led to this paper, and the editorial board of the Yale Law & Policy Review, especially Ali Fraerman, for excellent recommendations on edits to this Article.

would-be plaintiffs and avoid liability. Moreover, courts can use this model to determine whether organizations have made decisions that avoid real, foreseeable risk to the plaintiff. Indeed, amidst an increasing frequency and diversity of cyberliability claims, legal analysis informed by actual risk analysis ensures that reasonable, rather than perfect, cybersecurity practices can be developed precedentially over time.

INTRODUCTION 77

PART I: DEFINING CYBERSECURITY DUTY 85
A. What is Cybersecurity Duty? 86
B. Statutory Duty 88
1. Private Rights of Action 89
2. Duty to Execute a Contract 91
3. Federal Administrative Enforcement 92
C. Fiduciary Duty 94
D. Common-Law Negligence Duty 96
E. Contractual Duty (Obligation) 99

PART II: SOURCES OF REASONABLE DUTY 102
A. Reasonable Duty in Case Law 102
B. Federal and State Sources of Cybersecurity Legal Duty 104
C. Industry Standards as a Source for Cybersecurity Duty 106
1. The Development of Industry Standards for Cybersecurity . 107
2. The Purpose of Industry Standards in Cybersecurity 110
D. Leveraging Industry Standards to Determine Reasonableness 112
1. Risk Assessment 113
2. Risk Decisioning 115

PART III: WHY CYBERSECURITY LAW NEEDS REFERENTIAL STANDARDS OF ACCEPTABLE BEHAVIOR 117
A. Two-Part Duty Analyses 118
1. Statutory Requirements & Administrative Enforcement 119
2. Administrative Enforcement of Broad Duties 124
3. Fiduciary Duties 125
4. Contractual Duties (Obligation) 126
5. Negligence & Negligence Per Se 130
B. Reasonableness and Foreseeability 132
C. Practicing Reasonableness 135
1. Downstream Static and Dynamic Duty 135
3. Identifying Vulnerabilities and Assessing Risks 137

PART IV: INFORMING DUTY 140
A. Static Duty *141*
B. Dynamic Duty *142*
C. Common Law Duty *143*
1. Fiduciary Duties 144
2. Negligence and Negligence Per Se 145
3. Contracts 145
D. Statutory Cybersecurity *146*
E. Duty Inquiries in the Legal Process *147*
1. Statutory Duty 147
2. Fiduciary Duty 147
3. Contractual Duty 149
4. Negligence Duty 149

CONCLUSION 150

INTRODUCTION

Not all organizations that experience a cyberattack are bad actors. In late 2021, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an alert regarding a single sign-on and password management solution, ManageEngine ADSelfService Plus.[1] From September through October 2021, malicious actors had engaged in an ongoing assault on the solution, eventually compromising at least nine global entities.[2] In these attacks, the attacker used a number of different tools and steps demonstrating significant aptitude and persistence in gathering credentials for purposes of exfiltrating, or removing, sensitive data from target systems.[3] Sometimes known as advanced persistent threats, these types of

1. Robert Falcone, Jeff White & Peter Renals, *Targeted Attack Campaign Against ManageEngine ADSelfService Plus Delivers Godzilla Webshells, NGLite Trojan and KdcSponge Stealer*, UNIT 42 (Nov. 7, 2021, 6:00 PM), https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge [https://perma.cc/R2N6-RMF7].
2. *Id.*
3. *Id.*

attacks are often capable of compromising organizations that employ strong cybersecurity controls.[4]

Technology advancement has introduced many new threats. The emergence of mainstream Artificial Intelligence (AI) has similarly created the potential for innovation and efficiency gains, transforming a number of sectors, but has also created the potential for highly sophisticated cyberattacks.[5] Although AI can be targeted in cyberattacks, it can also be used to perpetuate attacks. A notable example is the 2018 Emotet trojan, contemporary malware that creates a spreading module within a network, making it difficult to contain while simultaneously locking users out of their accounts.[6] These sophisticated attacks may be very difficult to defend, even for experienced, well-resourced organizations with a high degree of cybersecurity maturity. [7]

The cybersecurity threat landscape is evolving, including what assets might be compromised and for what purposes. Regulations incorporating cybersecurity requirements focus primarily on data security, or *protecting* data,[8] and primarily ensure data are not exposed to untrusted organizations and people.[9] However, the contemporary threat landscape includes attacks designed to compromise the integrity of data essential for organizational

4. Mark Stone, *What is Advanced Persistent Threat? Explaining APT Security*, AT&T CYBERSECURITY (Oct. 1, 2021), https://cybersecurity.att.com/blogs/security-essentials/advanced-persistent-threat-explained [https://perma.cc/A3YW-5YAS].

5. *Artificial Intelligence in Cybersecurity: AI Cyberattacks, Securing Your Ecosystem with AI, and More*, [X]CUBE LABS (Sept. 23, 2021), https://www.xcubelabs.com/blog/artificial-intelligence-in-cybersecurity-ai-cyberattacks-securing-your-ecosystem-with-ai-and-more [https://perma.cc/7J2B-G86L].

6. Threat Hunter Team, *The Evolution of Emotet: From Banking Trojan to Threat Distributor*, SYMANTEC (July 18, 2018), https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor [https://perma.cc/WA8S-65Z7].

7. Tom Burt, *Microsoft Report Shows Increasing Sophistication of Cyber Threats,* MICROSOFT (Sept. 29, 2020), https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats [https://perma.cc/WD55-P8T6].

8. Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 995 (2018).

9. The focus on data *protection* originated in large part with laws that regulated the handling of personal information, anticipating that the biggest threats at that time involved stealing personal information and selling it for profit.

operations, as well as threats like ransomware, which make entire systems containing essential data and processes unavailable until the organization pays a "ransom."[10]

Despite the prevalence of sophisticated cyberattacks like advanced persistent threats,[11] eighty percent of cyberattacks are reasonably preventable.[12] The cost of cybercrime for organizations has increased over time, from $523 billion in 2018 to $945 billion in 2020, including legal costs.[13] In fact, for data breaches specifically, the average cost has increased ten percent between 2020 and 2021 to an average of $905 million in the U.S., with cyberkinetic (cyberattacks with some physical impact) and ransomware attacks amongst the most expensive.[14] Cyberattacks and data breaches are increasingly costing organizations money and lost

10. Alison Grace Johansen, *What is Ransomware and How to Help Prevent Ransomware Attacks*, NORTON US (Nov. 23, 2021), https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html [https://perma.cc/M6MU-DJPK]; *Ransomware Guide*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY 2, 4 (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf [https://perma.cc/KJ46-USHN].

11. *See* Suzannah Hastings, *Advanced Persistent Threat (APT): How to Protect Your Organization from Lurking APTs*, FARONICS (July 6, 2017), https://www.faronics.com/news/blog/advanced-persistent-threats-how-to-protect-your-organization-from-lurking-apts [https://perma.cc/7KQW-N57W]. Not only are some high-complexity attacks nearly impossible to defend, but electronic crime has increased significantly in the past two years, largely perpetuated by cyberattackers either permitted or financed by nation states. *2021 Global Threat Report*, CROWDSTRIKE 7, 12-13 (2021), https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf [https://perma.cc/9TCV-4VAJ]. Moreover, such attacks affected a wide variety of industries, even industries not typically regulated statutorily. *Id.* at 22.

12. *Interview: 80 Per Cent of Cyber Attacks are Preventable According to Cybercrime Expert,* AIRMIC (Jan. 9, 2017, 1:22 PM), https://www.airmic.com/news/guest-stories/interview-80-cent-cyber-attacks-are-preventable-according-cybercrime-expert [https://perma.cc/S4FY-TD4N].

13. *Total Cost of Cybercrime*, PARACHUTE (Feb. 23, 2021), https://parachute.cloud/cyber-attack-statistics-data-and-trends/total-cost-of-cybercrime [https://perma.cc/TN54-KAE2].

14. *Cost of a Data Breach Report 2021*, IBM SECURITY 4, 8 (2021), https://www.ibm.com/security/data-breach [https://perma.cc/2R24-MUN4]. The health sector still leads in the cost of data breaches, at an average $9.23 million per breach (an increase of nearly 30%). *Id.*

opportunities.[15] These impacts also affect consumers,[16] shareholders,[17] and organizational customers.[18]

But when are security-conscious organizations simply outmatched in high-complexity attacks and when are organizations to blame for poor cybersecurity practices? There is no "perfect" or "unbreakable" cybersecurity,[19] but when an organization experiences a cyberintrusion or data breach, the prevailing attitude, regardless of factual circumstances, is that the organization failed when the organization is also a victim of a crime. In fact, the cybersecurity world has shifted to the language of "cyber resilience," which is "the ability to continuously deliver the intended

15. The cost of lost business for an organization experiencing a cyberattack, including a data breach, is an average of $1.59 million. *Id.* at 16. And these costs are associated with organizations that can stay in business. Small businesses go out of business at a rate of sixty percent after a data breach occurs. *See* Robert Johnson III, *60 Percent of Small Companies Close Within 6 Months of Being Hacked*, CYBERCRIME MAG. (Jan. 2, 2019), https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked [https://perma.cc/W6MF-6CAM].

16. *See* Vyacheslav Mikhed & Michael Vogan, *How Data Breaches Affect Consumer Credit*, 88 J. BANKING & FIN. 192, 195 (2017) (describing the various effects on consumers following a data breach in the financial sector).

17. *See* Brad Rudisail, *How Cyberattacks Affect Share Holders and Board Members*, TECHOPEDIA (Mar. 19, 2018), https://www.techopedia.com/how-cyberattacks-affect-share-holders-and-board-members/2/33204 [https://perma.cc/24DT-96FP]. *See generally* Christos A. Makridis, *Do Data Breaches Damage Reputation? Evidence from 45 Companies Between 2002 and 2018*, 7 J. CYBERSECURITY 1 (2021) (describing how the largest data breaches negatively affect reputation, while others result in positive long-term growth, suggesting that regulatory guidance does not incentivize cybersecurity investment).

18. *See* Giora Orner, *The Top 5 Third-Party Data Breaches of 2020*, PANORAYS (June 4, 2020), https://panorays.com/blog/the-top-5-third-party-data-breaches-of-2020 [https://perma.cc/U6Q7-4NW7]; *see also 51% of Organizations Have Experienced a Data Breach Caused by a Third-Party*, SEC. MAG. (May 7, 2021), https://www.securitymagazine.com/articles/95143-of-organizations-have-experienced-a-data-breach-caused-by-a-third-party [https://perma.cc/N833-93ZS].

19. *See* George Finney, *The Illusion of Perfect Cybersecurity*, FORBES (Mar. 27, 2018, 8:45 AM EDT), https://www.forbes.com/sites/forbestechcouncil/2018/03/27/the-illusion-of-perfect-cybersecurity [https://perma.cc/N833-93ZS].

outcome despite adverse cyber events."[20] This changing model illustrates the need to anticipate that cyberattacks will continue and cannot be fully avoided.[21] While reputational damage may be unavoidable, public reputation should not be the legal measure of culpability.[22]

A complicating factor is the inability of exogenous players to avoid harm. When a cyberattack or data breach occurs, individuals,[23]

20. Fredrik Björck, Martin Henkel, Janis Stirna & Jelena Zdravkovic, *Cyber Resilience – Fundamentals for a Definition*, *in* 1 NEW CONTRIBUTIONS IN INFORMATION. SYSTEMS & TECHNOLOGIES 311-312 (Álvaro Rocha, Ana Maria Correia, Sandara Costanzo & Luís Paulo Reis eds., 2015). Cyber resilience accepts that cyberattacks are inevitable and instead focuses on how to defend attacks, maintain function even when attacks may be successful, and how to respond to such attacks.

21. Keri Pearlson, Brett Thorson, Stuart Madnick & Michael Coden, *Cyberattacks Are Inevitable. Is Your Company Prepared?*, HARV. BUS. REV. (Mar. 9, 2021), https://hbr.org/2021/03/cyberattacks-are-inevitable-is-your-company-prepared [https://perma.cc/7LLX-VG4H].

22. For this reason, some scholars have proposed avoiding, at least for torts, determinations of reasonableness completely by recognizing strict liability in these cases. When an organization or individual engages in statutorily identified activities and someone is injured and the proximate cause of such injury is engagement in these activities, courts may find the defendant liable without establishing breach of any reasonable duty. Strict liability is statutorily defined precisely because declaring a party liable without establishing breach of any reasonable duty puts a significant amount of responsibility on the organization to engage in extremely aggressive risk avoidance practices. *See* Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1543 (2017). This is largely why most strict liability centers around inherently dangerous activities, where exceptional care is needed to dramatically reduce potential injuries. Scholars have argued that strict liability may be a good fit for cyberattacks and data breaches due to the recent development of cyberrisk and cyberliability insurance policies that can offset cost and the difficulty of ascertaining reasonable duty. *Id*. at 1522-23 (describing cyberliability as a "classic case" for strict liability); *see also* Benjamin C. Dean, *An Exploration of Strict Products Liability and the Internet of Things*, CTR. FOR DEMOCRACY & TECH. (Apr. 2018), https://cdt.org/wp-content/uploads/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf [https://perma.cc/8WHU-C2QH] (positioning strict products liability for Internet-connected products). This author is operating within the existing legal regime to make it more effective and makes no comment on the advantage or disadvantage of strict liability as an alternative tort regime.

23. The term "individual" is used to represent individual human persons, who may be consumers, employees, or fill any other relevant role.

shareholders,[24] and customers[25] may be harmed despite having very little ability to influence or control practices that might reduce risk to them.[26] These parties likely lack the influence or control over an organization complying with a statute, cannot fully verify protective third-party contractual terms and preventative risk management activities,[27] and cannot guarantee the organization is employing preventative cybersecurity controls.[28] This inability stems from a lack of transparency with respect to internal cybersecurity practices because practices are often kept confidential from outside parties.[29] In short, these parties may be harmed in long-lasting and irreversible ways but cannot avoid injury.[30]

24. Shareholders may be individual human persons or organizations that purchase shares of a publicly traded company.

25. Other organizations, as described in this Article, are third parties to the organization experiencing the cyberattack or data breach. These may be clients or customers of the organization, or they may be third parties providing service to the affected organization.

26. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 747-753 (2018); Ioannis Agrafiotis, Jason R. Nurse, Michael Goldsmith, Sadie Creese & David Upton, *A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate*, 4 J. CYBERSECURITY 1, 7-8 (2018).

27. Business organizations may comparatively have some ability to influence cybersecurity practices, through third-party assessments, review of internal policies, and validation of external certifications prior to contracting; but these activities only provide some idea of the program in place, not the "stress-tested" version of the security program. Even so, there is only so much an organization can know about its contracting party at the moment of contracting.

28. Indeed, these parties may have great difficulty engaging in caveat emptor strategies to protect themselves because most practices cannot be shared outside an organization, lest they equip attackers with helpful information. Some organizations may not even have the information to share because they do not understand what their third parties may be doing from a security perspective. *See* Charlotte A. Tschider, *The Consent Myth: Improving Choice for Patients of the Future*, 96 WASH. U. L. REV. 1505, 1525-26 (2019).

29. *Id.*

30. *See* Solove & Citron, *supra* note 26, at 757.

Harmed parties often seek some legal remedy.[31] However, courts have not—and largely are not—prepared to decide cases involving a data breach on the merits. There are three primary reasons: 1) many courts have encountered standing issues related to whether harms claimed meet standing requirements (for example, a 12(b)(1) defense), which means that some cases will not be examined fully; 2) where many courts could examine reasonable duty, parties settle prior to a thorough analysis; and 3) even where courts have acknowledged some harm and parties have not yet settled, courts defer to general discussion rather than examining the contours of cybersecurity duty within the case. Scholars have written extensively on standing,[32] and settlement is often a combination of cost and legal outcome uncertainty.[33]

---

31. Stephen Wu, *Data Security Breaches: A Legal Guide to Prevention and Incident Response*, SILICON VALLEY L. GRP., https://www.svlg.com/data-security-breaches-a-legal-guide-to-prevention-and-incident.html [https://perma.cc/8WHU-C2QH].

32. Article III standing in federal court (which is often the court in which diversity-based and class-action cases are heard) is an initial consideration for courts and is usually considered before the merits of the case, including the claims based on the prima facie requirements. Standing requires an injury be claimed, regardless of the type of claim (contractual, tort, statutory non-compliance, or shareholder liability), and many of the injuries claimed are not a good fit for existing interpretation according to the Supreme Court of the United States. This has introduced a substantial roadblock for parties seeking a court to hear the case on the merits. *See* Solove & Citron, *supra* note 26, at 754-55; *see generally*, Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 452-55 (2017) (describing how the Supreme Court handled discussion of statutory harms when such harms challenge the notion of concrete, particularized, and non-speculative injury). As Wu explains, "When courts deny standing in these cases on the basis of the injuries being insufficiently concrete, they are not deciding whether the cases are ones that concern individual rights, but rather deciding the substantive content of those rights." *Id.* at 458.

33. Future (potential) injury has historically been most difficult for courts to recognize meeting Article III standing, yet some courts are recognizing future injury. *See*, *e.g.*, Rowe v. UniCare Life & Health Ins. Co., No. 09 C 2286, 2010 WL 86391, at *4-6 (N.D. Ill. Jan. 5, 2010); *In re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 527 (N.D. Ill. 2011); *In re* Adobe Sys., Inc. Priv. Litig., 66 F. Supp. 3d 1197, 1212 (N.D. Cal. 2014); Corona v. Sony Pictures Ent., Inc., No. 14-CV-09600 (RGK), 2015 WL 3916744, at *3-4 (C.D. Cal. June 15, 2015); Walker v. Boston Med. Ctr. Corp., SUCV201501733BLS1, 34 Mass. L. Rptr. 387,

This Article proposes a solution for cases that may survive standing inquiries and proceed in court analysis. This solution specifically offers instruction on how courts can determine "reasonable" cybersecurity duty and why they should.[34] This model can also be adapted to other legal entities

390 (Mass. June 7, 2017); *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, at *11 (N.D. Cal. May 27, 2016); *In re* The Home Depot, Inc., Customer Data Sec. Litig., No. 1:14-md-02583-TWT, 2016 WL 2897520, at *3-4 (N.D. Ga. May 18, 2016); *In re* Experian Data Breach Litig., No. SACV 15-1592 AG, 2016 WL 7973595, at *6 (C.D. Cal. Dec. 29, 2016); *In re* Premera Blue Cross Customer Data Sec. Breach Litig., 198 F. Supp. 3d 1183, 1205 (D. Or. 2016); Lavender v. Driveline Retail Merch., Inc., No. 18-CV-2097, 2019 WL 4237848, at *2 (C.D. Ill. Sept. 5, 2019). Although these cases did survive 12(b)(1) and 12(b)(6) challenges, they also settled prior to discussion of *reasonable* cybersecurity duty.

34. Some recent cases have mentioned reasonable duty, but few have discussed cybersecurity duties specifically. *See, e.g.*, Pa. State Emps. Credit Union v. Fifth Third Bank, No. 1:CV-04-1554, 2006 WL 1724574, (M.D. Pa. June 16, 2006) (finding a duty where contract specifies security obligations, here in relation to bank contracts and external credit-card industry security requirements); Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 427 (5th Cir. 2013) (referencing external credit-card industry security requirements); *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1309 (D. Minn. 2014) (describing Target Corporation's obligations based on foreseeability of harm and referencing external credit-card industry security requirements); Weinberg v. Advanced Data Processing, Inc., 147 F. Supp. 3d 1359, 1366 (S.D. Fla. 2015) (finding that the defendants undertook a duty with respect to the plaintiffs and were obligated to perform that duty); *In re* Cmty. Health Sys., Inc. v. Schnuck Mkts., 210 F. Supp. 1022 (S.D. Ill. 2016) (identifying a duty as extending from a contract that referenced HIPAA); Hapka v. Carecentrix, Inc., No. 16-2372, 2016 WL 7336407 (D. Kan. Dec. 19, 2016) (explaining that reasonable foreseeability of harm triggers a duty of care on the part of the defendant); *In Re* Sonic Corp. Customer Data Sec. Breach, No. 1:17-md-2807, 2021 WL 3269018 (N.D. Ohio July 30, 2021) (explaining that a reasonable foreseeability of harm triggers a duty of care for some plaintiffs); Savidge v. Pharm-Save, Inc., No. 3:17-CV-186, 2020 WL 265206 (E.D. Ky. Jan. 17, 2020) (describing the occurrence of unauthorized access to plaintiff data as the basis for the defendant not performing their duty); McGlenn v. Driveline Retail Merch., Inc., No. 18-CV-2097, 2021 WL 4301476, at *7-8 (C.D. Ill. Sept. 21, 2021) (explaining that fiduciary duty is not established under Illinois law); Deutsche Bank Nat'l Trust Co. v. Buck, No. 3:17cv833, 2019 WL 1440280 (E.D. Va. Mar. 29, 2019) (describing the requirement to establish an independent common-law duty for any tort that the state has not previously recognized); Buckley v. Santander Consumer

that make determinations of cybersecurity duty, such as administrative agencies and administrative courts.

The contributions of this Article include a descriptive analysis of contexts in which courts and administrative agencies may be determining cybersecurity duty or approximations of such duty today, what information may be relevant to determining cybersecurity duty, and how to appropriately separate good actors who are victims of sophisticated cyberattacks from those who have not fulfilled their reasonable duty. Courts and agencies ascertaining reasonable duty should use both *static* sources of reasonable cybersecurity duty, such as standardized practices, and *dynamic* analysis of reasonable duty, such as contextual, situational analysis of applied practices.

This paper proceeds in four Parts. Part I introduces the variety of legal domains where legal entities will evaluate reasonable duty, typically determined when a data breach occurs. Part II discusses how external legal requirements influence internal organizational governance of cybersecurity practices. Part III evaluates the specific nature of cybersecurity duty in various legal domains, the status of recent impediments to meaningful court engagement in the question of duty, and then explores limited cases that have discussed cybersecurity duty.

Finally, in Part IV, I propose a two-part analytic model that will provide courts and administrative agencies with a method for determining whether reasonable cybersecurity has been met: 1) an evaluation of static cybersecurity requirements and 2) a contextual, dynamic investigation of what is truly reasonable under the factual circumstances presented.

PART I: DEFINING CYBERSECURITY DUTY

Legally-recognized cybersecurity duties may be new, but the concept of duty is an important feature of statutes and the common law.[35] Duty

---

U.S.A., Inc., No. C17-5813, 2018 WL 1532671 (W.D. Wash. Mar. 29, 2018) (describing the common-law duty of businesses to protect customers from imminent and foreseeable criminal conduct).

35. Michael Parrington, *A Short History of the Common Law,* MICHAEL'S GEN. MUSINGS BLOG (Mar. 16, 2016), https://blogs.harvard.edu/mparrington73/2016/03/16/a-short-history-of-the-common-law [https://perma.cc/7GAM-KNFF]. As early as 1837, courts began recognizing duties of care beyond preexisting contractual relationships, such as when a person or organization owed a specialized or general duty to another. Courts first connected duty of this kind with questions of liability in *Vaughan v. Menlove* (1837) 132 Eng.

established by statute or common law informs what a person or organization *must* do (or should have done) to avoid potentially undesirable legal outcomes, including fines, injunction, or judgment.[36] Duty is a form of obligation, an obligation that, if not performed, may result in liability or other legal sanctions.[37]

Duty is classically difficult to determine because it is inherently contextual and dynamic, depending on the body of law in which it occurs. For example, duty pursuant to statute and elaborated by an administrative agency is different than duties as obligations in contract law or duty as established in tort by the common law. Yet these distinct doctrinal areas share a common problem: how to define whether an organization has fulfilled some duty or obligation with regards to cybersecurity activities.

A. What is Cybersecurity Duty?

Duty "signifies a thing due; that which is due from a person; that which a person owes to another [,] an obligation to do a thing."[38] Duty and debt are together represented by the Latin term *debitum*, describing some degree of action owed to another.[39] Colloquially, duty is obligation owed to another, inherently relational and contextual, established prior to engaging in any action or analyzed after alleged failure to perform that duty.

However, with the exception of overt statutory duties, duties are not usually identified or interrogated until something goes wrong. For cybersecurity, this involves a cyberintrusion or data breach stemming from a cybersecurity failure. Following a data breach or other compromise, courts and administrative agencies will need to determine whether an organization had a duty and whether the organization effectively met this duty. Duties owed to another can take many forms:

Rep. 490; 3 Bing. N.C. 468 and *Langridge v. Levy* (1837) 150 Eng. Rep. 863, 2 M & W 519, which found a duty of care related to fraud. Later, *Heaven v. Pender* established that a duty between parties can exist even when a contract has not established one, setting the foundation of the negligence tort. (1883) 11 QB 503 (Eng.).

36. RESTATEMENT (THIRD) OF TORTS § 37 (AM. L. INST. 2010).

37. *Id.* cmt. h.

38. *Duty*, BLACK'S LAW DICTIONARY (2d ed. 1995), https://thelawdictionary.org/duty [https://perma.cc/4THC-L2TC].

39. *Id.*

1) **Statute:** a statutory duty between an organization and individuals (or an agency on their behalf);

2) **Fiduciary Duties:** special duties that involve duties of care, expertise, loyalty, and confidentiality;

3) **Tort of Negligence:** a generalized duty of care between entities or individuals (a relational duty established by the occurrence of a tort);

4) **Private Contract:** contractual duties established by private contract between entities or organizations and individuals; and

5) **Duties to Shareholders:** publicly traded companies may be required to disclose material information, such as data breaches or substandard cybersecurity program data, to shareholders. [40]

Although each of these legal domains are distinct, none of them have created a replicable approach for determining what constitutes "reasonable" cybersecurity duty. Despite courts and administrative agencies not defining reasonable cybersecurity duty, cyberattacks increase in frequency by the year: 2021 marked the highest number of cyberattacks and data breaches ever reported.[41] Although many data breaches and cyberattacks are never reported, in 2022, 1802 cases of data breach were reported, affecting nearly 422 million individuals.[42]

Cyberattacks, including data breaches, can compromise almost any kind of data and affect anyone. Some cyberattacks may involve personal information of consumers or employees, while other cyberattacks may involve confidential business information or trade secrets. Many of these cyberattacks are preventable; nearly ninety-five percent of cyberattacks could have been prevented using "simple and common-sense approaches to

40. This Article does not discuss shareholder duties because these duties are limited to publicly traded companies and are established today through material information disclosure rather than direct obligations to shareholders.

41. Chris Brook, *2021 to Date Has Seen More Data Breaches than 2020*, DIGITALGUARDIAN (Oct. 14, 2021), https://digitalguardian.com/blog/2021-date-has-seen-more-data-breaches-2020 [https://perma.cc/LE4V-9QC6].

42. Joseph Johnson, *Annual Number of Data Breaches and Exposed Records in the United States from 2005-2020,* STATISTA (2021), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed [https://perma.cc/B66R-FJUH].

improving security."[43] Data breaches and their legal aftermath are likely to present unique challenges for determining liability, breach, or noncompliance.

Without using a replicable model for assessing reasonable duty, courts and administrative agencies will be unable to effectively administer justice, potentially rewarding ineffective and objectively unreasonable cybersecurity practices, while punishing subjectively reasonable ones. Or worse yet, legal entities may treat every cyberintrusion or data breach as evidencing a failure to implement reasonable cybersecurity practices. Moreover, a lack of clarity and approach for legally determining reasonable cybersecurity practices means that organizations will have great difficulty reasonably avoiding legal issues by employing strong cybersecurity practices.[44]

B. Statutory Duty

Statutorily-created duty is relatively straightforward: a legislative body at the municipal, state, or federal level has established a requirement within a body of law.[45] The statutory requirement, then, is positive law, or a published requirement to act or not act in some specified way, enforced by an administrative body or directly recoverable by a private party.[46] Although some laws include cybersecurity requirements, many use language such as "reasonable security measures" as the standard organizations must follow.[47] Some laws may designate a private right of action or require organizations to include identical statutory language in

43. Marc Wilczek, *Almost All Cyberattacks in 2018 Were Preventable*, CIO MAG. (Sept. 10, 2019), https://www.cio.com/article/3437778/almost-all-cyberattacks-in-2018-were-preventable.html [https://perma.cc/3P53-VVQE].

44. DEREK E. BAMBAUER, JUSTIN (GUS) HURWITZ, DAVID THAW & CHARLOTTE A. TSCHIDER, CYBERSECURITY: AN INTERDISCIPLINARY PROBLEM 457 (West 2021).

45. *See* Perry v. S.N., 973 S.W.2d 301 (Tex. 1998).

46. For example, a financial institution under the Gramm-Leach-Bliley Act must employ reasonable safeguards to protect financial nonpublic information. *See* The Gramm-Leach-Bliley Act (aka Financial Services Modernization Act of 1999), 15 U.S.C. §§ 6801-6809.

47. Scott Shackelford, Annie Boustead & Christos Makridis, *Defining "Reasonable" Cybersecurity: Lessons from the States*, COUNCIL ON FOREIGN RELS. (Mar. 7, 2022), https://www.cfr.org/blog/defining-reasonable-cybersecurity-lessons-states [https://perma.cc/K76W-6UGV].

contracts with subcontractors, effectively exporting and extending these laws through private contract.[48]

1. Private Rights of Action

If the statute establishes a private right of action, individuals who have standing to sue under the statute may do so under the common law.[49] A private right of action almost always involves a negligence per se claim. In a negligence per se claim, the duty is not an independent showing of what reasonable behavior would have been but rather what the law requires statutorily.[50] However, even when duty may be specified within the statute, courts may not automatically recognize such a duty.[51] If the duty is created through an explicit statutory requirement, courts may apply it; however, if the duty is interpreted by an administrative agency rather than established by statute directly, courts may determine that the duty does not exist.[52] This

48. This statutory practice is used increasingly often as contracted parties are increasingly not regulated by the same regulators (or any U.S. regulators in the case of international organizations). The effect is an exportation or long-arm statute effect mobilized through private contracting using statutory duties as contractual promises or obligations.

49. A private right of action may be explicit, specified within the statute, or implied by the courts. Private rights of action recognized by implication have largely been rejected historically. *See generally* Anthony J. Bellia Jr., *Justice Scalia, Implied Rights of Action, and Historical Practice*, 92 NOTRE DAME L. REV. 2077, 2081-82 (2017) (describing the evolution from determining private rights of action from legislative intent to Cort v. Ash, 422 U.S. 66 (1975), which established a multifactor test).

50. *See* Stenger v. Timmons, No. 10AP-528, 2011 WL 941586 (Ohio Ct. App. Mar. 17, 2011); *Judicial Council of California Civil Jury Instructions*, JUD. COUNCIL OF CAL. (2022), https://www.justia.com/documents/trials-litigation-caci.pdf [https://perma.cc/Z5HB-WWCV].

51. Andrew E. Costa, *Negligence Per Se Theories in Pharmaceutical & Medical Device Litigation*, 57 ME. L. REV. 52, 60 (2005) (citing the Third Circuit's note that the "Restatement (Second) of Torts provides that a court 'may' adopt a regulation to define the standard of care").

52. For example, courts may find that an agency's interpretation is unreasonable or inconsistent with the plain meaning of statutory language if the agency did not itself draft the rule and is not expressly delegated by a legislative body to interpret the law. *See* Sullivan v. Everhart, 494 U.S. 83, 88-89 (1990); NLRB v. Curtin Matheson Sci., Inc., 494 U.S. 775, 786-87 (1990); Curtin Matheson Sci.,

might occur if courts hold that the legislative intent of the state or federal legislature did not include such a requirement or that an administrative agency does not have the statutory authority to establish that requirement.[53]

Alternatively, the statute may create a private right of action that courts recognize, but the duty created by the statute may be imprecise. For example, statutes could use language like "reasonable security procedures

---

Inc., 494 U.S. at 797 (Rehnquist, C.J., concurring); K Mart Corp. v. Cartier, Inc., 486 U.S. 281, 291-92 (1988); Thomas Jefferson Univ. v. Shalala, 512 U.S. 504, 510-14 (1994); Mullins Coal Co. v. Director, Office of Workers' 15 Comp. Programs, 484 U.S. 135, 159 (1987); ABF Freight Sys., Inc. v. NLRB, 510 U.S. 317, 323-25 (1994).

53. The California Consumer Privacy Act of 2018 (CCPA) created a private right of action for noncompliance with CCPA provisions, including the CCPA's reasonable security requirement for protecting personal information. *See* CAL. CIV. CODE § 1798.150. (West 2022). The CCPA's reasonable security requirement is only referenced in relation to a private right of action, but the CCPA permits the California Attorney General (AG) to promulgate general requirements. The AG is required to "solicit broad public participation to adopt regulations . . . as necessary to further the purposes of this title." *Id.* This seems to suggest that the Attorney General's interpretation of certain requirements, following public consultation, could establish the source of duty in a private right of action. And perhaps courts applying the CCPA could similarly defer to the AG's interpretation per the CCPA's statutory language and California's approach to judicial deference (to administrative interpretation). Generally, federal agencies with broad rulemaking authority or field preemption benefit from *Chevron* deference. *See* Chevron v. Nat. Res. Def. Council, Inc., 468 U.S. 837 (1984) (holding that courts generally defer to agency interpretation unless the interpretation is unreasonable or Congress has specifically addressed the issue at hand). Such deference is limited to formal legal proceedings such as adjudication and notice-and-comment proceedings under the Administrative Procedure Act. This means that pseudo-rulemaking activities, such as formal opinions and guidance do not generally qualify and courts are required to interpret the statute to determine what is actually required. California's (and perhaps other states') judicial deference is a less stringent standard than *Chevron*, depending on the text of the law itself and contextual information that provides input into judicial decision-making, with varying degrees of deference. *See, e.g.*, Yamaha Corp. of America v. State Bd. of Equalization, 960 P.2d 1031 (Cal. 1998) (explaining the binding power of administrative agencies as "contextual"); Ramirez v. Yosemite Water Co., 928 P.2d 2 (Cal. 1999) (examining whether the scope of interpretation was within a delegated scope of authority).

or practices" and either leave it open-ended or convey some expectation of where additional details might be provided.[54]

2. Duty to Execute a Contract

In addition to private rights of action conferred by a statute, a statute may also require organizations to execute a contract with third parties who may or may not be directly regulated under the statute. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires execution of a Business Associate Contract (Business Associate Agreement, or BAA), which specifies a third party's compliance with the HIPAA Security Rule and Data Breach Notification Rule.[55] In the event of a data breach or other cyberattack, the first party can enforce an otherwise valid contract executed with a non-U.S. third party, even if that third party cannot be directly regulated by the Office for Civil Rights.[56]

When the law requires a regulated organization to execute contract terms with its subcontractors or business affiliates (third parties) that are the same or similar, the law creates a pseudo-statutory duty via contract; a statutory duty that becomes a contractual promise or obligation.[57] Moreover, these third parties are typically obligated within the contract to execute these same contractual terms with any of their third parties or business affiliates that have access to the information referenced in the contract.[58] Any failure to perform according to the contract's terms may result in breach of contract, enforceable as a garden-variety, common-law contracts case. Although these obligations may not be enforced by an administrative agency, the agency can enforce these obligations on the primary regulated party, and that party can sue for breach of contract to recover damages.

54. CAL. CIV. CODE § 1798.150 (West 2022).

55. *Business Associate Contracts*, U.S. DEPT. HEALTH & HUM. SERVS. (Jan. 25, 2013), https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html [https://perma.cc/AS4R-MH62].

56. *Id.*

57. *Id.*

58. *Id.*

3. Federal Administrative Enforcement

Statutory duty is created by a statute, but it is typically interpreted, extended, and enforced by a specific administrative agency. Depending on the details of the specific statute, a state or federal administrative agency may be permitted to promulgate more specific rules associated with the statute under the Code of Federal Regulations (CFR).[59] For example, the Food, Drug and Cosmetics Act (FDCA) permits the Food and Drug Administration (FDA) to promulgate rules subject to the federal Administrative Procedure Act's (APA) mandatory notice-and-comment process that may include cybersecurity requirements.[60]

Federal administrative rules properly promulgated under the CFR may then be enforced in the agency's administrative court,[61] whose decisions may potentially be appealed to federal court.[62] Statutory duty, then, is established directly by the statute, but may be expanded by the administrative agency when the agency can promulgate rules, and explained using agency opinions and guidance.[63] Duties established by these processes are enforceable when explicitly stated within the statute or formally issued as administrative rules consistent with the APA.[64]

---

59. *Federal Statutes and Regulation,* U.S. DEP'T INTERIOR (Oct. 2021), https://www.doi.gov/library/collections/law/statutes [https://perma.cc/4A97-YTHU]; *A Guide to the Rulemaking Process*, U.S. OFFICE FED. REG. (Jan. 2011), https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf [https://perma.cc/GHE8-Y7E7]; Administrative Procedure Act of 1946, Pub. L. No. 79-404, 60 Stat. 237.

60. 21 U.S.C. § 371(a) (2018).

61. Administrative courts are typically referenced as Article I courts and include administrative law judges conducted as bench trials. *See Administrative Hearings*, JUSTIA (2022), https://www.justia.com/administrative-law/administrative-hearings [https://perma.cc/7258-SMP4].

62. Once a party has exhausted their "agency-level appellate remedies," a party can appeal to a state or federal court. *See Appeals from Administrative Proceedings*, JUSTIA (2022), https://www.justia.com/administrative-law/appeals-from-administrative-proceedings [https://perma.cc/M4KL-JHKY].

63. *Administrative Agency Interpretation of Laws*, USLEGAL (2022), https://administrativelaw.uslegal.com/administrative-agencies/administrative-agency-interpretation-of-laws [https://perma.cc/GX6Y-JHHK].

64. VALERIE C. BRANNON & JARED P. COLE, CONG. RSCH. SERV., R44954, CHEVRON DEFERENCE: A PRIMER 1 (2017).

When interpretation of the statute or rule is in question, federal courts may incorporate the agency's interpretation, at least where express delegation language is included in the statute; Congress "has explicitly left a gap for the agency to fill," and potentially when legislative delegation is implicit but the agency's interpretation is reasonable.[65] Practically speaking, this means that statutory duty could be dependent on an agency's interpretation rather than only what is specified in a statute, which could be communicated in policy statements or interpretive rules (collectively "guidance").[66]

When a statute does not clearly articulate a duty, or when a statute specifies a general duty, administrative agencies and courts are left to examine whether an organization has fulfilled its duty on their own. Consider the following:

> *De Rigeur Foods is a prepared food delivery service. Although De Rigeur does not directly interface with insurers or healthcare providers, it often provides food for individuals with a variety of specific health needs and dietary requirements. For example, meal selection could be labeled "halal" or "diabetic." De Rigeur delivers meals in California and recently experienced a data breach that compromised personal information of California residents.*

De Rigeur is regulated under the California Consumer Privacy Act (CCPA), which permits plaintiffs to sue if "nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[67] However, the CCPA does not offer any specificity regarding what this "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information" actually means.[68] The only instruction offered to organizations like De Rigeur is that they are required to notify individuals

65. Chevron v. Nat. Res. Def. Council, Inc., 468 U.S. 837, 843-44 (1984).

66. The Administrative Procedure Act, which typically regulates administrative rule-making that has the force of law in its enforcement, specifically exempts non-legislative rulemaking. *See* 5 U.S.C. § 553(b)(A) (2018); *see also Agency Guidance Through Interpretive Rules*, ADMIN. CONF. U.S., (Aug. 8, 2019), https://www.acus.gov/recommendation/agency-guidance-through-interpretive-rules [https://perma.cc/ELA4-SJY9].

67. California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.150(a).

68. *Id.*

and the state when the data breach has occurred and that they may be subject to liability. California's Attorney General's office has not published anything that would enable De Rigeur to avoid liability or to understand its likelihood of prevailing at trial.[69]

It is uncertain how a court fielding a private right of action from De Rigeur's customers would analyze duty in this scenario, or even how the California Attorney General's office would apply the standard. Although some standards informing duty might be obvious, such as not conducting regular cybersecurity risk assessments, others, like advanced network security settings or adversarial war game simulations, could be far less obvious and comparatively less "reasonable."

C. Fiduciary Duty

Fiduciary duties are established by statute and create a reasonable duty defined vis-à-vis specific contexts and relationships.[70] Fiduciary duties are established when there is risk of one party taking advantage of another, when one party has special knowledge or is in a position of expertise with respect to the other, or when reliance and trust of one party with respect to the fiduciary is essential to the relationship or transaction.[71] For example, fiduciary duties frequently include trustee-trust beneficiary, agent-principal, lawyer-client, guardian-ward, director-corporation, and partner-fellow partner relationships, with enhanced duties being reserved for parties that perform a specific role.[72] Fiduciary duties include specialized

69. In 2016, the California Data Breach Report did list 20 Center for Internet Security (CIS) Critical Security Controls, but these have not been explicitly referenced elsewhere in relation to CCPA. *See* Kamala Harris, *California Data Breach Report*, CAL. DEP'T OF JUST. 39 (Feb. 2016), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf [https://perma.cc/T3VY-HGAL].

70. Gregory S. Alexander, *A Cognitive Theory of Fiduciary Relationships*, 85 CORNELL L. REV. 774, 776-77 (2000) (describing the special legal distinction given to certain relationships that are subject to "more stringent legal norms").

71. Paul B. Miller & Matthew Harding, FIDUCIARIES AND TRUST: ETHICS, POLITICS, ECONOMICS, AND LAW 9 (2020).

72. *See* Deborah A. DeMott, *Breach of Fiduciary Duty: On Justifiable Expectations of Loyalty and Their Consequences*, 48 ARIZ. L. REV. 925, 935 (2006). Fiduciary duties may also be broader than traditionally recognized relationships of trust. "A fiduciary relation exists between two persons when one of them is

versions of duty, such as a duty of loyalty, wherein a person must act in the interest of the other person first and foremost, and a duty of competence, where a person must perform their role competently.[73] These special duties for fiduciaries are established by state law or recognized by courts, but fiduciary relationships were historically formed through mutual assent in contract.[74]

Although fiduciary relationships are typically established or evidenced via contract, there are limited situations in which courts will recognize a fiduciary relationship. Typically, these duties are interpreted by courts to be vertical in nature: the duty lies with the person in a position of power over another. These relationships are inherently asymmetrical because a structural, power or knowledge imbalance exists.[75] For example, a lawyer may be required to reasonably protect client confidentiality, which could

---

under a duty to act for or give advice for the benefit of another upon matters within the scope of the relation." *Id.* at 933 n.38. Most breaches of fiduciary duty are torts. *See id.* at 928.

73. *See Fiduciary Duty,* BLACK'S L. DICTIONARY (2d ed.), https://thelawdictionary.org/fiduciary-duty/ [https://perma.cc/5FBJ-CAWJ]. Key to the concept of a fiduciary is the subordination of one's interests in favor of another's.

74. *See* Alexander, *supra* note 70, at 776. A fiduciary duty based on information collection and use has been proposed as one model for regulating privacy and cybersecurity interests. *See* Ian Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CAN. BUS. L.J. 419 (2001); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 102-103 (2006) (explaining the role of data brokers and a potential connection to fiduciary roles, including stockbrokers and clients, lawyers and clients, physicians and patients, parents and children, corporate officers and shareholders, and insurance companies and their customers); Jack M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. 1217, 1227-28 (2017); Frank Pasquale, *Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society*, 78 OHIO ST. L.J. 1243, 1244-45 (2017); Richard Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 SANTA CLARA HIGH TECH. L.J. 79, 95-98 (2019); Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559, 591; Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. UNIV. L. REV. 961, 992-93 (2021) (describing the evolution of fiduciary duty from contractual to relationship-based); Neil M. Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 4 EUR. DATA PROT. L. REV. 1, 3 (2020).

75. *See* Alexander, *supra* note 70, at 777.

include employing reasonable security practices.[76] However, the majority of fiduciary duties are highly contextual, making it difficult to ascertain whether a fiduciary has breached their duty of loyalty without understanding the facts and nature of the relationship.[77]

When considering cybersecurity duties, courts should also consider context-specific information, such as how sensitive the compromised data is, how critical access to the data would have been, and who might wish to compromise these data. Consider the following example:

> *Santos, Rooter & Bolaji LLP is a law firm specializing in plaintiff-side personal injury litigation. As part of litigation preparation, attorneys collect extensive personal information about their clients' cases, including medical records, psychiatric records, GPS data, and other personal information. They maintain these records in a third-party system, which previously passed a security certification, SSAE-16 SOC 2 Type I. The third-party system was recently compromised by an attacker and plaintiff records were disseminated to defendant parties.*

In a legal action involving a breach of fiduciary duty, would a court determine that Santos, Rooter & Bolaji fulfilled its fiduciary duty to its clients? Although the firm selected a reputable third party, it is unknown whether that third party continued to effectively manage security after beginning the engagement and if the firm effectively supervised and assessed the third party to protect its clients' confidentiality. Moreover, a fiduciary duty of confidentiality could include more than purchasing reputable software. For example, the firm might have needed to consider limiting access to certain client files to specific attorneys working on the case only or taking more drastic measures based on the potential for an adverse party to compromise the system.

D. Common-Law Negligence Duty

The legal concept of tort functions to determine fault between two or more parties where the action (or inaction) of one party results in harm to

76. *See id.* at 776. For example, a trustee may be liable for all losses in a trust, regardless of their action. In some cases, fiduciary behavior that results in any loss to the other is recoverable as strict liability.

77. *See id*. at 777.

another.[78] Although civil tort liability may function to punish parties that inflict harm on another party and to deter similar behavior, tort law primarily allocates risk, burdens, and responsibilities.[79] To resolve legal questions, courts must ask, *ex post*, which party would have been better positioned to reduce the probability or severity of an injury—that is, which party could have appreciated the risk, had more responsibility to act, and was practically positioned to avoid an injurious result.[80] But the law must also deal with a threshold issue: whether the law has historically recognized this specific type of tort (or wrong). This becomes a particular issue when talking about torts related to cybersecurity. If there is no wrong, there is no cause of action that can result in defendant liability.[81]

Unlike negligence per se, where the standard of care is established by statute, negligence requires the courts to determine what the reasonably prudent defendant's duty would have been at the time the claimed tort occurred.[82] Under negligence, duty (and, reciprocally, fault) is part objective and part subjective: it is objective because duty is evaluated from the perspective of a reasonably prudent person or organization, specifically what would a reasonably prudent (or reasonable) person or organization have done in the moment the person or organization acted, *ex ante*, and with

78. *See* Joost Bloom, *Tort, Contract, and the Allocation of Risk*, 17 SUP. CT. L. REV. (2D) 289, 289 (2002).

79. *See* Kenneth W. Simons, *Tort Negligence, Cost-Benefit Analysis, and Tradeoffs: A Closer Look at the Controversy*, 41 LOY. L. REV. 1171, 1194-96 (2008).

80. *See id.* at 1195. As Kenneth Simons cautions, overly focusing only on the plaintiff's injuries rather than duty of care from an *ex ante* perspective fails to acknowledge both general reasonable precautions all potential defendants might take to reduce risk generally and that under some circumstances plaintiffs might also be expected to take a precaution, as well. One area of future inquiry, not explored in detail here, is the degree to which cybersecurity risks might be connected to activities that are to the sole benefit of the defendant, resulting in harm, versus activities that are essential activities that the plaintiff cannot reasonably avoid. *See id.* at 1196.

81. In addition, practical barriers to recovery include the status of the plaintiff and whether the harm alleged is only monetary. For a large portion of cyberattacks and data breaches, the harms will be primarily monetary, and if the plaintiff is an organization (and in limited states, individuals), the plaintiff will likely barred from bringing an action under the economic-loss doctrine.

82. *See* Alan Calnan, *The Fault(s) in Negligence Law*, 25 QUINNIPAC L. REV. 695, 697 (2007).

respect to the world at large.[83] Context for such behavior is inherently subjective and dependent on the facts that led to the injury—although an organization is evaluated according to the objective reasonably prudent person standard,[84] the subjective evaluation could involve the intentions and values of each actor.[85]

Whether an organization took sufficient steps to avoid a cyberattack or data breach would likely depend on what a reasonable organization would have done with the type of information available to them, along with the corresponding risk to another organization, customers, employees, or consumers based on the given scenario.[86] For example, a reasonable duty would likely be determined by both how reasonable organizations protect this type of data *and* by the potential risk to individuals.[87] Consider the following scenario:

> *Gatos Mobile is a wireless service provider. Last year, Gatos Mobile suffered a cyberattack when a professional hacking organization, ThetaKan, targeted a primary set of Gatos Mobile servers using a distributed denial of service (DDoS) attack. Although Gatos Mobile monitors its networks, it did not monitor its networks frequently enough to stop the DDoS attack before it interrupted business. As a result of the ThetaKan attack and Gatos Mobile's failure to prevent the attack, wireless customers lost access to their mobile services. At least ten mobile subscribers attempted to contact police officers on their mobile devices to report crimes and were unable to receive assistance.*

This scenario describes a common complexity in determining duty for common-law negligence: the role of foreseeable duty. Gatos Mobile owes a reasonable duty of care to its customers. Although Gatos Mobile provides service to customers, it is the intervening unilateral actions of ThetaKan that directly caused the breach. When examining duty, courts would first

83. *See id.* at 700.

84. *See* Keith N. Hylton, TORT LAW 103-104 (2016).

85. *See* Calnan, *supra* note 82, at 700.

86. As Alan Calnan succinctly explains, "no matter what standard is used, fault imbues with it a universal character. A faulty act is faulty regardless of its consequences. For example, throwing a rock at a defenseless child would be fault even if the child were not struck." *Id.* For cyberattacks and data breaches, however, usually this distinction is not so clear: is not doing enough to protect customers as blameworthy as directly perpetrating the tort?

87. *See* RESTATEMENT (THIRD) OF TORTS § 6 cmt. B (AM. L. INST. 2010).

examine whether ThetaKan's actions were foreseeable from the perspective of Gatos Mobile and, if they were, what duty Gatos owed to customers.[88] If ThetaKan's DDoS attack was foreseeable, a court would then examine Gatos' actions related to preventing a DDoS attack to determine if it satisfied its reasonable duty.

Whether Gatos Mobile met a duty of reasonable care depends heavily on whether 1) a duty with respect to subscriber data existed, and 2) whether that duty had been fulfilled. For cybersecurity duty, however, it may be difficult to evaluate whether Gatos' actions were actually reasonable. For example, a cybersecurity standard may have required Gatos to monitor external requests to its internal resources (as would occur during a DDoS attack), but it would not likely mandate the frequency of monitoring that would have prevented a DDoS attack. When examining duty, a court could find the existence of a duty, but whether reasonable duty has been breached is a question that involves a reasonableness inquiry consisting of what a similarly situated organization would have done under the circumstances.[89]

E. Contractual Duty (Obligation)

Contractual duties, also known as obligations or promises, provide the clearest example of a dutys, at least where the parties forming the agreement have effectively established and negotiated material cybersecurity terms. Contracts, contracts implied in fact, and quasi contracts may exist between organizations and individuals, such as a terms-of-use agreement, click-wrap or browse-wrap agreements, or a privacy notice.[90] Between an organization and individuals, contractual duty

88. Customers would sue Gatos rather than ThetaKan in data breach litigation. *See* Alicia Solow-Neiderman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, YALE L.J.F. 614, 628-29 (Jan. 11, 2018), https://www.yalelawjournal.org/forum/beyond-the-privacy-torts [https://perma.cc/DG7Z-RBSS].

89. Duty is the only element of a negligence claim that a court decides as a matter of law. This means that courts have tremendous power in establishing duty.

90. *See* William A. Keener, *Quasi-Contract, Its Nature and Scope*, 7 HARV. L. REV. 57, 57-58 (1893).

specified in such agreements may also provide the basis for duty within a tort action or in an equitable remedy, such as unjust enrichment.[91]

Contracts that include cybersecurity language are frequently formed between sophisticated entities. Between organizations, cybersecurity language may be included when organizations contract *for* cybersecurity services or when organizations contract for other goods and services.[92] Contracts may be formed using traditional master services agreements, master supply agreements, or may leave many details to performance outside basic contours of an agreement.[93] Organizations contracting for other goods and services may include cybersecurity to varying degrees of detail, from ranging from general confidentiality provisions to many pages of cybersecurity details.[94] For example, consider the following sample provision from a contract:

> *Each party acknowledges that it may have in its possession Confidential Data of the alternate party and shall use best efforts to secure such Data. Shanleigh Computerwerks [Supplier] shall employ reasonable security practices in its protection of Holters Customer Personal Information and trade secret information. In the event of any reasonably suspected cyberintrusion or data breach regarding such Customer Personal Information or Confidential Data, Supplier shall notify Holters without unreasonable delay and in no event longer than 48 hours after discovery and at a regular cadence thereafter, consistent with the severity of the cyberintrusion or data breach. Holters reserves the right to participate in any forensic investigation, request and timely receive forensic investigation results, or conduct a confirmatory audit following the conclusion of remediation procedures. Supplier shall contact Holters prior to providing any information regarding the cyberintrusion or data breach*

91. *See id.* at 71; *see also* Stephen A. Smith, *Unjust Enrichment: Nearer to Tort than Contract*, *in* PHILOSOPHICAL FOUNDATIONS OF THE LAW OF UNJUST ENRICHMENT 4 (Robert Chambers ed., 2009).

92. *See, e.g., Vendor Cybersecurity & Contract Language*, ASPEN TECH. POL'Y HUB (June 2020), https://www.aspentechpolicyhub.org/wp-content/uploads/2020/06/Vendor-Cybersecurity-Contract-Language.pdf [https://perma.cc/XP9M-K4J8] (describing recommended contractual clauses and sample boilerplate provisions).

93. *See* Charlotte A. Tschider, *Legal Opacity: Artificial Intelligence's Sticky Wicket*, 106 IOWA L. REV. 126, 145 (2021).

94. *See* CHARLOTTE A. TSCHIDER, INTERNATIONAL CYBERSECURITY & PRIVACY LAW IN PRACTICE, 379-80 (2018).

to any administrative agency or law enforcement, so that Holters can acquire a protective order, if necessary.

In the example above, the parties have opted not to include specific cybersecurity terms in the contract but rather to provide some flexibility in the interpretation of reasonable practices, for example if industry standards change. Although some parties may include more detailed terms, these terms may not be tremendously specific.

In the event a cyberattack or data breach impacts one of the parties and compromises the information of another, the party seeking to recover will attempt to rely on nonperformance of a cybersecurity term as the basis for breach of contract.[95] For a court to find that an organization had a duty to perform as the basis for breach of contract, the organization will need to prove that: 1) the term was material with respect to the contract, 2) the term's performance was due and was not performed or substantially performed, and 3) the organization seeking to recover was economically injured as a result.[96]

Perhaps the most significant challenge to ascertaining duty is when there is no specific material term, but rather a generalized term such as "will provide reasonable security," the nonperformance of which exposed the organization to a cyberattack or data breach. If the party demanding remedy did not specify any specific examples of these practices, courts may have difficulty ascertaining whether the third party's actions or omissions could be construed as reasonable.[97] If courts find that such a term is ambiguous, it may trigger introduction of parol evidence.[98] In such a situation, it is

95. *See* RESTATEMENT (SECOND) OF CONTRACTS § 235 (AM. LAW. INST. 1981) ("[W]hen performance of duty under a contract is due any nonperformance is a breach.").

96. *Id.* at § 241; *see also* Hudson v. Wakefield, 645 S.W.2d 427, 430 (Tex. 1983) (deciding whether a party's breach is material is a matter of fact).

97. Indeed, even reasonable foreseeability is crucial to both contract and tort actions. "[T]he fundamental test [for both tort and contract recovery] is one of reasonable foreseeability: if the loss or injury for which damages are claimed was not reasonably foreseeable under the circumstances, there is no liability." *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108 (quoting ANDREW M. HORTON & PEGGY L. MCGEHEE, MAINE CIVIL REMEDIES § 4-3(b)(3) (4th ed. 2004)). Generalized terminology like "reasonable cybersecurity," too, can be interpreted differently depending on the facts and circumstances, which will likely survive the parol evidence rule barring other information that could aid in interpretation.

98. *See* RESTATEMENT (SECOND) OF CONTRACTS §§ 220, 222, 223.

unknown what a court might permit for such evidence to interpret these terms.

Each of these bodies of law provide distinct aspects of the concept of duty, and this Article does not aim to describe them as uniform. Despite these differences, they each share a common issue: cybersecurity duty as a concept is profoundly underdeveloped and applicable to each of these bodies of law. Without some method for identifying reasonable cybersecurity duty, courts and administrative agencies risk incentivizing the wrong behaviors—or worse, creating a fractured legal approach that neither holds organizations accountable nor creates any repeatable expectations for how organizations should behave.

PART II: SOURCES OF REASONABLE DUTY

A starting point for locating reasonable cybersecurity duty is in statutory law. However, despite passage of limited cybersecurity regulation, most laws do not explicitly specify detailed security requirements or even mention cybersecurity specifically.[99] Therefore, examinations of cybersecurity duty will frequently be determined in a manner that is open-ended to some extent. In situations where a statute does establish specific cybersecurity duty, often the requirements are open-ended and non-specific, creating a lack of consistency in how courts might examine these duties.

A. Reasonable Duty in Case Law

One might hope that recent case law could give some indication as to how courts hearing cases involving cyberattacks and data breaches apply the law and ultimately decide these cases. Unfortunately, many courts have either failed to analyze duty at all or have defaulted to assumptions rather than engage with the issues on the merits.[100] For example, in *Adkins v. Facebook, Inc.* (previously *Bass v. Facebook, Inc.*), the court considered a coding error that led to the limited personal information of 15 million Facebook users being compromised by hackers.[101] In the case, the District

99. See Kosseff, *supra* note 8, at 1010.

100. According to the Author's research, No cases analyzing duty made it past a motion to dismiss action, and where they analyzed duty, it offered very little direction in how courts will do this in the future.

101. *See* Bass v. Facebook, Inc., 394 F. Supp.3d 1024, 1030 (N.D. Cal. 2019).

Court for the Northern District of California observed a duty without engaging in whether behaviors were actually reasonable:

> [S]ome of the information here was private, and plaintiff plausibly placed trust in Facebook to employ appropriate data security. From a policy standpoint, to hold that Facebook has no duty of care here "would create perverse incentives for businesses who profit off the use of consumers' personal data to turn a blind eye and ignore known security risks."[102]

Here, the court has not engaged with any of the details of what "appropriate data security" actually means. Rather, the fact that data was exposed by accident appears to presume that Facebook breached some duty to the plaintiff.

In *Finesse Express LLC v. Total Quality Logistics, LLC*, the District Court for the Southern District of Ohio examined a case where financial customer information was breached by a carrier performing service on behalf of a freight broker.[103] In the court's analysis, they seemed to suggest that contractual confidentiality could be expansive:

> While the [contract] does not specifically mention "necessary data security policies, rules, and procedures" or "adequate IT security measures," Plaintiffs have adequately plead a claim for breach of contract. It will be Plaintiffs' burden at a later stage of the litigation to prove that the failure to provide such measures constitutes a violation of Defendant's promise to treat Plaintiffs' information "as confidential."[104]

The contractual frame in this analysis is significantly different from that in *Facebook*, as confidentiality is reviewed from what the parties reasonably could have expected given the contours of the agreement, and outside such an agreement, what parol evidence might indicate. Although this case does not discuss reasonable cybersecurity duty, many contracts do include this language and rely on parol evidence to establish this, such as industry standards.

In re Marriott International, Inc. offered a glimpse into how courts might analyze negligence per se claims. The District Court for the District of Maryland held that negligence per se claims under Georgia law might effectively be established by generalized duty under the Federal Trade

102. *Id.* at 1039 (quoting *In re Equifax, Inc., Customer Data Sec. Breach Litig.*)

103. Finesse Express, LLC v. Total Quality Logistics, LLC, 2021 WL 1192521, at *1.

104. *Id.* at *17.

Commission Act's Section 5 prohibiting unfair or deceptive trade practices.[105] Despite the FTC Act not conferring any private right of action based on FTC guidance or other documents, inadequate cybersecurity practices could, at least in Georgia, constitute negligence per se.[106]

The court also held that citing contractual provisions committing to "'reasonable organizational, technical and administrative measures to protect [customers'] Personal Data,'" as well as provisions promising the safeguarding of information "using appropriate administrative, procedural and technical safeguards," with "detailed examples of the methods [that will be used]" is sufficient to demonstrate at a motion to dismiss that the plaintiffs have plausibly alleged the terms of the contract could have been breached.[107]

The court, however, does not explain why this could be the case. It is possible that the existence of the breach and some security failure could justify a plausible argument that cybersecurity measures were unreasonable.

None of these cases demonstrate with any detail how *reasonable* cybersecurity duty is defined because courts haven't defined it. It could be possible to define reasonable cybersecurity duty using existing law or industry standards, but the test used for reasonableness should also consider the contextual application of such law and standards.

B. Federal and State Sources of Cybersecurity Legal Duty

Beginning in 1999, the Gramm-Leach Bliley Act of 1999 (GLBA) mandated security safeguards for the financial services industry, and in 2000, Regulation S-P essentially copied the GLBA Safeguards rule for the investment industry.[108] The GLBA Safeguards rule, the portion of GLBA that establishes cybersecurity controls, broadly requires that financial institutions implement an information security program, designate a person to lead such a program, offer training, oversee third-party service providers, identify internal and external risks, and design safeguards to

105. *In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 478-79 (D. Md. 2020) (citing The Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45).

106. *Id.* at 481-82.

107. *Id.* at 484-85.

108. FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314.4 (2022); SEC Regulation S-P, 17 C.F.R. § 248.30 (2022).

control such risks.[109] Regulation S-P adopts this rule for application to investment organizations.

The Department of Health and Human Services, via the Health Insurance Portability Act of 1996, implemented a Security Rule in 2003 for some of the biggest players in the healthcare industry (including healthcare providers and insurers).[110] HIPAA establishes a much more detailed set of requirements in its Security Rule, including primarily program-based controls like risk assessments, access management, policy development, and incident response.[111] These controls are divided into addressable and required controls, and more technical processes either are not specified or are addressable, meaning that their application is flexible to some degree.[112]

However, HIPAA applies to a limited number of organizations specifically defined as covered entities under the law, namely healthcare providers, health plans, and healthcare clearinghouses.[113] Although the Health Information Technology for Economic and Clinical Health (HITECH) Act expressly expanded the Security Rule to apply to business associates, or service providers for these entities, HIPAA does not apply to all organizations collecting, processing, or storing personal health data.[114] GLBA, Reg S-P, and HIPAA do not permit a private right of action, but agencies charged with enforcing such laws do interpret whether organizations have met their duties under each statutory regime.

Both to establish consistency and to respond to consumer concerns, states began including limited controls through statute as early as 2002. In 2002, states, starting with California, began to recognize the necessity of consumer notification, in observance of the impact data breaches could

109. *Id.*

110. HHS Administrative Data Standards, 45 C.F.R. §§ 160, 164 (2022); *see* Tschider, *supra* note 28, at 1505.

111. HHS Data Security Standards, 45 C.F.R. §§ 164.306-.318 (2022).

112. *See* Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, 26 ANNALS HEALTH L. 1, 13-14 (2017).

113. *See id.* at 11.

114. Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub L. No. 111-5 §13400, 13404, 123 Stat. 226, 260, 264 (2009). HIPAA security requirements only apply to electronic Protected Health Information (PHI), which is identifiable health data about a person's bodily or mental state collected by a covered entity. 45 C.F.R § 160, 164(A), 164(E) (2022). This means that PHI is a portion of all personal health data (PHD), or all identifiable health-related data, regardless of who collects it.

have on customers.[115] Although these laws largely did not require specific security measures, this started to change in 2013 when states began requiring basic security program development and associated policies.[116]

In 2018 and 2019, respectively, New York State passed two laws focusing on cybersecurity. The first, the NYDFS Cybersecurity Law, created specific cybersecurity requirements for covered entities under the law, specifically the financial and insurance industries.[117] Next, New York passed the Stop Hacks and Improve Electronic Data Security Act (SHIELD), which increased liability for data breaches and requires organizations to implement "reasonable" security requirements.[118] California similarly includes a reasonableness standard in both its 2018 California Consumer Privacy Act (CCPA) and the California IoT Security Law, which focus on Internet of Things (IoT) devices.[119]

C. Industry Standards as a Source for Cybersecurity Duty

Absent clear legal directives in regulation, industry standards have largely filled the void in assisting legal departments approximate potential

115. *See* Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45 (2015) (describing the current state and development of data breach notification statutes).

116. *See id.*

117. New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies, N.Y. COMP. CODES R & REGS. tit. 23, § 500 (2017). Notably, although the Department of Financial Services may enforce the cybersecurity regulation, there is no private right of action.

118. Stop Hacks and Improve Electronic Data Security (SHIELD) Act, S.B. S5575B, 2019-2020 Leg., Reg Sess. (N.Y. 2019) (enacted). SHIELD offers specific controls that, *de facto*, put an organization employing these controls in compliance with SHIELD. It does not prescribe these controls directly or offer a private right of action.

119. California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100-.199 (West 2018); Information Privacy: Connected Devices, CAL. CIV. CODE § 1798.91.04(a) (West 2018). The IoT Security Law defines this as "appropriate to the nature and function of the device," and offers some specificity as to system design, specifically authentication.

cybersecurity risks.[120] Perhaps most importantly, industry standards have populated a menu of security options, providing flexibility for sophisticated organizations and cybersecurity professionals to select appropriate security measures.[121] Such measures depend on potential risk to the organization or consumers, the overall business context, and the specific technology implementation.[122]

These industry standards have been created to holistically inform organizational cybersecurity programs. However, standards are only part of the equation, a scaffolding of sorts. Standards enable organizations to have useful conversations about how best to reduce risk to the organization and to other parties, such as individual customers. Additionally, standards can function as a kind of business-facing rebuttable presumption—organizations can use a specific control as a starting point for appropriate controls given the special risks and type of probable cyberattacks an organization might face.

1. The Development of Industry Standards for Cybersecurity

As early as 1995, international organizations like the International Standards Organization (ISO) began to take an interest in creating standards related to the cybersecurity practice.[123] The National Institute of Standards and Technology (NIST) similarly began writing standards related

120. Indeed, compliance with industry standards or best practices may not reflect reasonable behavior that the law would have otherwise required. For example, differences in industry capabilities or organizational size and sophistication might establish different considerations of reasonableness, specifically whether an organization might be better than average or worse.

121. The NIST Cybersecurity Framework (CSF), for example, includes specific implementation tiers and cross-references several other industry standards. The CSF is considered voluntary guidance that should reduce risk to critical infrastructure, although it has been used in a wide variety of industries. *Cybersecurity Framework*, NAT'L INST. STANDARDS & TECH. (July 14, 2021), https://www.nist.gov/cyberframework/getting-started [https://perma.cc/C8PD-FFHC].

122. *See id.*

123. Understanding ISO 27001:2022, ISMS ONLINE, https://www.isms.online/iso-27001 [https://perma.cc/U6JJ-MRZV].

to cybersecurity as part of the overall technology standards suite.[124] In 2006, the major credit card brands organized as the Payment Card Industry, seeking to minimize the frequency of fraudulent credit card transactions, and created the Payment Card Industry Data Security Standards (PCI-DSS).[125]

Accountants and auditors similarly began to see a need for identifying risks, especially following the passage of the Sarbanes-Oxley Act, which required compliance with security standards to prevent unauthorized changes of key financial record keeping.[126] This law, along with enhanced awareness of potential cybersecurity risks, resulted in the monetization of service offerings to identify such risks and reduce work for organizations via SSAE 16, COSO, and COBIT updates.[127] These standards have been re-released on an ongoing basis to keep up with changing industry norms and a changing risk landscape.[128]

In 2014, the National Institute for Standards and Technology, pursuant to the 2013 Executive Order 13636, published the first version of the Cybersecurity Framework.[129] The Cybersecurity Framework not only cross-

124. *See, e.g.*, Nat'l Inst. Standards & Tech., Technical Guide to Information Security Testing and Assessment, U.S. DEP'T COMMERCE (Sept. 2008), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf [https://perma.cc/G4DT-2XHY].

125. About Us, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/about_us [https://perma.cc/88F5-MZ49].

126. *See* Dan Seider, *Sarbanes-Oxley Information Technology Compliance Audit*, SANS 6 (May 17, 2005), https://www.sans.org/reading-room/whitepapers/auditing/sarbanes-oxley-information-technology-compliance-audit-1624 [https://perma.cc/8R35-8NRU].

127. *See id.* at 13; Nichole Hemmer, *SOC Audit Report Overview: The Definitive Guide* (Oct. 21, 2020), https://linfordco.com/blog/soc-audit-report-guide/ [https://perma.cc/TF4F-HF63].

128. *See About Us*, COMM. SPONSORING ORGS. TREADWAY COMM'N (Apr. 26, 2022), https://www.coso.org/SitePages/About-Us.aspx [(describing changes to the Internal Control Integrated Framework); John Lainhart, *Introducing COBIT 2019: the Motivation for the Update*, INFO. SYS. AUDIT & CONTROL ASS'N (Oct. 29, 2018), https://www.isaca.org/resources/news-and-trends/industry-news/2018/introducing-cobit-2019-the-motivation-for-the-update [https://perma.cc/69LT-TPBT] (describing the latest update to COBIT).

129. Nat'l Inst. Standards & Tech., History and Creation of the Framework, U.S. DEP'T COMMERCE (July 14, 2021), https://www.nist.gov/cyberframework/

references multiple industry standards but also connects security controls under NIST and other standards to maturity levels of an organization.[130] However, only federal agencies, not organizations, are mandated to follow NIST requirements.[131] In the event a subcontractor provides information technology for a government entity, they may be required to comply as well.[132]

For organizations implementing or maturing their cybersecurity programs, these standard-creating bodies simplify the process of creating a replicable set of controls, or internal organizational requirements. Controls originate with organizational audit functions, wherein an auditor (internal or external to the organization) evaluates whether an organization meets all internally required activities.[133] The nonfulfillment of a required activity

---

online-learning/history-and-creation-framework [https://perma.cc/32AN-P7NX].

130. *See, e.g., New CIS Critical Security Controls Mapping to the NIST CSF in a Standardized Data Format*, CTR. FOR INFO. SEC. (Dec. 10, 2019), https://www.cisecurity.org/blog/new-cis-controls-mapping-to-the-nist-csf-in-standardized-data-format [https://perma.cc/DRG3-87EE] (describing one mapping for CIS controls).

131. The Federal Information Security Management Act (FISMA) of 2002 directly regulates federal agencies, but such agencies may export these requirements via contract to their subcontractors. 44 U.S.C.A. § 3554(a)(1)(A) (West 2014) Under FISMA, government agencies are required to follow NIST. These requirements, however, are flexibly applied. FISMA specifically requires "information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized use, disclosure, disruption modification, or destruction . . . ." *Id.*

132. *See id.* at § 3552(b)(6)(A); Off. of the Chief Info. Officer, *Table 3: Federal Information Security Safeguard Requirements – Summary*, U.S. NAT'L INSTS. OF HEALTH (Jan. 14, 2010), https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Pages/table3.aspx [https://perma.cc/M7L6-HJ5T]. Although some agencies may require demonstration of compliance with FISMA, other agencies may not, depending on the election of the federal agency's director. *See* NIST Risk Management Framework, Nat'l Inst. of Standards & Tech. (Feb 23, 2023), https://csrc.nist.gov/projects/risk-management/fisma-background [https://perma.cc/WAS2-97CA].

133. *See* T.A. Lee, *The Historical Development of Internal Control from the Earliest Times to the End of the Seventeenth Century*, 9 J. ACCT. RSCH. 150-51, 150 n.2 (1971) ("Internal accounting control comprises the plan of organization and the coordinated procedures used within the business to (1) safeguard its assets from loss by fraud or unintentional errors, (2) check the accuracy and

(answering 'no' to a control framed by an audit question) results in risk to an organization.[134] Noncompliance with a control is identified as a "risk," and the controller subsequently communicates to organizational leadership, and sometimes a board of directors, for purposes of making a decision.[135]

2. The Purpose of Industry Standards in Cybersecurity

Industry standards typically exist to inform organizations of control options collectively present in a strong information security program. But they are not mandatory and allow for flexible application of specific security controls based on risk.[136] Security is not a matter of meeting one specific control, but rather the implementation of security measures that collectively reduce the risk of a cyberattack or data breach.[137] In some cases, choosing to implement some controls and not others might even be objectively reasonable for an organization's overall defensive cybersecurity posture.[138]

---

reliability of the accounting data which management uses in making decisions, and (3) promote operational efficiency and encourage adherence to adopted policies in those areas in which the accounting and financial departments have responsibility, directly or indirectly.") (quoting Paul Grady, *The Broader Concept of Internal Control*, 103 J. ACCOUNTANCY 36, 41 (1957)). The first signs of internal control and internal audits were as early as 3600 to 3200 B.C. Lee, *supra*, at 151.

134. *See* Jessica Ackerman, Theresa Koursaris, Jim Traeger & Reshma Shah, *Internal Controls and Risk Assessments: What Every Private Company Should Know*, DELOITTE (2021), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/internal-controls-and-risk-assessments-pov1.pdf [https://perma.cc/Y4ND-YPJ].

135. *See* Magali Welch, *Internal Controls – Risk Assessment*, JOHNSON LAMBERT (Sept. 19, 2017), https://www.johnsonlambert.com/post/internal-controls-risk-assessment [https://perma.cc/YPM3-M5CZ].

136. *See Cybersecurity Management: Implementing Cybersecurity Controls*, BAKER TILLY (Jan. 26, 2016), https://www.bakertilly.com/insights/cybersecurity-management-implementing-cybersecurity-controls [https://perma.cc/F2D8-ENJ3].

137. *See id.*

138. *See* Mike Davis, *Cybersecurity Risk, What Does a "Reasonable" Posture Entail and Who Says So?*, ALLIANT CYBERSECURITY (Apr. 3, 2019), https://www.alliantcybersecurity.com/cybersecurity-risk-what-does-a-reasonable-posture-entail-and-who-says-so [https://perma.cc/8X2V-AKNE].

When organizations apply industry standards with appropriate cybersecurity expertise, even if they do not implement every control, they reduce cyberattack probability while controlling cybersecurity costs.[139] If organizations applied the same requirements across all technical systems and business processes, regardless of potential risk to them, it would be tremendously expensive but not very effective.[140]

This flexibility of risk-based decisions, while potentially leading to better cybersecurity risk posture and facilitating smart business decisions, does not necessarily help organizations that are hoping to avoid downstream legal issues. A court may have great difficulty determining whether an organization actually employed reasonable security practices when a cyberattack or data breach occurs because this judgment requires engagement with context-specific risk decisions. Without courts engaging in the hard work of contextual analysis as is typical in traditional duty inquiries, organizations will likely reduce the likelihood of cyberattacks but still be exposed to considerable liability even if they actively work to avoid it.

While flexibility may be desirable, especially for prioritization purposes, the fractured and generalized nature of cybersecurity legal requirements reduces organizational confidence in a cybersecurity program's ability to avoid or reduce legal risk. If an organization's leadership has no idea whether or not they will be subject to a lawsuit or administrative investigation or whether these efforts will likely be successful, it may be tempting to not try to improve such programs. These organizations may opt instead for more comprehensive cyber-risk or cyber-liability insurance or incident response activities, which do not prevent

139. *See* Abdullah Al-Moshaigeh, Denise Dickins & Julia Higgs, *Cybersecurity Risks and Controls*, CPA J. (July 2019), https://www.cpajournal.com/2019/07/08/cybersecurity-risks-and-controls [https://perma.cc/EEH6-UMY5].

140. *See* Bob Kolasky, *A Risk-Based Approach to National Cybersecurity*, U.S. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Jan. 14, 2021), https://www.cisa.gov/blog/2021/01/14/risk-based-approach-national-cybersecurity [https://perma.cc/7NM3-AM3H] (noting that a customized, risk-based model is more effective and also is far less expensive than older models); Jim Boehm, Nick Curcio, Peter Merrath, Lucy Shenton & Tobias Stähle, *The Risk-Based Approach to Cybersecurity*, MCKINSEY & CO. 5 (Oct. 2019), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20risk%20based%20approach%20to%20cybersecurity/The-risk-based-approach-to-cybersecurity.pdf [https://perma.cc/F45W-7XUM].

cyberattacks from occurring but simply subsidize responsive activities after a cyberattack has occurred.[141]

These efforts primarily focus on response to data breaches and other cyberattacks rather than preventing them, in part because the most uniform body of cybersecurity law in the United States consists of data breach notification statutes.[142] This means that organizations will likely rather spend scarce resources responding to cyberattacks than performing or expanding core organizational activities.

A useful model for analyzing cybersecurity duty will incentivize investment in preventative activities while also enabling effective interpretation of reasonableness in a myriad of situations, including common-law legal analysis.[143] "Reasonableness" will likely continue to be referenced explicitly in statutes and private contracts but will also be examined at common law. Even where laws currently include cybersecurity requirements, these laws do not provide the necessary framework for determining contextual reasonableness.

D. Leveraging Industry Standards to Determine Reasonableness

A starting point for contextual reasonableness involves industry standardization, which involves static programmatic requirements all organizations should have. Standards bodies create standards to provide consistency—usually from the perspective of safety, efficacy, predictability, or some other goal—to all organizations that follow them. Cybersecurity standards are designed to create some degree of predictability and confidence in an organization's ability to adequately protect its technology systems.

However, if an organization implements a standard, this is not a guarantee that the technology system is protected. How a standard is implemented, and to what degree it is implemented, can be the difference between a very secure system that an attacker will struggle to compromise and a system that is easy to compromise. All cybersecurity standards

141. *See Preventing and Responding to Ransomware Attacks,* HANTZMON WIEBEL LLP (Apr. 12, 2021), https://hwllp.cpa/preventing-and-responding-to-ransomware-attacks [https://perma.cc/HXW7-ELXR].

142. *See* Tschider, *Experimenting with Privacy*, *supra* note 115.

143. It should be noted that legal scholars often debate whether more specific requirements should be included or included by reference, and whether and to what extent ex ante statutory and regulatory action should be used rather than ex post legal recovery.

incorporate some concept of risk management, which includes evaluating technology systems to identify noncompliance with *controls*, such as legal requirements or industry standard requirements.

For example, in 2019, a data breach at a chain of convenience stores and gas stations caused considerable cost to financial institutions doing business with the company.[144] Despite the company implementing industry standards required for payment cards, the Eastern District of Pennsylvania reasoned on a motion to dismiss that:

> This Court is persuaded by the [Financial] Institutions' contention that Pennsylvania law . . . imparts on companies an independent duty to reasonably secure their payment systems. [Defendant] argues that the [Financial] Institutions cannot claim that it owed them an independent duty because their Amended Complaint refers to a set of rules and industry standards that companies must comply with when processing payment card transactions.[145]

The Eastern District, relying on Pennsylvania Supreme Court precedent, found a duty to use reasonable care in safeguarding payment data separate and apart from broad industry standards that were arguably fulfilled and applied. This might demonstrate that 1) standards are not dispositive to determining duty and 2) even when standards are fulfilled, additional duties may remain.

1. Risk Assessment

Risk assessment is prescribed under most industry standards and all laws that include specific cybersecurity requirements. The purpose of requiring organizations to complete risk assessments is to enable organizations to engage in risk-based analysis of potential cyberattacks. The goal is to avoid cyberattacks that are likely to occur with significant impact to the organization (and the organization's customers or business partners). The organization examines requirements that apply to it (via industry standards or legal requirements), and if these are not satisfied, the organization identifies a "risk." This risk is then evaluated for potential mitigating activities or complete remediation.

144. *In re* Wawa, Inc. Data Security Litigation, No. 19-6019, 2021 WL 1818494, at *1 (E.D. Pa. May 6, 2021).

145. *Id.* at *5.

However, some organizations do not complete such assessments in such a way that motivates effective decision making. Therefore, the fact that an organization completes a risk assessment is not enough to demonstrate that it has satisfied its duty.

Cybersecurity practitioners dub these "risks" because they represent the likelihood of a vulnerability being compromised by some threat. Specifically, the risk identified through a risk assessment has not been realized—for now, it is just a risk of something undesirable happening, not something more. Consider the following example:

> *ArTicle is an organization that conducts live art auctions online. As part of its offerings, ArTicle promises buyers that it can maintain anonymity. ArTicle's system permits individuals to authenticate themselves for bidding purposes and obscures their identity by assigning a pseudonym named after famous artists. During an annual risk assessment, ArTicle determined that it is still authenticating users with a third-party certificate as part of its authentication process. However, the third-party certificate is no longer valid given recent cyberattacks compromising authentication systems. ArTicle determined that this risk, given recent cyberattacks and known threats to their system, has a medium likelihood of occurring and a critical impact if it does occur, which resulted in an overall "High" risk.*

Risk decisions, or what an organization like ArTicle decides to do with a specifically identified risk, may be reasonable or unreasonable depending on the potential risk of cyberattack and the type of threats, threat actors, and attackers an organization faces. Organizations prioritize decisions so that the highest-rated risks are remediated more quickly than lower-rated risks. Remediating all identified risks is often very expensive and may not actually be necessary. In other cases, based on the design of a system, complying with all industry standards might interfere with the security of a system rather than improving it.

For example, a small clothing boutique may maintain a database of 100 customer addresses it uses to distribute promotional material, and these addresses are considered personal information. A manufacturing organization may maintain a database of 100,000 supplier quotes requiring confidentiality according to contracts negotiated with these suppliers. If the industry standard or law requires both organizations to encrypt the database, which they do, and the data are later compromised, should the analysis stop? Are both organizations de facto acting reasonably? Or should courts engage with how well they encrypted the data given the potential risk? Which of these organizations is more legally unreasonable?

There is not an obvious answer because both organizations are fundamentally different: the potential threats to their systems, the size of their organizations and overall sophistication, and likely the type of data and systems they operate. Testing whether or not encryption was used does not adequately examine whether an organization was behaving reasonably because it misses important contextual, dynamic details. The database of 100 customer addresses could have been protected behind an intranet (internal network) with appropriate security controls, and access could have been limited to two people with appropriate authorization. It also does not interrogate whether the type of encryption used was appropriate given the risk, or, for example, how encryption keys are managed and rotated, all of which could dramatically increase the likelihood of compromise.

Because an attacker was successful and a standard was not met does not, without further inquiry, render an answer as to whether this behavior was reasonable. One tool that can help organizations make reasonable decisions is included in many cybersecurity standards: the risk assessment. Risk assessments help organizations determine the risks present in a well-organized, comprehensive manner. Risk assessments involve applying a control to a technology system, such as "encrypt data at rest," which is evaluated for a specific portion of technology, such as a database. To "pass" the control, the database must be encrypted. Controls originate from an authoritative source that establishes a required action, such as a law, industry standard, or internal policy.[146]

Organizational controls, then, are the source for assessment questions used to proactively measure internal compliance.[147] However, organizations could make the wrong decision given potential risk or implement these controls in an insufficient manner. Knowing whether the organization made the right decision based on the foreseeability of compromise and downstream harm, is a contextual inquiry that demands more than rote review of an industry standard.

2. Risk Decisioning

When non-compliance with an internal control results in a risk being identified, an organization rates the risk based on the impact of the risk

146. *See* LEIGHTON JOHNSON, SECURITY CONTROLS EVALUATION, TESTING, AND ASSESSMENT HANDBOOK, 5, 9 (2016).

147. *See id.*

being realized and the probability of such an impact.[148] The "impact" is evaluated in part due to the risk type, and risk types for cybersecurity-related risks are often distinct from broader business risk types.[149] As described above, many enterprise risk management models involve evaluation of probability times impact, or *P x I = R*, which informs the risk rating.[150]

Risk, then, is positioned as risk of a threat, such as an attacker, compromising the technology system. For example, an e-Commerce business collects customer data for purposes of placing orders and selling merchandise. As part of that process, payment information may be collected to facilitate a transaction and charge a credit or debit card or payment function like PayPal. An account may be created to facilitate this and future transactions that includes shipping and contact information, as well as previous purchase history.

When the e-Commerce business attempts to identify potential cybersecurity risks, it considers the e-Commerce website's potential risk of cyberattack or data breach given a specific control. For example, if a control requires encryption of all order data entered by the purchaser as it is transmitted to backend systems, the e-Commerce business would assess how a lack of encryption might expose systems and information to cyberattack or data breach. The e-Commerce business might identify that a cyberattack or data breach could expose customer data for sale on the Dark Web, exposing it to potential identify theft. A cyberattack could also compromise availability of the e-Commerce website, leading to sales losses; or entail the exposure of confidential third-party data, which could lead to legal liability.

148. *See* Jim Kent, *Risk = Likelihood x Impact*, CIO (Aug. 23, 2016), https://www.cio.com/article/3111304/risk-likelihood-x-impact.html [https://perma.cc/UB3M-6UZZ].

149. *UW-Madison's Risk Management Framework*, UW-MADISON INFO. TECH. (Dec. 9, 2016), https://it.wisc.edu/wp-content/uploads/RMF-Infographic_12-09-2016_FINAL.pdf [https://perma.cc/KD82-SVN6].

150. *See Risk Taxonomy*, OPEN GRP. 11 (Jan. 2009), https://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf [https://perma.cc/RGR4-CP3V]. Although Impact x Likelihood = Risk is a common short-hand for risk calculation, impact and likelihood, even for non-legal risk calculations are difficult to make. Loss Event Frequency, Threat Event Frequency, Control Strength, and Probable Loss Magnitude are all examples of specific calculations that must be made to accurately reflect potential risk. These are even more difficult to determine when considering risks from the perspective of legal risk. *See id.* at 11-16.

The assessed risk of compromise is an internal organizational construct intended to identify risks and make decisions about organizational financing priorities. However, risk assessments consider a variety of inputs simultaneously—such as strength of controls in place and likelihood of compromise—that can actually illustrate reasonable cybersecurity decision making. These facts can be tremendously useful when analyzing whether an organization's decisions were reasonable, at least subjectively, to them. Although only applicable for common-law torts, such as negligence actions, understanding whether an organization subjectively believed risk of compromise was high can certainly provide evidence related to foreseeability, a critical determination for intervening criminal cyberattacks.

The applicable industry standard practices and information about the risk of compromise is also useful in determining whether such activities are objectively reasonable. Implementation (or not) of corrective, remedial measures in response to reasonably foreseeable risk and consideration of the dynamic, contextual environment of organizational activities, technology, and potential threats could demonstrate reasonable duty.

Fulfilling reasonable cybersecurity practices requires at least three actions. First, organizations must engage in programmatic cybersecurity practices that are based on controls. Second, the organization must engage in risk assessment processes to determine whether such controls are effectively met. Third, organizations must actively make decisions about risk, and the decisions must be reasonable with respect to the likelihood and potential impact, which includes organizational knowledge, prioritization of significant risks, and anticipation of known threats.

PART III: WHY CYBERSECURITY LAW NEEDS REFERENTIAL STANDARDS OF ACCEPTABLE BEHAVIOR

As described in Part I, broad duties, even duties established through statute, are not necessarily specific. Duties of all kinds are expounded upon administratively or established via litigation and developed precedentially in the common law for a variety of non-cybersecurity activities, such as those impacting public safety. However, cybersecurity duties today are not readily examined. In response, cybersecurity scholars have explored alternatives to identifying some reliable source of information for organizations to anticipate cybersecurity duty, such as administratively-

created duties established through consent decrees and orders.[151] Most promising thus far has been William McGeveran's claim that statutory and administrative law, as well as private ordering, are already converging on a principles-based consensus.[152]

However, as Gus Hurwitz has observed, despite McGeveran's description of an objective standard, duties should be contextualized both as objective and subjectively reasonable.[153]

This Article seeks to incorporate the perspectives of both of these scholars by proposing a new, two-part approach to establishing reasonable duty for courts and administrative agencies. The first step is an analysis of static duty based on industry standards. The second is an inquiry into dynamic duty, a context-dependent assessment that depends on the risk facing a particular actor.[154]

A. Two-Part Duty Analyses

A two-part analysis of static duty and dynamic duty, as explained in this Part and Part IV, could be used in a variety of ways depending on the doctrinal legal approach and court precedent. For example, a two-part *test* may not be useful or compatible with all doctrinal areas, even if an *analysis* could be instructive or useful. Some doctrinal areas could benefit from a two-part analysis to structure examination without a test, such as contract

151. While very astute scholars have examined the role of the Federal Trade Commission in creating a common law for privacy, ultimately administrative law functions quite differently than litigation, and such an approach for cybersecurity has reached substantial roadblocks absent overt administrative rulemaking. *See* Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) (describing the role of the FTC with respect to administrative actions, mainly involving privacy activities); *c.f.* Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955 (2014) (describing the differences between administrative action and the common law, especially in relation to security rather than privacy actions).

152. William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1143-44 (2019). Due to the sparsity of cases describing duty at the time of writing, Professor McGeveran's analysis of duty focused principally on standards, professional education, and statutory language.

153. Justin (Gus) Hurwitz, *Response to McGeveran's the Duty of Data Security: Not the Objective Duty He Wants, Maybe the Subjective Duty We Need*, 103 MINN. L. REV. HEADNOTES 139, 155 (2019).

154. *See infra* Parts III and IV.

law, regulatory investigations, or allegations of breach of fiduciary duty; whereas other areas like tort might benefit from a more formal two-part test. In order to understand how this analysis or test could be used, this Section describes how duty is established in each doctrinal area and how a cybersecurity duty could be evaluated.

1. Statutory Requirements & Administrative Enforcement

A variety of administrative agencies regulate cybersecurity at the federal and state levels. In the statutory context, duty is typically created by the text of the law, but administrative agencies often interpret the specific application of that duty contextually. They may do this formally through rule-making pursuant to the Administrative Procedure Act,[155] which includes a formal notice and comment period. Or agencies may signal their expected enforcement approach less formally, such as by publishing non-binding guidance.

Administrative agencies could be described as engaging in interpretation and construction as part of the process of investigating statutory compliance.[156] Whether or not agencies officially engage in interpretation and construction, they nevertheless do evaluate and interpret the statutory requirement, which they then apply to the context being evaluated. The interpretation step is informed by the agency reviewing its rules and guidance to interpret a statute, then applying it to the specific organization required to follow the statute. This naturally maps to discussions identifying a fixed standard and how that standard applies to a given situation.

David Thaw, applying Cary Coglianese and David Lazer's "management based regulatory delegation," describes a balance of cybersecurity standards with some flexibility in their application as most desirable.[157] Management based regulatory delegation identifies the contours or obligation to manage a program without specifically mandating detailed requirements within a program. This approach offers substantial flexibility for organizations to determine which requirements to employ and when.

155. Administrative Procedure Act of 1946, 5 USC § 551.

156. *See* Frederick Schauer, *Constructing Interpretation*, 101 B.U. L. REV. 103, 105 (2021).

157. As Thaw explains, the goal is flexibility with accountability, rather than direct regulation (or specific requirements via statute). David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 324 (2014).

Most statutes use this approach, including more prescriptive statutes like HIPAA.[158]

Most statutes and many private contracts reference flexible, "reasonable" security practices, and some require "best practices." Management-Level Regulatory Delegation, as Thaw explains it, is a regulatory approach where administrative agencies enforce broad regulations designed to promote internal organizational cybersecurity management proactively.[159] For example, Management-Level Regulatory Delegation involves regulations and the agencies enforcing them to permit some flexibility and selectivity in how organizations actually follow the law. This can include both planning and implementation of such activities.

Although this approach presumes that a statute or regulation exists (rather than only the common law), a hallmark of Management-Level Regulatory Delegation is that it creates contours of statutory duty while leaving specific decisions to each organization, with evaluation from agencies as to the sufficiency of those decisions.[160] Under some regimes, organizations may be required to produce documentation that demonstrates how the organization has met general duties.[161] Management-Level Regulation typically is used when an organization is best positioned to make decisions about risks and potential controls to mitigate them.[162]

However, assessing whether organizations act reasonably is not necessarily easy. As Thaw notes, regulatory enforcement actions often demonstrate a "race to the bottom," where organizations meet the requirement specified while simultaneously operating ineffective, insecure cybersecurity programs likely to experience a cyberattack or data breach.[163] Indeed, the size, scope, and complexity of an organization may affect what

158. *See id.* at 324-27.

159. *Id.* at 308, 324. Indeed, cybersecurity laws heavily rely on "reasonableness" requirements, which are not well-known or developed in the cybersecurity context. *Id.* at 309, 325 n.166.

160. *See* Cary Coglianese & David Lazer, *Management-Based Regulation: Prescribing Private Management to Achieve Public Goals*, 37 LAW & SOC'Y REV. 691, 694 (2003).

161. *See id.*

162. *See id.* at 695.

163. *See* Thaw, *supra* note 157, at 368.

cybersecurity controls are reasonable,[164] without even beginning to incorporate foreseeable threats and associated risks.

The HIPAA Security Rule establishes required and addressable statutory duties, and these discrete requirements are broadly written, very similar to industry standards.[165] Under 45 C.F.R. § 164.306(b), the Security Standards: General Rules, Flexibility of Approach, the Department of Health and Human Services established that covered entities and their business associates may consider their organizations' capabilities and potential risk when determining how to implement the security rule duties.[166]

Security Rule requirements to conduct risk assessments and engage in risk management activities enable regulated organizations to make context-based decisions.[167] The Office of Civil Rights (OCR), which enforces HIPAA, appears to be implementing some form of contextual analysis in its resolution agreements following investigations. One HIPAA Business Associate, CHSPSC LLC, agreed to pay a substantial fine of $2.3 million and implement corrective measures under its resolution agreement.[168] The breach involved an Advanced Persistent Threat compromising a VPN using administrative credentials they gained.[169] In completing the investigation, OCR determined that CHSPSC had not effectively monitored its systems

164. *See id.*

165. 45 C.F.R. §§ 160, 164; *see* Tschider, *supra* note 28, at 1505.

166. 45 C.F.R. § 164.306(b).

167. 45 C.F.R. §§ 164.308(a)(1)(ii)(A) to (B); U.S. DEP'T HEALTH & HUM. SVCS., HIPAA SECURITY SERIES 4 SECURITY STANDARDS: TECHNICAL SAFEGUARDS (Mar. 2007), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf#:~:text=The%20Security%20Rule%20defines%20access%20in%20%C2%A7%20164.304,rights%20as%20specified%20in%20%C2%A7%20164.308%28a%29%284%29%5BInformation%20Access%20Management%5D.%E2%80%9D [https://perma.cc/9WXD-47YA].

168. Resolution Agreement #14-189589, CHSPSC LLC, U.S. DEP'T OF HEALTH & HUM. SERVS. 2 (Mar. 30, 2020), https://www.hhs.gov/sites/default/files/chspsc-ra-cap.pdf [https://perma.cc/AW8P-U5X4]. Resolution agreements, like consent decrees and orders, are settlements between the organization and the administrative agency and do not have direct force of law.

169. *Id.* at 1.

(amongst other issues), despite receiving notice from the FBI of system compromise.[170]

Notably, HIPAA requires "log-in monitoring" as an addressable requirement but does not offer any other specificity as to what is sufficient or insufficient log-in monitoring.[171] Despite this, OCR determined that CHSPSC was obligated to conduct monitoring in such a way that it could have reasonably prevented the VPN compromise.[172] This example illustrates that administrative enforcement, *even if* a statute establishes a specific duty, will necessarily evaluate an organization based on contextual, dynamic, and responsive behavior, not simply whether the organization has met the statutory requirement.

Statutes may be enforced by an administrative agency or may permit a private right of action. For example, the California Consumer Privacy Act (CCPA) permits a private right of action when:

> Any consumer whose nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action [. . .][173]

In this statute, California references a "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[174] However, a court interpreting duty within this context still must ascertain what is reasonable. Statutes calling for reasonableness could similarly use the static and dynamic duty inquiries to examine reasonableness.

This is precisely how organizational cybersecurity risk management functions from a business and technical perspective. Not only are organizations best positioned to make risk and control decisions, but many

170. Press Release, U.S. Dep't Health & Hum. Svcs., HIPAA Business Associate Pays $2.3 Million to Settle Breach Affecting Protected Health Information of Over 6 Million Individuals (Sept. 23, 2020), https://www.hhs.gov/about/news/2020/09/23/hipaa-business-associate-pays-2.3-million-settle-breach.html [https://perma.cc/P9NS-GT3M].

171. 45 C.F.R. § 164.308(a)(5)(ii)(C).

172. *See* Resolution Agreement #14-189589, *supra* note 168, at 1-2.

173. California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.150(a)(1) (West 2023).

174. Id.

are already making these decisions today.[175] Organizations must make judgment calls regarding various types of risk. They must allocate resources to remediate some but not all issues based on risk to customers, employees, or the organization itself as it manages its compliance plan.[176] Often these decisions are informed by overall cost to remediate issues that could increase the probability of a cyberattack occurring and finding an optimal blend of expense versus risk. These internal decisions' reasonableness will very likely be questioned after a cyberattack occurs.[177]

175. Despite the fact that many organizations do make risk-based decisions related to cybersecurity, there are several organizations that do not. *See* Dan Lohrmann, *Why Many Organizations Still Don't Understand Security*, GOV'T TECH. (Feb. 23, 2019), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/why-many-organizations-still-dont-get-security.html [https://perma.cc/WF9T-SW96]; *Why You Need A Cybersecurity Management Program*, CYBERSECOP, (Mar. 6, 2019), https://cybersecop.com/news/2019/3/6/why-you-need-a-cybersecurity-management-program [https://perma.cc/6LTN-VEYE]; Steve Ursillo, Jr. & Christopher Arnold, *Cybersecurity Is Critical for All Organizations – Large and Small*, INT'L FED'N OF ACCTS. (Nov. 4, 2019), https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small [https://perma.cc/3AJ3-GLU4].

176. Indeed, no organization practices "perfect" legal compliance. Tradeoffs are often analyzed as organizations make decisions about risk. The absence of perfect compliance does not necessarily mean that an organization's practices are incomplete, unsubstantial, or even unreasonable. Indeed, compliance professionals use the concept of reasonableness to determine what actions are necessary. *See* Mark P. Ruppert, *Roles and Responsibilities – Corporate Compliance and Internal Audit*, ASSOC. OF HEALTHCARE INTERNAL AUDITORS 2, 4 (Apr. 5, 2006), https://ahia.org/assets/Uploads/pdfUpload/WhitePapers/AuditCompliance-RolesResp04052006.pdf [https://perma.cc/6R8C-4GTL]. Under the common law, it becomes even more challenging to ascertain what reasonableness looks like without any statutory scaffolding, which is typically how corporate compliance programs manage and make decisions about reasonableness related to risk.

177. Even the National Institute for Standards and Technology (NIST), the regulatory agency responsible for establishing technical standards, including cybersecurity standards, acknowledges different cybersecurity maturity levels, flexible control applications, and risk-based decisioning. NAT'L INSTITUTE OF STANDARDS & TECHNOLOGY, NIST RISK MANAGEMENT FRAMEWORK (2022), https://csrc.nist.gov/projects/risk-management/about-rmf [https://perma.cc/QP2X-A9DJ].

2. Administrative Enforcement of Broad Duties

The Federal Trade Commission (FTC) has communicated its desire to protect consumers from poor security practices.[178] The FTC handles two key areas of the law: antitrust and unfair or deceptive trade practices from the perspective of the consumer.[179] Enforcement of cybersecurity issues largely extended from data breaches involving personal information, framed by the FTC as "unfair or deceptive trade practices" under Section 5 of the FTC Act.[180] Basically, duties here are analyzed in the reverse: when an organization has not fulfilled its duty to consumers by engaging in unfair or deceptive trade practices.

Section 5 confers broad latitude to define what "unfair or deceptive" trade practices mean, but the lack of specificity has created problems for cyberintrusion and data breach administrative enforcement.[181] Although the Third Circuit federal appeals court in *FTC v. Wyndham Worldwide Corp*[182] established that the FTC could regulate security requirements under Section 5, the Eleventh Circuit in *LabMD v. FTC*[183] held that to regulate security, the FTC needed to establish specific security obligations in the form of administrative rules so that organizations have appropriate notice.[184] To date, the FTC has not established any specific cybersecurity requirements (other than data breach notification).[185]

178. *See* Charlotte A. Tschider, *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENV. U. L. REV. 87, 129 (2018).

179. The Federal Trade Commission Act of 1914, 15 U.S.C. § 45(a)(1).

180. *Id.*

181. Daniel Solove & Woodrow Hartzog, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. Rev. 2230, 2246-50 (2015) (describing challenges to the FTC's authority in *Wyndham* and *LabMD* cases, not only in relation to the imprecision of Section 5 but also critiques related to actual consumer harm).

182. 799 F.3d 236 (3d Cir. 2015).

183. 783 F.3d 814, 824 (11th Cir. 2018).

184. So far, state attorneys general have not been restricted in their ability to enforce state unfair and deceptive trade practices laws. However, the frequency of their enforcement is still subject to administrative discretion, making these decisions difficult to interpret for purposes of legal risk evaluation.

185. 45 C.F.R. §§ 164.400-414.

Under Magnuson-Moss, the FTC is required to publish both an Advanced Notice of Proposed Rulemaking and a Notice of Proposed Rulemaking, both of which must be submitted to congressional oversight committees. The law also requires an informal hearing that permits cross-examination rights to interested parties.[186] The process is arduous and likely to reduce the likelihood of successful rule passage or at least timely passage.[187]

Despite criticism of these limitations, the FTC has recently announced its intention to press on in the form of a cybersecurity ANPR, which should permit the FTC to engage in rule-making related to the topic.[188] In the event the FTC is successful in its ANPR, a two-step duty analysis, later passed as a rule under the CFR, could potentially give the FTC the ability to analyze unfair or deceptive trade practices related to cybersecurity and create the structure called for in *LabMD*.

3. Fiduciary Duties

Although a breach of fiduciary duty may be analyzed differently depending on the type of fiduciary, for example if someone is a physician or an attorney, all fiduciaries are required to act within their specialty with a duty of expertise, care, confidentiality, and loyalty. These duties are established through a standard (as in 'standard of care') as well as the context and nature of the relationship.

For physicians, a duty of care involves using information provided by professional medical associations (like the American Medical Association) and established by independent research and publication.[189] In order to demonstrate that they did not fall below the independent standards establishing a duty of care, physicians must use the prevailing standard of care at that time; standards of care are designed to evolve as medicine evolves.

186. Jeffrey Lubbers, *It's Time to Remove the 'Mossified' Procedures for FTC Rulemaking*, 83 GEO. WASH. L. REV. 1979, 1982-83 (2015).

187. *Id.* at 1997.

188. FED. TRADE COMM'N, Trade Regulation Risk on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, (proposed Aug. 22, 2022) (to be codified at 16 C.F.R. 464 (2022).

189. Other duties of care, such as those for attorneys, are informed by national and state standards through the American Bar Association and state bar associations. The financial services field is similarly regulated.

However, an inquiry regarding the standard of care involves information about the patient and the condition—contextual information that is relevant to a full analysis. For example, if a patient has an undesirable outcome after knee surgery, the court will evaluate whether 1) the doctor used the proper standard of care when completing the knee surgery, and 2) whether the doctor considered the patient's individual risk factors and appropriately advised the patient of the risks.

Duty of care is evaluated in much the same way as a two-step analysis for cybersecurity duty could also be evaluated. Cybersecurity is a natural part of both duties of confidentiality (for data breaches) and care (for other cyberintrusions). For example, if an attorney does not adequately employ reasonable cybersecurity practices (or does not hire someone to do so), and client confidentiality is compromised, a plaintiff may argue that the attorney did not take proper precautions to protect their confidentiality. Duties of care could also be breached. Consider the following example:

Apostle Health Services is a religiously affiliated non-profit health system that contracts with a third party, ApexSolutions, which has created an electronic medical records application and bespoke storage solutions for its customers. ApexSolutions permits local AHS doctors to change permissions for their individual patients. Dr. Evan Jacobi recently set permissions for these records to include access to all people with a "link" to the records. An attacker used the link to access files, escalated their provisions to include edit features, and proceeded to delete and change a variety of medical record details. As a result, Dr. Jacobi's patients received incorrect medicine, resulting in at least one death and two serious allergic reactions. If patients (or decedents suing on their behalf) experiencing harm bring a malpractice case or another breach of fiduciary duty, has Dr. Jacobi satisfied his standard of care or confidentiality for these patients?

In the event cybersecurity practices are part of this analysis, it would make sense that these practices would also be subject to an analysis of the standard and the context of applying that standard. This means that standards must exist somewhere, if not in professional standards at least in available research or continuing education.

4. Contractual Duties (Obligation)

As described in Part II, contractual duties are established: 1) by private contract between organizations; 2) between a regulated organization and its third parties, with specific duties established by statute; or 3) by quasi-contract between a business and an individual person (e.g. corporation and consumer).

In the first and second instances, contract law leaves almost all obligations specified to the determination of the parties. Courts in almost all circumstances seek to uphold the meaning and intention of the parties as written in the contract, through the plain meaning rule and parol evidence rule.[190]

For non-goods contracts, such as technology service agreements that might be impacted following a cyberattack, these rules collectively establish that 1) the writing of the contract controls and 2) at least in the majority of jurisdictions, a court determination of ambiguity of a term on its face (within the "four corners" of the contract) means that parol evidence can be admitted.[191] Parol evidence is admitted in the following order: 1) performance under this contract (course of performance), 2) performance between the parties under other contracts between them (course of dealing), and 3) usage of trade.[192] For goods contracts organized under the UCC, parol evidence may always be admitted to explain existing terms in the same order.[193]

Contractual cybersecurity terms as duties to be performed can take a lot of forms. They may be very specific, such as "implement the newest version of Transport Layer Security when transmitting customer data." Conversely, these terms may be very general and subject to interpretation, such as "use reasonable cybersecurity practices to protect customer data," or even a generic confidentiality provision.

---

190. Joshua M. Silverstein, *Contract Interpretation and the Parol Evidence Rule: Toward Conceptual Clarification*, 24 CHAP. L. REV. 89, 143, 156, 164 (2020) (describing the movement from ambiguity to contextualism as the legal justification for exploring outside an agreement under the parol evidence rule).

191. Courts will not engage in any discussion of the meaning of such terms unless several bars have been cleared first. For example, a claim for breach of contract must be premised on which terms have been breached, and those terms must be material to the contract. Because often these terms might be boilerplate, not actively negotiated or redlined, or added very late in the process, it is possible that courts may not consider these terms material and therefore breach of contract claims could be dismissed on a motion to dismiss before any discussion of term meaning actually occurs. Although this article does not examine the details of these impediments, duty analysis will likely occur for cases where it is more possible to overcome any affirmative defenses of non-materiality.

192. *See* Schauer, *supra* note 157, at 122.

193. Uniform Commercial Code § 1-303 (AM. LAW INST. & UNIF. LAW COMM'N 2001).

These terms may also reference some standard without giving many specifics. For example, if the contract specifies that "STK Enterprises [Sub-contractor] shall implement industry standard authorization controls," and later STK Enterprises is sued by their business customer for breach of contract after a successful cyberattack, a court needs, courts need a model for determining whether the term was fully performed. Fortunately, interpretative rules have already been established for contracts, which means that courts can defer to these rules when examining the term in question.

For terms that are specific, courts may still engage in contextual analysis regarding how they have been performed and whether nonperformance amounts to a breach of contract. For example, courts examining non-goods contracts accept the principle of substantial performance, wherein performance may be determined by the courts to be functionally the same as what is required by the contract.

When analyzing performance, courts may use evidence at will because they are determining whether the settled contractual term has been performed, rather than interpreting the term itself. However, courts must analyze whether, given the facts, an organization has actually performed. Because even facially specific cybersecurity terms can be performed differently (and, without further inquiry, such performance could seem substantially interchangeable), this means that courts can use a two-step analysis even when an interpretation of the term itself is not needed. Consider the following example:

> *BrainFood Education [Service Provider] shall implement asymmetric encryption for its products with Customer, including a salted hash.*

Here, the terms are very specific: asymmetric encryption is more specific than just "encryption," and a salted hash is a method for employing asymmetric encryption that is arguably more secure. However, there are far more details in this term's performance that could demonstrate a party has not actually met these requirements, details that create a more secure system and details that do not.

In contract law, courts then will evaluate, given the term established, whether such a term was implemented reasonably, given the principles of good faith and fair dealing impliedly part of every contract and plausibly in keeping with the term specified. This is where courts already are engaging in contextual analysis in performance even if a term is reasonably specific.

For contracts established according to statute and where a statute establishes the terms, courts can either 1) defer to administrative interpretation according to the prevailing Supreme Court views at the time or 2) engage in interpretation of the term as applied to the given situation

and assess performance of the term.[194] Because a variety of laws could be explicitly referenced in the contract, not all laws could be interpreted in the same way. For example, the General Data Protection Regulation requires organizations transferring European Union (EU) residents' personal information outside of the EU to execute contractual clauses that enforce provisions within the GDPR.[195] The GDPR does not currently offer much specificity on cybersecurity, except for requiring "reasonable administrative and technical measures" and encouraging practices like "encryption."

If a court in the U.S. is hearing a breach of contract case where the basis of the breach involves mandatory contractual clauses, it might have to engage in some interpretation of that term, which could also use a two-step model for analysis, rather than deferring to what the GDPR's enforcement body, the European Data Protection Board (EDPB), has suggested but does not require.

Finally, quasi-contract, or a contract implied in fact, might offer another avenue for courts to engage in cybersecurity duty analysis. Consumer protection statutes and other statutes, such as HIPAA, require organizations to disclose their data handling practices in the form of a privacy notice.[196]

---

194. This Article does not engage deeply in the topic of administrative deference, and indeed this will be contingent on language within the statute as well as prevailing Supreme Court views on administrative deference. *See* Yoav Dotan, *Deference and Disagreement in Administrative Law,* 71 ADMIN. L. REV. 761, 765 (2019); Timothy Sandefur, *State Courts Are Growing Increasingly Wary of Administrative "Deference*," GOLDWATER INSTITUTE (Aug. 27, 2020), https://www.goldwaterinstitute.org/state-courts-are-growing-increasingly-wary-of-administrative-deference/ [https://perma.cc/5JQY-L8ZF].

195. *See* Council Regulation 2016/679, 2016 O.J. (L 119). Although other conditions of transfer exist, such as transfer within the European Economic Area, within an organization across geographies through Binding Corporate Rules, or to another country that has achieved adequacy status through the EU, contractual clauses (sometimes called standard contractual clauses or model contractual clauses) are favored for most organizations and are used extensively. Directorate-General for Justice and Consumers, *Standard Contractual Clauses for International Transfers*, EUROPEAN DATA PROTECTION BOARD (June 4, 2021).

196. Contract law has not historically provided a great avenue for regulating privacy specifically, but privacy notices are still required by state and federal laws, which means that at least some disclosures could be made upon which individuals might use to recover. *See* Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy*

Alternatively, organizations may choose to provide services or goods subject to terms of use, click or browse-wrap agreements, or other one-sided contracts of adhesion.[197] Cumulatively, these contracts may or may not be enforced as contracts binding an individual person, but they frequently are binding upon the organization that executed it.

Organizations are frequently including references to cybersecurity in these quasi-contracts. For example, organizations may include language like the following:

> Throttle Watersports uses reasonable cybersecurity practices to protect your personal information. However, we do not guarantee security in all cases.

In the event a consumer's data was compromised in a data breach involving Throttle, a court would likely first determine whether—in reading both the reasonable cybersecurity duty and the disclaimer together—a duty was owed the consumer. In the event a duty is owed, the court would again need to determine whether the term is ambiguous, and what interpretative approach could be taken.

Because we are dealing with consumer quasi-contracts, it is unlikely that course of performance or course of dealing would apply. Rather, courts would engage in identifying the industry source of information, or usage of trade, to define this term. Similar to all interpretive activities, courts could determine the usage of trade not just by looking at standards but how and under what circumstances it is applied.

Across all of these scenarios, a common denominator is that usage of trade can be used to explain ambiguous terms, but additional contextual information is needed about what the term really is and whether or not the defendant performed consistent with the term the court has defined. In this way, definition of duty and determination of whether it has been performed is a two-step analysis, which would benefit from both fixed and contextual information.

5. Negligence & Negligence Per Se

As described in Part II, negligence and negligence per se require a consideration of duty as part of the plaintiff's prima facie case requirement. Similar to contracts that incorporate statutory language, negligence per se

---

Protection Model, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 181, 189-90 (2016).

197. THOMPSON REUTERS PRACTICAL LAW, *Browsewrap Agreement* (2023).

incorporates duty from a statute with a private right of action rather than asking courts to determine duty from the perspective of reasonably prudent person. It might seem that if a defendant can demonstrate it followed the law, that the defendant might successfully affirmatively defend this claim.

However, even negligence per se claims require a factual inquiry into whether the statutory requirement is met. For example, under the CCPA, plaintiffs could bring a cause of action when a defendant fails to use reasonable security practices to protect their personal information. A plaintiff bringing this claim would need to illustrate how these practices were unreasonable, or how the defendant had breached their statutory duty.

To decide a case that proceeds to trial, courts could accept that the statute establishes a duty. However, as under the CCPA, courts will need to determine what "reasonable security practices" means not only from the perspective of a defendant expected to follow this, but potentially involving interpretive information about the practices at a high level that are expected by California's Attorney General. In addition, whatever these practices are, they must not be considered in the abstract. To determine whether the defendant's conduct was, in fact, reasonable under the circumstances, courts must consider defendant's implementation of the practices and the corresponding risk profile.

For negligence cases that make it to trial, courts will engage in a similar analysis. This analysis involves determining whether a plaintiff-identified duty (for example, a duty to protect personal information transmitted over the open Internet) is a duty that would apply to this organization and that a reasonably prudent person (organization) in the same position would have owed the plaintiff.[198] Then, courts engage in a discussion of whether the duty was performed or whether the duty was breached.[199]

The biggest challenge in this analysis is determining the type of (reasonable) duty owed, a duty that is informed both by duties that everyone must perform with respect to others and duties that may be specific to the situation. For example, a driver owes a general duty of safe-driving behaviors—such as driving the speed limit or below—to other drivers, passengers, pedestrians, and property owners. If someone is harmed or something is damaged and the driver was driving above the speed limit, courts would likely find the driver negligent. However, if the

198. *See* Benjamin C. Zipursky, *Reasonableness In and Out of Negligence Law*, 163 U. PENN. L. REV. 2131, 2136 (2015).

199. David G. Owen, *The Five Elements of Negligence*, 25 HOFSTRA L. REV. 1671, 1675-77 (2007).

driver was driving under the speed limit, the case is not automatically dismissed. Rather, a plaintiff may have to show more, and courts may have to analyze more than what the standard or law said at the time. A plaintiff could show that it was snowy and icy that day, conditions under which a reasonably prudent person would have taken greater care and slowed down significantly.

As Benjamin Zipursky observes, the use of reasonableness in negligence demands a moderation and restraint that would not come from blankly applying a "clear-cut attribute":

> Not only do these ['reasonable'] qualifiers ensure that it is a moderate level of the quality being designated, they also ensure that one applying the law (be it legal actor or judge) is being guided in a manner that requires the exercise of judgment.[200]

Cybersecurity questions are no different. Conditions change and demand greater diligence and performance in some situations as compared to others. Specifically, the concept of reasonableness as encapsulated in so many laws and doctrinal concepts is inextricably linked, at least for cybersecurity practices, with foreseeable risk.

B. Reasonableness and Foreseeability

Organizations should be held accountable to general standards with an opportunity for some justifiable discretion. This type of model is analogous to contractual relationships with implicit freedom to contract, a corporate officer's obligations to shareholders (informed by the business judgment rule), and tort-based relationships, whether fiduciary or simply reasonable duties (with reasonable duty of care). Discretion, as illustrated by risk management programs involving risk assessment and decisioning is where both objective standards and subjective risk-based decisions are relevant.

If cyberattacks are, at least for some attack types, inevitable or at least extremely difficult to prevent, organizations that reasonably reduce the probability and impact of cyberattacks and data breaches may well be meeting their foreseeable duty, even if injury later occurs. This model makes logical sense, too: if complete prevention of all cyberattacks and data

200. *See* supra note 198, at 2146.

breaches is nearly impossible, organizations must only protect against reasonably foreseeable harm or risk of harm.[201]

Reasonable foreseeability is crucially important in evaluating duty, because the organization does not directly cause the harm or risk of harm. Rather, it is the absence of some reasonable action that creates an opening for intervening criminal behavior that directly causes harm or risk of harm. When that harm or risk of harm is foreseeable, depending on the jurisdiction, organizations may be required to perform some reasonable duty to prevent it.[202]

Foreseeability is important in other bodies of law, too, where it applies to the concept of reasonableness. For example, in contract, a contractual term requiring "reasonableness" presumes that the obliged party has some concept of what reasonableness will mean: referenced in the contract, subjectively decided and established through parol evidence, or objectively informed by industry standard to explain it.[203] The final preferred interpretive approach to parol evidence—usage of trade—may well be relied upon heavily in cybersecurity litigation because many parties do not contemplate or discuss cybersecurity practices prior to contracting.[204] Understanding what industry standards might apply to the usage of trade

201. Whether harms are calculated based on actual harm or future risk of harm depending on how the courts begin to accept such harms as the basis for claimed injury. *See* Solove & Citron, *supra* note 26, at 756-61 (describing risk as harm).

202. CACI No. 432. *Affirmative Defense – Causation: Third-Party Conduct as Superseding Cause*, Judicial Council of California Civil Jury Instructions (2022), at 230-232 (describing the varying ways in which foreseeability of specific risks in a particular circumstance may be included in tort analysis as distinct from duty analysis).

203. The difference in use of parol evidence between non-UCC subject matter (Restatement-informed state statute) and UCC subject matter does not matter for our purposes. *If* a court is analyzing cybersecurity terms, such as "reasonable" or other general, standards-level terminology, it could use a similar two-step analysis.

204. Both in Restatement and UCC, usage of trade is the least preferred interpretive tool, with the meanings of the parties established through multiple performances or multiple alternative contracts preferred over usage of trade. This model makes sense in that private contract involves private ordering – two parties decide what the rules will be. Using a two-step analysis applies only when internal rules to not reveal what the parties actually meant within the contract and is not intended to supersede private meanings in these agreements.

interpretation, and under what circumstances, takes a degree of foreseeability of potential risk of compromise to apply these standards in an optimal manner.

Although reasonableness can be evaluated based on foreseeable risk, risk is difficult to measure without an internal process for doing so. Organizations may have even more trouble anticipating potential legal risk and avoiding it because they lack appropriate information to anticipate issues. First, organizations do not always know whether a control is actually required by law,[205] unless it is established in statute which, as discussed in Part II, may not occur. Second, organizations do not know whether, and with what probability, failing a control will result in an administrative fine or court action.[206] Neither of these issues actually promote better cybersecurity for organizations and people affected by cyberattacks, yet this is how organizations may analyze cybersecurity issues.

Even where a statute offers a legal requirement, failing to pass the requirement in a risk assessment and deciding not to remediate the risk may not measurably influence the frequency of a data breach at all. Risk factors—such as whether a particular vulnerability has been used to perpetuate an advanced persistent threat-based attack (an attack that requires several steps and often does not turn on the ineffectiveness of just one control) are inherently dynamic[207] Effective risk identification, followed by risk rating, prioritization, and remediation, largely turns on having accurate, reasonably predictive information to feed into risk rating models.[208]

205. *See* OPEN GRP., *supra* note 151, at 23.

206. *Id.* at 17. Note that a typical input for legal risk is "fines and judgments." Without any useful data for predicting fines and judgements, even a more quantitative model for risk analysis can fall short in approximating legal risk.

207. Nate Lord, *What is an Advanced Persistent Threat? APT Definition*, DATA*INSIDER* BLOG (Sept. 11, 2018), https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition [https://perma.cc/AX3T-BK9A].

208. Some risk rating methodologies have reconceived of this by integrating an "additive" model of risk evaluation, weighs different factors in coming to a risk rating and, following, prioritization. However, these models still require some information be added. A lack of an effective model for legal risk identification is a critical issue for these models, as well. *See, e.g.*, Shawn A. Butler & Paul Fischbeck, *Multi-Attribute Risk Assessment*, PROC. OF SYMP. ON REQUIREMENTS FOR ENG'G FOR INFO. SEC. (2002), http://www.cs.cmu.edu/~Compose/butler-fishbeck-02.pdf [https://perma.cc/7XT6-VC67] (generally describing the varieties of factors influencing accurate risk assessment).

C. Practicing Reasonableness

Cybersecurity practitioners know well that effectively evaluating risk is a key aspect of effective risk remediation and prioritization, that is, determining what to fix in what order given limited organizational resources. Risk prioritization is central to any organizational decision.[209] The concept of remediation and prioritization planning presumes that an organization does not have unlimited capital to spend and that decisions are made by considering potential operational, reputational, financial, and legal risks. This means that sometimes cybersecurity decisions are made to avoid organizational impacts that have no legal impact at all. Courts evaluating whether practices are reasonable must have some understanding of the ecosystem of organizational priorities to better determine whether a decision was ultimately reasonable or not.

For example, consider the findings from a recent risk assessment. One risk rated "high" noted that an organization's database including historical and highly confidential records would likely be compromised, including personal emails from executives engaged in personal activities that would be inappropriate for the workplace. Another risk rated "high" specified that authentication tools were not working effectively for a customer-facing site, exposing individual log-in credentials to cyberattack. The organization decides to remediate the second risk because it involves customers, and it is concerned that administrative agencies and state attorneys general will likely sue.

Perhaps a hacker compromises the highly confidential record database and posts all data, including embarrassing emails from the executives, in a public place. The executives sue the company for failure to protect their personal information. How might a court, with no awareness to cybersecurity risk management and no test for evaluating reasonableness, determine this case?

1. Downstream Static and Dynamic Duty

Surely, not all data breaches result in legal action, but increasingly they do. Unfortunately, perfect security is a myth, and even organizations with

209. Mike Perkowski, *Everything Can't Be Urgent: Why You Need to Prioritize Cyber Risks*, SECURITYROUNDTABLE.ORG (Oct. 9, 2018); *see* Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1521 (2017) (describing how organizations will never spend more money preventing a circumstance from occurring than what they pay if it does occur).

strong security programs can experience a data breach. However, if an organization has implemented security controls appropriate for their use and evaluated their implementation based on risk and priority, these organizations should collectively experience fewer data breaches and lower impact when breaches do occur.[210] Moreover, the overall required aptitude of an attacker will likely also be higher, which means that if an organization is not worth the effort to compromise, the organization is likely reasonably protected.

Performing one's duty reasonably, though, is not static, it is contextually dynamic. For purposes of this article, I call these variations *static duty* and *dynamic duty*. Static duties are duties that are known to be good choices for organizations as a whole, duties which are typically included as policy and controls for a risk management program. Static duties are not necessarily compulsory—they can be subject to risk-based decisions, but they are policies because they are likely to be necessary for reasonable cybersecurity, at least some version of the duty.

Dynamic duties are duties that are dependent on adversarial anticipation: duties that by definition must change based on the scenario.[211] Dynamic duties consider the entire security system as a whole, analyzing potential threats and vulnerabilities to inform exactly how and *to what extent* static duties should be performed. Dynamic duties ask: will these controls reasonably and foreseeably prevent a cyberattack or data breach based on what I know in this moment. Dynamic duties must be assessed and performed regularly to anticipate potential attacks.

A driving metaphor may help to demonstrate key differences between static and dynamic duties. For example, good driving behaviors may be informed by both static and dynamic informational inputs. Good driving behaviors are informed by standardized behavior, such as not driving under the influence of drugs or alcohol, using headlights, asking all vehicle occupants to wear a seatbelt, obeying traffic signs, and using your turn signals. Dynamic inputs might include road conditions and visibility that night, the actions of other drivers, and any other situational inputs. If the roads are slick and many drivers appear to be under the influence, a reasonably prudent driver is going to take far more precautions than if they are driving on clear roads. Such dynamic inputs might create more

210. Data breaches are not completely inevitable, but most organizations will experience many incidents and one or more data breaches.

211. This differentiation is not unusual: consider police action reviews. Much of appropriate police action is based on the scenario. Still, there are procedures and protocols that must always be fulfilled for the general safety of residents.

restrictive or different standards and affordances. A posted speed limit sign might establish a speed appropriate under normal conditions but that would be dangerous on packed snow and ice.

Cybersecurity is no different in its static and dynamic inputs, but it also is distinct in its adversarial nature: an organization's duties change depending on the threat landscape, not highway conditions. Specific duties, therefore, are both dynamic and relational. For example, even though an organization may be best positioned to avoid cybersecurity risk, some attacker behavior may be unforeseeable or require so many resources that no reasonable organization would have implemented them. Analogous to the driver's obligations to pedestrians, many controls should be implemented in *any* system or architecture, regardless of the situation.

For example, each new exploit, or method for compromising a system, creates a vulnerability. In cybersecurity, vulnerabilities may be broad, such as not encrypting a database. Or they may be more discrete, such as a code-level issue in a third-party's software that needs to be patched immediately because an attacker has already compromised the vulnerability, a "zero-day exploit."[212]

3. Identifying Vulnerabilities and Assessing Risks

A risk assessment process is used to review existing systems and identify potential vulnerabilities (deemed 'risks' in a risk assessment) based on a set of applicable controls, or requirements based on some predefined structure, such as a law or an industry standard.[213] A vulnerability management program avoids potential issues by prioritizing patching fixes corresponding to a dynamic threat landscape.[214] An incident response process responds to incidents or potential data breaches to avoid an attack,

212. *What is a Zero-day Attack? - Definition and Explanation,* KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit [https://perma.cc/JL65-WJZU].

213. RON ROSS, VICTORIA PILLITTERI, KELLEY DEMPSEY, MARK RIDDLE, & GARY GUISSANIE, NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUBL'N 800-171, REVISION 2, PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS 33-36 (Feb. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf [https://perma.cc/8BMP-JRK9].

214. MURUGIAH SOUPPAYA & KAREN SCARFONE, NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUBL'N 800-400, REVISION 4 , GUIDE TO ENTERPRISE PATCH MANAGEMENT PLANNING: PREVENTIVE MAINTENANCE FOR TECHNOLOGY at ii (Apr. 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf [https://perma.cc/9BPW-E89S].

to minimize the severity of attack, or to identify that an incident or potential incident has occurred.[215] All three are typically used in an industry standard cybersecurity program.

Some vulnerabilities are well-known and intended to be closed by implementing existing industry controls to reduce the risk of an incident occurring. The Cybersecurity & Infrastructure Security Agency maintains a list of known vulnerabilities.[216] It may be considered a static duty to patch them. An example of situations that involve both vulnerabilities and identified risks might be access control issues, such as shared log-in credentials.

Access controls in cybersecurity are extremely important because, typically, accessing software, applications, networks, databases, or servers is one of the many steps used in an attack.[217] For example, an employee might open a phishing e-mail and click on the link provided, which causes a file to be downloaded onto their machine.[218] This file could include a keylogger, which records all keyboard clicks the employee makes, including passwords to internal software that contains customer financial records.[219]

If the attackers also have gained access to the internal network, they may be able to access customer financial records and remove, or exfiltrate,

215. Organizations are becoming more interested in active defense, or rather defending their systems by shutting down attackers. More sophisticated programs may also employ red or blue teams to mimic an attack and reveal system issues not identified by a common risk assessment.

216. *Known Exploited Vulnerabilities Catalog,* U.S. CYBERSECURITY & INFRA. AGENCY, https://www.cisa.gov/known-exploited-vulnerabilities-catalog [https://perma.cc/TQJ3-5JFV].

217. James Martin, *What is Access Control? A Key Component of Data Security*, CSO (Aug. 21, 2019), https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html [https://perma.cc/TQJ3-5JFV].

218. Josephine Jordan, *How to Put A Phishing Keylogger Into an Email Download?* COMPUTER FORENSICS WORLD (Jan. 20, 2022), https://www.computerforensicsworld.com/how-to-put-a-phishing-keylogger-into-an-email-download/#:~:text=Hackers%20can%20access%20your%20personal%20data%20by%20using,it%20to%20be%20accessed%20before%20they%20use%20it [https://perma.cc/H8ZC-WM5N].

219. *Id.*

the records.[220] If very few employees have access to full customer records, called least user access, or least privilege, the probability of all records being compromised is very low.[221] Perhaps an organization might additionally ensure that users with power user, root, or otherwise comprehensive access are comprehensively trained on security, including to avoid phishing e-mails to minimize the risk of attackers using a keylogger to access sensitive data.

In the previous scenario, access controls are but one potential block to exfiltration of the data during a data breach, serving as one of the layers of defense. Access controls usually involve procedures, and sometimes automated means, to ensure access given is appropriate for the job function of the user.[222] When that user is terminated from a role or has changed their job, it is important to ensure the user no longer has access to certain systems and that the new access is appropriate for the corresponding job function. Access controls are a good idea no matter what system is involved. Therefore, user access and access provisioning, deprovisioning, and termination procedures (and following such procedures) are *always* important. They are static duties because they do not change based on the circumstances.

Dynamic duty is a bit more difficult to assess because it reflects the relationship between an attacker and a defender, known as an "adversarial" relationship.[223] In soccer, if a player scores a goal, is the player that good, or is the goalie that bad? How might you determine whether the goalie has performed reasonably or even well? Surely, we would not assume the goalie performed poorly when an adversary was successful; the adversary might just be Lionel Messi. In this analogy, you would begin by determining a threshold for the goalie, and the threshold depends on their skill and sophistication. A middle school soccer player is not expected to be as skilled as a professional soccer player, but there are certain skills you might expect based on age and experience. If a middle school soccer player knew they were going to be playing a professional soccer player in a year, they might

220. Jareth, *Ransomware data exfiltration detection and mitigation strategies*, EMSISOFT BLOG (Jan. 23, 2020), https://blog.emsisoft.com/en/35235/ransomware-data-exfiltration-detection-and-mitigation-strategies/#:~:text=To%20exfiltrate%20data%2C%20attackers%20first%20need%20to%20gain,organization%20or%20person%20or%20people%20within%20an%20organization [https://perma.cc/MV2Q-LG8H].

221. *Id*.

222. Martin, supra note 218.

223. *See* BAMBAUER ET AL., *supra* note 44, at 92.

spend more time preparing for how the professional soccer would play. And if you thought you'd be playing Lionel Messi, you'd probably try to recruit Gianluigi Buffon.

An analogy can be made to dynamic duty in cybersecurity. There are static "best" practices, and there are other practices that may best your opponent but are highly situational and change depending on the skill of the attacker.

The key difference in cybersecurity is that middle school goalies (small organizations) and professional goalies (large organizations) are expected to play any number of professional soccer players (experienced hackers) while blocking every single shot. Carrying the analogy a bit further, in soccer, a single goalie is not expected to defend several teams simultaneously. Even if the players are evenly matched, we would expect that the best goalies would be bested sometimes. Expecting perfect security in all cases does just that: it sets an impossible standard. On the other hand, deferring to basic standards alone is not enough to respond to real threats.

This is precisely the reason why duty is so difficult to establish comprehensively by statute. It is also why cybersecurity duty is often difficult to examine in a court of law. To actually evaluate duty *in situ*, Part IV will examine how courts might interpret reasonable security taking into account static and dynamic sources of information. Ultimately, this Article does not aim to determine which legal mechanism for creating a better cybersecurity ecosystem is optimal. Rather, it seeks to illustrate why duty is so difficult to ascertain and to offer some recommendations for courts and agencies to approximate reasonableness in a variety of legal situations.

PART IV: INFORMING DUTY

As William McGeveran's contribution describes, there is considerable overlap between duties established in statute, industry requirements, professional certifications, and administrative activity, such as consent orders.[224] The value of such an approach is truly in the normative value of the exercise—where various legal inputs create consistency through synthesis.[225] The synthetic attributes of these inputs are programmatic or process-based, which are useful for determining whether an organization may owe a duty. Because duty is analyzed in a wide variety of circumstances, from federal and state statutes to the common law, it is important to understand how McGeveran's objective, or static duty

224. *See* McGeveran, *supra* note 153, at 1195.

225. *Id.* at 1175.

approach, along with a dynamic duty inquiry, might play out in a variety of legal forms.

A. Static Duty

Static duties might include conducting a risk assessment, employing access controls, or drafting policies.[226] McGeveran lists five framework-specific requirements for any program:[227]

- Risk assessments, or the activity of identifying and making decisions about risk;
- Formal policy, or drafting internal documentation to create behavioral consistency for an organization;
- Leadership, or formally designating someone to lead security-related activities and advise decision-makers;
- Training or enabling a workforce to understand their policy obligations and responsibilities with regard to data; and
- Audit, or independent, ongoing monitoring.

These key requirements are tremendously useful for creating a management-based regulatory delegation framework that organizations prefer. It may also work effectively as an initial objective inquiry in doctrinal areas discussed throughout this paper. However, this analysis will likely require further inquiry based on the facts and circumstances of individual cases.

Ultimately, standardization is not enough. More is needed. ISO 27001, for example, offers top-level domains of activity that could form a foundation for static duty analysis, as do several other industry standards.[228] These standards help to establish a more comprehensive initial program. In fact, the NIST cybersecurity framework, created by the U.S. agency specifically tasked with creating standards, has designated 23 categories that could satisfy an initial static duty inquiry.[229]

226. *Id.* at 1182.

227. *Id.* at 1183-88.

228. *See* ISMS ONLINE, *supra* note 124.

229. *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS & TECH. at 23 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [https://perma.cc/3Q8V-VKXF].

Information security domains (or concentration areas), such as identify management and access control, access management, supply chain risk management, asset management, security continuous monitoring, response planning, data security, recovery planning, and governance are reflected in industry standards, as well as in some federal statutes.[230] To what extent organizations actually use these practices in relation to foreseeable threats and downstream risks of harm, however, is truly what informs reasonable duty determinations.

B. Dynamic Duty

Dynamic duty is the process of identifying *how* an organization has actually performed the statutory duty in relation to potential threats. Importantly, as described in Parts II and III, the crucial aspect of how an organization fulfills its dynamic duty is based on the nature and circumstances of the situation, especially whether an organization has effectively identified potential threats and foreseeable risk (and responded effectively to them). Fulfilling duty dynamically means an organization prospectively determines probable risks of harm that could be perpetrated by an ascertainable number of attackers.

Assessing potential threats means that the organization has considered how its systems or information could be compromised given potential threats rather than only followed a basic cybersecurity law or framework. Threat modeling, a method for ascertaining foreseeable attacks, is a necessary step to determining whether an organization's response to a cyberattack is reasonable.

The terminology of threat modeling may seem intimidating, but organizations do it all the time. Does a business owner with a brick-and-mortar location monitor crime reports? Why do liquor store owners in some locations place bars over their windows while others do not? This same logic informs why a financial services organization encrypts their account information in a database but why a small local retailer using an iPad and third-party credit card processor may not do the same with their customer mailing list. It may also demonstrate why it is perhaps not reasonable to expect the small local retailer to have implemented the same level of sophistication in their program. A program that includes policies and associated controls establishes these as their modus operandi, but where controls are applied and how they are applied is informed by risk determinations an organization makes.

230. *Id.*

For a dynamic duty inquiry, this context matters a great deal. For example, imagine a personnel management process that includes talent management and employee appraisal applications, hosted by a third party within a remote cloud server in India. If the organization conducts a risk assessment of the process, including each application, the organization might find that the third party is not regularly reviewing who has access to the system.

In fact, several employees who have moved to new jobs and some who have been terminated still have access to the system. This means that controls specific to access termination and access review will fail for purposes of a risk assessment. However, the organization has completed a risk assessment, as required by a law, and has some access controls in place. By statute alone, the company has passed their internal compliance practices and would likely pass a static duty inquiry. It matters little whether the organization actually remediated a known issue or not and what the real impact to a person might be.

Normative wrongs and standards of duty are inherently dynamic, in that they have a relational capacity. The common law, as an arbiter of duties (whether contractual, fiduciary, or tortious) has the unique capacity to determine these relational positions and fine-grained reasonable duties over time with some degree of consistency. Simply because the common law is imperfect and slow to develop does not make it incompatible with defining cybersecurity duties.

C. Common Law Duty

A two-step test assessing static and dynamic duty inquiry could be very useful in adjudicating cases as well as for administrative decisions that turn on questions of cybersecurity reasonableness.[231] In several doctrinal areas,

231. Although courts have wrestled with standing issues for some time due to difficulty meeting Article III requirements, some cases have involved past harms that easily survive Fed. R. Civ. P. 12(b)(1) and 12(b)(6) challenges, though most of them have settled. This has made it difficult for plaintiffs to claim a breach of fiduciary duty, negligence, or breach of contract based on data breaches. Indeed, with few exceptions, courts have spent much of their energy tackling Article III standing issues regarding the type of harm plaintiffs have faced in data breach litigation. *See* Kristin L. Bryan, *2021 Year in Review: Data Breach and Cybersecurity Litigation*, NAT'L. L. REV. (Dec. 23, 2021), https://www.natlawreview.com/article/2021-year-review-data-breach-and-cybersecurity-litigations [https://perma.cc/H8AN-USQT]. Shareholder

a two-step analysis or, more formally, a test, will ensure that following a successful cyberattack, such as a cyberintrusion or data breach, organizations are held accountable for their failure to use reasonable cybersecurity practices. However, it can also ensure that organizations that do engage in reasonable cybersecurity practices are not held accountable simply because they experienced a cyberintrusion or data breach, regardless of their actions. By creating more replicability in assessing reasonable cybersecurity duty, doctrinal areas will better satisfy the principles of fairness.

1. Fiduciary Duties

As fiduciaries are typically established by law, the duties associated with each role are well-defined. Although there has been considerable interest in new fiduciary roles, such as the information fiduciary,[232] all fiduciary relationships include duties of expertise, confidentiality, and loyalty.[233] While expertise is typically a professional skills duty, confidentiality and care could be evaluated (and usually are evaluated) from the perspective of reasonableness. The key difference for fiduciaries, at least those existing under the law today such as lawyers, doctors, or bankers, is that their duties are established in part by their profession.

When analyzing reasonable duty, therefore, a duty of confidentiality and a duty of care would normally be established in legal, medical, or other professional practice (both formally through professional organizations and by research and external sources) and compared against other professionals, for example. Because these professions stand in a relationship of trust with respect to a client, patient, or customer and

derivative lawsuits have similarly had great difficulty demonstrating harm. *See* Alison Frankel, *SEC's Stepped-up Cyber Scrutiny Won't Save Shareholder Data Breach Suits*, REUTERS (Oct. 7, 2021), https://www.reuters.com/legal/litigation/secs-stepped-up-cyber-scrutiny-wont-save-shareholder-data-breach-suits-2021-10-07/ [https://perma.cc/42PH-D6BZ].

232. *See* Ian Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CAN. BUS. L.J. 419 (2001); SOLOVE, *supra* note 75, at 102-103 (explaining the role of data brokers and a potential connection to fiduciary roles); Jack M. Balkin, *supra* note 75, at 1227-28 (2017); Frank Pasquale, *supra* note 75, at 1244-45; Richard Whitt, *supra* note 75, at 95-98 (2019).

232. Ari Ezra Waldman, *supra* note 75, at 595-96; Richards & Hartzog, *supra* note 75, at 52-57 (2021); Richards & Hartzog, *supra* note 75, at 1.

233. Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. 11, 14 (2020).

because information is often sensitive and entrusted, their obligations could be higher than an average organization.

For example, because the confidentiality of information is so crucial to these positions, fiduciaries may have less latitude to decide not to remediate a risk when a standard establishes a static duty. Organizations may also be subject to greater expectations in how and to what extent they meet the static duty (dynamic duties) because the potential for compromise given the nature of this work (health data, banking data, legal proceedings) is high.

2. Negligence and Negligence Per Se

In the event of a negligence per se claim, the static duty inquiry would be based on the applicable statutory requirement. If the static duty is imprecise, courts may have to engage in traditional discussions of statutory interpretation and administrative deference to determine the starting point for duty analysis. If administrators have not expanded and defined otherwise imprecise duties, courts should defer to industry standards to approximate reasonableness, as with other doctrinal areas. Dynamic duty would be examined as described below for common-law negligence.

For common-law negligence, the static duty inquiry could be based on a combined framework as described in Part III. The court would then examine dynamic duty as a matter of law depending on the claims. Dynamic duty would be a fact-specific inquiry, considering the size, complexity, and sector in which the organization operates. It would also consider data type, number of records, the type of technology systems, associated threats, and overall security program controls. Under a negligence model, the court would consider the facts and circumstances that apply, such as whether the defendant failed to act in a manner commensurate with foreseeable risk to others.[234] Then, based on this information and information supplied by the defendant, courts will need to determine what risks were foreseeable with respect to this specific plaintiff.

3. Contracts

Contracts are a function of private ordering, so, most of the time, duty will be established specifically by what the parties have memorialized in their written agreement, if one exists. However, it is certainly possible that an oral agreement, a set of documents that include terms that disagree and collectively knock each other out, a failure to include cybersecurity terms,

234. *See* Hurwitz, *Cyberensuring Security*, *supra* note 209, at 1522.

or ambiguous terms like "reasonable cybersecurity practices" could require the court to determine what duty was owed.

Courts may need to determine the allocation of risk with respect to the contract, for example who might be responsible if a system stops working or if a shipment is cancelled by a cyberattacker. Courts may also need to determine if parol evidence can be introduced generally or only in instances where there is ambiguity. It is likely that courts can determine what terms are expected by the parties based on what the parties themselves intended.

For non-goods contracts, courts should follow their existing practice: consider whether ambiguity exists on the face of the contract, and if it does (and frequently for cybersecurity, it will), employ the three interpretive inquiries. If parol evidence for course of performance or course of dealing does not shed light on the term's meaning (and often it won't), courts can then use a two-step analysis for interpretation.

Where static and dynamic duty inquiry may become relevant is when courts cannot find useful information based on analysis of documents and parol evidence of prior dealings. Where static and dynamic duty inquiry will be useful is when terms in completely integrated contracts are ambiguous on their face or for Uniform Commercial Code contracts to explain terms using usage of trade.

In the event courts explore duty framed as a contractual term, courts can similarly consider the term in a two-step analysis. First, courts can establish the static duty requirement as defining the term in question then second, courts can examine whether the party obligated to perform the requirement performed it as would be reasonably expected (dynamic duty). The examination of performance would also need to take into account what would have been reasonable given the facts and circumstances of the contractual relationship, additional terms in the contract, who controlled the system affected, whose information was affected, and potential threats to the system.

D. Statutory Cybersecurity

Administrative agencies and courts enforcing statutes can assess compliance with static duties in the form of verifying statutory requirements, as they typically do as part of investigations, audits, and cases. Agencies, however, can also investigate how an organization has met its dynamic duties. For example, an agency can find non-compliance easily if an organization has not met a basic statutory requirement. However, an agency can also find non-compliance if it asks an organization to provide detailed rationale and evidence for how it has satisfied the static duty and that duty does not demonstrate reasonable implementation of it.

Dynamic duty inquiry should require explanation of how the organization has oriented its performance of the static duty towards foreseeable threats and associated risk of harm and should include demonstrating how the risk was assessed and why the decision was made to implement the legal requirement in a particular way. Such an exploration could be conducted preventatively, in periodic audits or examinations, after a complaint is filed, or during an investigation.

E. Duty Inquiries in the Legal Process

The areas of law that could benefit from a two-step inquiry are many, and each of these legal regimes currently have a structure and process under which duty may be analyzed. This Article does not seek to dramatically change broad court processes but rather to fit within existing legal analyses, all of which easily incorporate a two-step analysis. This means that each doctrinal area could work differently to incorporate this analysis.

1. Statutory Duty

An agency could engage in a two-step analysis both in requesting information (which it currently does in an investigation or audit), in follow-up requests for information, and in administrative court. In the event this record could be included in an appeal to a federal court from an administrative court, agencies may prefer to include the analysis sooner, so that it is part of the legal record before it is heard in administrative court (if it ever is). There is also an opportunity to specify details about what would have been expected in any resulting settlement, such as a consent order, consent decree, or the like, which has the opportunity to influence behavior of other organizations who read them.

2. Fiduciary Duty

Fiduciary duty could follow a similar process to what exists today, which involves establishing what fiduciary duties, specifically, are owed to customers or patients. For example, courts will engage in identifying that a fiduciary duty exists, then examine plaintiff claims that the behavior of the fiduciary is within the contours of the duty established. It is within examination of the fiduciary's behavior that a two-step analysis can occur. The first step, as described in Part III, can be established by the professional industry, and depending on the profession, the source of this information

could be different. For example, a medical standard of care (establishing the duty for a specialized duty of care in medicine) and legal duty of confidentiality derive from different sources of information. Regardless of the source of the static duty, courts could engage in discussion of dynamic duty after the static duty has been established.

In common pre-trial motions, such as a motion to dismiss or motion for summary judgment, courts must accept all allegations to be true and to construe facts in the "light most favorable to the plaintiff."[235] This acceptance applies to all civil cases and although it is favorable to the plaintiff, it does require the plaintiff to argue all contours of the case. The plaintiff's claims, unless they are later amended, will flow through the case's lifecycle. For this reason, plaintiffs should initially argue both static and dynamic duty, to the extent they can with evidence available to them at the time.

Summary judgment is typically brought when "the movant [can] shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law."[236] For this reason, in summary judgment, the primary concern of a court is to determine whether static duty has or has not been fulfilled. In the event static duty has not been fulfilled, a plaintiff could be successful at summary judgment. In the event a static duty has been met, the case will continue to determine whether this also demonstrates dynamic duty has been met. This approach tracks with how civil cases work and likely how cybersecurity practices will be revealed: after a discovery conference and associated discovery activities have been completed.[237] Ultimately, this means that plaintiffs will arguably have an advantage in pre-trial motions, but as described above, pre-trial motions are supposed to be construed favorably with respect to plaintiffs.

In pre-trial motions, courts engage in analyses consistent with ensuring that first, the relationship is a properly formed fiduciary relationship, and second, that the plaintiff has plausibly argued the claim. In these motions, it is plausible that courts would at least review the plaintiff's claims of breached cybersecurity duty and determine whether there is at least some basis for that duty in the professional industry in which the breached fiduciary duty is alleged. Due to the function of court review in these initial motions, it is not likely that courts will engage in discussion of contextual, fact-based analysis of dynamic duty, though it is possible given the plaintiff's arguments do touch on elements of dynamic duty in addition to static duty.

235. Harry v. Marchant, 237 F.3d 1348, 1351 (11th Cir. 2000).

236. Fed. R. Civ. P. 56.

237. Fed. R. Civ. P 26(f).

Courts, therefore, could take this information into account in construing the arguments in a favorable light.

3. Contractual Duty

Contractual duty can also be examined statically and dynamically. Static duty may be established by formally identifying a term's meaning from the perspective of the parties' intent.[238] This likely involves some interpretation if the basis for a breach of contract action is nonperformance or imperfect performance of the term. Dynamic duty is best fit with an analysis of performance of the duty because not only does performance involve analyzing how, factually, an organization has performed a term, but also the obligation of performing in good faith. The timing of such a detailed inquiry, like evaluating fiduciary cybersecurity duty, likely requires a thorough fact-based analysis of the performance, which will require a more detailed review, typically at trial, though courts could at least evaluate both the meaning of the term and its performance facially during pre-trial motions.

4. Negligence Duty

Negligence presents a more challenging determination of where in the trial process duty should be examined. Specifically, plaintiffs in negligence actions bring a claim for what reasonable duty was at the time of the injury, and how the duty was breached. At least in part, plaintiffs must demonstrate plausibly that reasonable duty has been breached. This means that in motions to dismiss or motions for summary judgment, courts examine static duty, but it is likely to be a more effective analysis, *even in pre-trial motions*, if courts also examine dynamic duty, at least as plaintiffs have specifically detailed in their complaints.

As the standards for examining a motion to dismiss and summary judgment are distinct from trial (specifically regarding facts of a case being reviewed in a 'light most favorable to the plaintiff'),[239] courts do not yet need to engage fully in facts presented in the case, arguments based on evidence, or expert testimony. Ultimately, courts can engage in full two-step duty analysis at trial as they more fully interrogate whether a defendant's

238. Gregory Klass, *Contracts, Constitutions, and Getting the Interpretation-Construction Distinction Right*, 18 GEO. J. L. & POL'Y 13, 19 (2020).

239. Mayer Brown LLP, Fed. App. Prac. 358 (Philip Allen Lacovara, ed. in chief, BNA Books, 2008).

actions, from the perspective of foreseeable risk, fulfill static and dynamic reasonable duties.

CONCLUSION

It is often hard to shake the specter of blameworthiness when a cyberattack occurs, even if an organization's practices are arguably reasonable. The overused cybersecurity adage that "it's not a matter of *if*, but *when* an organization will be breached" demonstrates that an attacker's intrusion is inevitable, even for organizations with "reasonable" or "best" cybersecurity practices.[240] This creates a problem for reasonable duty: if duty is construed to be any and all activities that address any potential cybersecurity risks, organizations will not be likely to do business at all.[241]

Regardless of a business' size, doing business requires collection, use, and sharing information, which creates some risk of exposure.[242]

240. *Data Breach Preparation and Notification for Electronic Data*, MN.IT SERVICES 3, https://mn.gov/mnit/assets/Data%20Breach%20Preparation%20and%20Notification_tcm38-245447.pdf#:~:text=Electronic%20data%20breaches%20are%20not%20a%20matter%20of,a%20plan%20in%20place%20will%20help%20an%20agency%3A [https://perma.cc/K2UL-UU7Y].

241. Specifically in tort law, overly broad constructions of duty may be difficult to enforce. *See., e.g.,* Kennedy Krieger Inst., Inc. v. Partlow, 460 Md. 607 (2018) (reasoning that duties to clinical trial participants does not likely extend to siblings of such participants despite some degree of foreseeability). Further, most businesses cannot operate if organizations completely secure everything. Industry standards have similarly embraced the concept of resiliency and responsiveness to issues rather than a completely defensive position. Mike Lloyd, *Perfect Cybersecurity Makes No Business Sense*, FORBES (Sept. 21, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/09/21/perfect-cybersecurity-makes-no-business-sense/?sh=36c6e70a1757 [https://perma.cc/Q2TC-HTZ6].

242. *What are the Risks Associated with Collecting Personal Data*, GLS Group (May 28, 2020), https://www.gls.global/en/startupresources/what-are-the-risks-with-collecting-personal-data [https://perma.cc/HT8E-U73D]; David R. Owen & Kenneth Ritz, *Maintaining Cybersecurity with Third Parties and Vendors Receiving Sensitive or Private Data*, LEXOLOGY (July 20, 2020), https://www.lexology.com/library/detail.aspx?g=5fb10800-07d7-47e1-a71a-eba1ec18e045#:~:text=Even%20for%20a%20company%20with%20state-of-the-art%20information%20security%2C,data%20inaccessible%20until%20an%20extortion%20payment%20is%20made [https://perma.cc/538Y-5TG3].

Cyberattacks and data breaches are inevitable, but organizations can protect themselves from falling victim to low-skill, reasonably preventable attacks. Organizations can, and often do, significantly reduce the likelihood of a successful cyberattack or data breach by implementing cybersecurity controls. However, they fare far better when they anticipate risks and consider potential threats dynamically.

As described in some detail throughout this Article, reasonable cybersecurity continues to elude many parts of our legal system. Despite "reasonable cybersecurity" becoming a cornerstone of statute and contract and reasonableness a longtime standard in fiduciary relationships and in tort, courts have not sought many opportunities to examine and establish its contours. An examination of cybersecurity reasonableness, however, perhaps is not that complicated. Leveraging models already used in cybersecurity risk management will prepare courts and administrative agencies to examine whether an organization has engaged in reasonable cybersecurity practices.

By following a two-part analysis or test of static and dynamic duties, courts and administrative agencies will avoid rewarding compliant organizations with poor cybersecurity and instead raise the bar by truly interrogating the quality of cybersecurity programs.