2023

What Cybersecurity Policymakers Can Learn from Medical, Accounting, and Legal Professionals

Vadim Barkalov

What Cybersecurity Policymakers Can Learn from Medical, Accounting, and Legal Professionals

I. INTRODUCTION

This paper advocates for adopting specific reasonable expectations in the cybersecurity profession by drawing parallels to the medical, accounting, and legal professions because, as a relatively new profession, cybersecurity can benefit from incorporating the mature standards of care used in these three longer-established professions. The second part of the paper explores legal issues governing conduct in all four professions. The third part draws parallels between cybersecurity and the other three to establish specific expectations for the three groups chiefly controlling a company's cybersecurity strategy. Internal cybersecurity professionals must identify and relay recommendations to management concerning cybersecurity risks, mitigation strategies, and the need to involve external cybersecurity professionals. External cybersecurity professionals must serve as the final authority in their respective areas of specialization, preserve independence, and deliver advice untainted by their relationship with their clients. A company's management must bear the final responsibility for implementing internal controls and following cybersecurity professionals' advice but is not *per se* liable for a data breach if cybersecurity professionals failed to inform management despite the latter's good-faith effort to remain informed or if management made an informed but incorrect judgment call.

II. LEGAL ISSUES AFFECTING PROFESSIONALS' LIABILITY

This part explores legal issues governing professional conduct in the cybersecurity, medical, accounting, and legal professions. As a relatively new profession,[1] cybersecurity can benefit from incorporating standards of care used in three longer-established professions of

[1] Vikki Davies, *The History of Cybersecurity*, CYBER MAGAZINE (Oct. 4, 2021), https://cybermagazine.com/cyber-security/history-cybersecurity (last visited on Jan. 21, 2023) ("Cybersecurity began in the 1970s when researcher Bob Thomas created a computer programme called Creeper that could move across ARPANET's network, leaving a breadcrumb trail wherever it went.").

medicine, accounting, and law[2] because they have had more time to consider the benefits of costs of different frameworks for regulating professionals' conduct. Now is the right time to ensure the soundness of the standard of care in the cybersecurity profession because the digital technology continues to be the lifeblood of modern society in the aftermath of the COVID-19 health emergency,[3] and data breaches have become an epidemic of their own with no sign of abating and no silver bullet capable of preventing them.[4] Courts and legal scholars have considered several legal theories and causes of action to allow data subjects—employees or customers whose privacy is violated by the breach—to recover from companies whose systems are breached.[5] This part explores the current cybersecurity landscape, legal theories and causes of actions available to data subjects, and the standards of care used to regulate conduct in the three other professions.

A. Cybersecurity Landscape

1. Definition of a Data Breach

Cybersecurity researchers distinguish data incidents from data breaches.[6] A data incident compromises the confidentiality, integrity, or availability of data.[7] A data breach is an incident

---

[2] *E.g.*, The Development of a Medical Malpractice Lawsuit, THE PERSONAL INJURY CENTER, https://malpracticecenter.com/legal/medical-malpractice-lawsuit/ (last visited on Jan. 21, 2023) ("Medical malpractice law dates back at least to the recorded case of Stratton v. Swanlond, an English case that was decided in 1374").

[3] Daniel M. Filler et. al., *Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data*, 54 CONN. L. REV. 105, 105 (2022) ("Personal data is a cost of admission for much of modern life. Employers, tech companies, advertisers, information brokers, and others collect huge quantities of data about us all.").

[4] *Data Breach Investigations Report*, VERIZON (2022), https://www.verizon.com/business/resources/reports/dbir/ (last visited on Nov. 2, 2022) [hereinafter *Verizon Report*] ("Preventing cybercrime requires a multi-pronged strategy including increasing cybersecurity resilience and pursuing criminals and seizing illicit gains to deter and prevent future crimes.").

[5] Daniel M. Filler et. al., Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data, 54 Conn. L. Rev. 105, 116 (2022) ("Within this gap of legislative protections for privacy, and particularly with the limited recourse for individual victims, litigants and courts have looked to tort law to fill the gap. The common law offers two leading approaches to protecting privacy--first, the privacy torts, and, second, the law of negligence.").

[6] *Verizon Report*, *supra* note 4 ("Incident vs. breach").

[7] *Id.*

that involves a confirmed disclosure of data to an unauthorized party.[8] In other words, if there is no actual disclosure of data, there is no breach.[9] Because legal action requires showing cognizable harm, which may be difficult to establish even after a data breach,[10] data incidents, which do not involve disclosure, cannot give rise to legal action by data subjects, and this paper focuses exclusively on data breaches.

2. Sources of Data Breaches

Although cybersecurity researchers use different terminology when describing cyberattacks leading to data breaches, they typically distinguish between what is being attacked, e.g., web application or email, and how it is being attacked, e.g., denial of service or ransomware.[11] This paper refers to the former as an attack vector and the latter as an attack variety. To carry out an attack, an attacker must choose both an attack variety and an attack vector, e.g., by delivering ransomware via email.

Despite there being numerous attack vectors and attack varieties, most successful breaches depend on only a handful of them.[12] For example, the top ten varieties account for 73% of all attack varieties used in data breaches.[13] Similarly, the most popular attack vectors unsurprisingly consist of the systems exposed to the internet, with web applications and email topping the list.[14]

---

[8] *Id*.
[9] *Id*.
[10] Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1339 (11th Cir. 2021) ("if the hypothetical harm alleged is not "certainly impending," or if there is not a substantial risk of the harm, a plaintiff cannot conjure standing by inflicting some direct harm on itself to mitigate a perceived risk").
[11] *Cf. Verizon Report*, *supra* note 4 (listing ransomware as an attack variety) *with* Rachel Holmes, *Attack Vector vs. Attack Surface: What is the Difference?*, BITSIGHT (May 3, 2022), https://www.bitsight.com/blog/attack-vector-vs-attack-surface-what-difference (last visited on Nov. 2, 2022) (listing malware as an attack vector).
[12] *Verizon Report*, *supra* note 4 ("73% of breach varieties are found in the top 10 varieties").
[13] *Id*.
[14] *Id*. ("the main ways in which your business is exposed to the internet are the main ways that your business is exposed to the bad guys").

3. What Do Businesses Do About Data Breaches?

Companies employ a variety of cybersecurity measures to protect data under their control. For example, 87% of companies conduct cybersecurity awareness training for their employees at least once a quarter,[15] 99% of companies have a system for monitoring email-borne threats,[16] and more than 70% of companies perform penetration testing to uncover vulnerabilities in their systems.[17]

However, deploying individual cybersecurity measures is not enough in today's environment.[18] To create a cohesive system of safeguards against the top attack vectors and attack varieties, a company must develop a comprehensive cybersecurity program.[19] The details of the program can vary, but an effective program typically requires choosing a cybersecurity framework, conducting a risk assessment, and establishing an incident response plan, among other elements.[20] Some companies also undergo independent certifications attesting to the quality of their cybersecurity controls, including ISO 27001.[21]

---

[15] THE STATE OF EMAIL SECURITY, MIMECAST (2022), https://www.mimecast.com/state-of-email-security/ (last visited on Nov. 2, 2022) [hereinafter *Mimecast Report*].
[16] *Id*.
[17] *Penetration Testing Leaving Organizations with Too Many Blind Spots*, HELP NET SECURITY (Apr. 29, 2021) https://www.helpnetsecurity.com/2021/04/29/penetration-testing-blind-spots/ (last visited on Nov. 2, 2022) ("70 percent of organizations perform penetration tests as a way to measure their security posture"); Ioana Rijnetu, *100+ essential penetration testing statistics [2022 edition]*, PENTEST TOOLS (July 29, 2022) https://pentest-tools.com/blog/penetration-testing-statistics (last visited on Nov 2, 2022) ("72% of companies actively use free or open-source pentesting tools").
[18] *Verizon Report*, *supra* note 4 ("Preventing cybercrime requires a multi-pronged strategy including increasing cybersecurity resilience and pursuing criminals and seizing illicit gains to deter and prevent future crimes.").
[19] *Id*.
[20] Raj Chaudhary, *The 5 Essential Elements of Cybersecurity*, CROWE LLP (Sept. 22, 2015), https://www.crowe.com/cybersecurity-watch/5-essential-elements-cybersecurity.
[21] *ISO 27001, the International Information Security Standard*, IT GOVERNANCE, https://www.itgovernanceusa.com/iso27001 (last visited on Nov. 2, 2022) ("ISO 27001 certification demonstrates that your organization has invested in the people, processes, and technology . . . to protect your organization's data and provides an independent, expert assessment of whether your data is sufficiently protected.").

B. Overview of Legal Theories and Causes of Action by Data Subjects Against Businesses After a Data Breach

This section explores three legal theories commonly employed by data subjects after a data breach: statutory compliance, privacy torts, and negligence. Of the three, statutory compliance and negligence are most applicable against businesses that store breached data.

1. Statutory Requirements

Data privacy in the U.S. is regulated at both federal[22] and state[23] levels. Perhaps recognizing the rapid pace of change in the cybersecurity landscape, the statutes focus on standards rather than specific rules.[24] The below table summarizing some of the statutes illustrates this focus.

Federal or state	Statute	Standard or duty of care
Federal	Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936	Parties maintaining or transmitting health information must maintain reasonable safeguards against its disclosure.[25]
Federal	Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999)	Financial institutions must develop safeguards against reasonably foreseeable risks to the confidentiality,

[22] *E.g.*, Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (providing privacy standards for financial institutions); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (providing privacy standards for health records); Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 571 (providing privacy standards for educational records); Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-730 (providing privacy standards for children's online activity).

[23] *E.g.*, California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.100; California Privacy Rights Act of 2020 (CPRA), 2020 Cal. Legis. Serv. Prop. 24 (Proposition 24); Virginia Consumer Data Protection Act (VCDPA), 2021 Virginia Laws 1st Sp. Sess. Ch. 35 (enacting Va. Code § 59.1-575 et seq.).

[24] *See* Daniel M. Filler et. al., Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data, 54 Conn. L. Rev. 105, 112 n. 22 (2022) (summarizing four federal statutes as "providing privacy standards").

[25] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 ("Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards.").

		integrity, and security of customer data.[26]
Federal	Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 571	Educational agencies and institutions must implement appropriate procedures for granting parents' requests to access their children's records within a reasonable time.[27]
Federal	Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-730	Operators of websites directed at children and collecting children's personal information must make a reasonable effort to obtain parents' consent.[28]
California	California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798.100	Consumers have a right of action against businesses that lack reasonable security procedures to protect consumer data.[29]
California	California Privacy Rights Act of 2020 (CPRA), 2020 Cal. Legis. Serv. Prop. 24 (Proposition 24)	Businesses must have reasonable security procedures to protect consumer data.[30]

[26] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) ("each agency or authority [including the Federal Trade Commission] described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards"); Standards for Safeguarding Customer Information, 86 FR 70272-01 ("a financial institution must identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information [and] design and implement safeguards to control the risks identified through the risk assessment").

[27] 20 U.S.C. § 1232g ("[e]ach educational agency or institution shall establish appropriate procedures for the granting of a request by parents for access to the education records of their children within a reasonable period of time").

[28] 15 U.S.C. § 6502 ("require the operator of any website or online service directed to children . . . to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children"); 15 U.S.C. § 6501 ("'verifiable parental consent' means any reasonable effort (taking into consideration available technology) , including a request for authorization for future collection, use, and disclosure described in the notice").

[29] Cal. Civ. Code § 1798.150 ("[a]ny consumer whose nonencrypted and 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").

[30] Cal. Civ. Code § 1798.100 (amendment effective Jan. 1, 2023) ("[a] business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure").

Virginia	Virginia Consumer Data Protection Act (VCDPA), 2021 Virginia Laws 1st Sp. Sess. Ch. 35 (enacting Va. Code § 59.1-575 et seq.)	Data controllers must implement reasonable safeguards to protect personal data from unauthorized disclosure.[31]
Colorado	Colorado Privacy Act, Senate Bill 21-190, 73d Leg., 2021 Regular Sess. (Colo. 2021), to be codified in Colo. Rev. Stat. ("C.R.S.") Title 6	Data controllers must implement reasonable safeguards to protect personal data from unauthorized disclosure.[32]

As the above overview demonstrates, many federal and state privacy laws and regulations require businesses to employ reasonable safeguards to protect consumer data. Recognizing the diversity of the circumstances and business environments faced by companies and the resulting impossibility of creating a universal rule, the statutes and regulations promulgate standards—focusing on reasonableness—rather than specific rules and rely on each company to apply those standards to its circumstances.

2. Privacy Torts

An individual's privacy may be violated through one of four common-law privacy torts: intrusion upon seclusion, public disclosure of embarrassing private facts, public placement of an individual in a false light, and appropriation of name and likeness.[33] For various reasons discussed below, none of these torts implicates a business that suffers a data breach.

---

[31] VA. CODE ANN. § 59.1-578 ("[a] controller shall . . . [e]stablish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue"), https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-578/ (last visited on Nov. 2, 2022).

[32] Colorado Privacy Act, Senate Bill 21-190, 73d Leg., 2021 Regular Sess. (Colo. 2021), to be codified in Colo. Rev. Stat. ("C.R.S.") Title 6, https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf (last visited on Nov. 2, 2022); *The Colorado Privacy Act: Enactment Of Comprehensive U.S. State Consumer Privacy Laws Continues*, GIBSON DUNN (July 9, 2021) https://www.gibsondunn.com/the-colorado-privacy-act-enactment-of-comprehensive-u-s-state-consumer-privacy-laws-continues/.

[33] Daniel M. Filler et. al., Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data, 54 Conn. L. Rev. 105, 127 (2022).

The first tort—intrusion—involves intentionally interfering with another's solitude in an offensive manner.[34] Even if a breached business's inadequate cybersecurity practices are the cause of the breach and the resulting interference with the data subjects' solitude, the business can hardly be said to *intend* to cause the breach and interference. The second tort—disclosure—involves publicly disclosing private facts.[35] To succeed, the plaintiff must show that the private information was disclosed widely.[36] Even if a data breach is viewed as disclosure and the private information is eventually leaked to the public, the initial disclosure by the breached business is typically limited to a hacker or a group of hackers. The third tort—false light—involves publicly disclosing false facts.[37] To prevail, the plaintiff must demonstrate that the defendant exhibited actual malice.[38] A business is unlikely to cause a breach out of malice toward its data subjects. The fourth tort—appropriation—involves using another's name or likeness for one's benefit.[39] A breached business does not appropriate the data subjects' names and likeliness and does not benefit from the breach.

Therefore, while privacy torts may play a role in the data breach context, they do not implicate the breached business.

---

[34] Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 150 (2007)

[35] *Id*. at 151 ("Under the public disclosure of private facts tort: One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.").

[36] *Id.* at 152 ("the public disclosure tort was limited to instances when the information was disclosed widely to the public").

[37] Hogan v. Winder, 762 F.3d 1096, 1110-11 (10th Cir. 2014).

[38] Neil M. Richards & Daniel J. Solove, Privacy's Other Path: Recovering the Law of Confidentiality, 96 Geo. L.J. 123, 154 (2007) ("in Time, Inc. v. Hill, the Court held that the First Amendment required the actual malice standard to establish a false light claim").

[39] *Id.* at 151 ("the tort of appropriation provides: 'One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.'").

3. Negligence

Because privacy torts do not provide consumers with the necessary framework to seek remedies from businesses, consumers overwhelmingly turn to negligence in data breach cases.[40] The starting point of a data breach negligence claim is the business's duty to establish reasonable cybersecurity controls to protect the information it collects.[41] The same duty exists in various settings, including employee-employer[42] and consumer-business.[43] Besides duty, plaintiffs must also show a breach of duty, causation, and injury.[44] If a business chooses to collect confidential information, it cannot shed its duty to protect it.[45] In many instances, a business also cannot disprove the causation element because successful cyberattacks rely on vulnerabilities in the business's own defenses. Similarly, although attacking the injury element may be a valid litigation strategy, it is not a sound cybersecurity strategy because a business may not be able to forecast what kind of injury its data subjects will suffer. Therefore, avoiding data breach liability requires avoiding the data breach or avoiding the breach of the duty to establish reasonable cybersecurity controls.

---

[40] Daniel M. Filler et. al., Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data, 54 Conn. L. Rev. 105, 117 (2022) ("negligence is currently the predominant theory under which data breach class action plaintiffs seek recovery. In 2017, sixty-five percent of all federal data breach class actions alleged negligence as their primary theory of liability, and ninety-five percent of such complaints included it as a cause of action.").

[41] *Id.* at 121 ("Applying the negligence principle that a person assumes a duty of care where their affirmative actions have created a risk of harm, the Court held that the act of collecting and storing employee data on a computer system gives rise to a duty on the part of the data collector, requiring the exercise of reasonable care to protect the data subjects against an unreasonable risk of harm arising out of its actions").

[42] Dittman v. UPMC, 196 A.3d 1036, 1038 (Pa. 2018) ("an employer has a legal duty to exercise reasonable care to safeguard its employees' sensitive personal information stored by the employer on an internet-accessible computer system").

[43] In re Sony Gaming Networks and Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014), order corrected, 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014) ("Although neither party provided the Court with case law to support or reject the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity, the Court finds the legal duty well supported by both common sense and California and Massachusetts law").

[44] In re Sony Gaming Networks and Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 963 (S.D. Cal. 2014), order corrected, 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014).

[45] *Id*.

C. Standards of Care in Other Professions

1. Standard of Care for Medical Professionals

Courts apply two standards of care in medical malpractice cases: a locality rule and a national standard.[46] Under the locality rule, one commits malpractice if one fails to exercise a degree of skill and care ordinarily exercised by other medical professionals in good standing who practice in the same or similar locality.[47] There are two variations of the locality rule: the strict locality rule and the similar locality rule.[48] As the name suggests, the strict locality rule compares the defendant's actions to the standard of care exercised by other medical professionals in the defendant's own community or locality.[49] The similar locality rule compares the defendant's actions to the standard of care exercised either in the defendant's own locality or a similar locality.[50] Courts adopted the strict locality rule more than a century ago because of the disparity between the level of care that could be provided in large urban centers and the one that could be achieved in rural areas.[51] Since then, the trend has been to expand the geographic boundary when comparing the defendant's standard of care to the one exercised by the defendant's peers: first by adopting the similar locality rule instead of the strict locality rule and eventually by considering the national standard in some cases.[52]

---

[46] Shilkret v. Annapolis Emerg. Hosp. Ass'n, 349 A.2d 245, 249 (Md. 1975).
[47] Steeves v. United States, 294 F. Supp. 446, 453 (D.S.C. 1968) ("A physician is bound to use reasonable care in the treatment of his patient and the rendering of professional services. However, he is bound only to possess and exercise that degree of skill and learning which is ordinarily possessed and exercised by members of his profession who are in good standing and live in the general neighborhood or in a similar locality.").
[48] *Shilkret*, 349 A.2d at 246–47.
[49] *Id.* at 246.
[50] *Id.* at 247.
[51] *Id.* at 249.
[52] *Id.* at 249–51 ("These deficiencies in the locality rules and the increasing emphasis on the availability of medical facilities have led some courts to dilute the rules by extending geographical boundaries to include those centers that are readily accessible for appropriate treatment. . . . In any event, the trend continues away from standards which rest solely on geographic considerations.").

The national standard of care in medical malpractice cases compares the defendant's actions to the standard of care exercised by other medical professionals within the same field without imposing geographic restrictions.[53] The national standard focuses on ensuring that medical professionals learn and apply the latest medical advances in their practices regardless of their location.[54] Although some states now apply the national standard in all medical malpractice cases,[55] others apply the locality rule to medical generalists, e.g., primary care doctors, and the national standard to specialists.[56] The reason typically cited for this distinction is that specialists are subject to a higher standard of care than their generalist colleagues.[57] Furthermore, the distinction is based not on one's skill but on how one holds oneself out to the public, i.e., a one's extensive experience of treating certain conditions does not automatically subject one to a higher standard of care if one did not present oneself as a specialist in that area.[58] The inescapable conclusion is that the distinction in the standard of care reflects societal expectations that specialists serve as the final authority in diagnosing and treating conditions within their areas of

---

[53] *Id.* at 250-51 ("a specialist should be held to the standard of care and skill of the average member of the profession practising the specialty, taking into account the advances in the profession").
[54] Shilkret v. Annapolis Emerg. Hosp. Ass'n, 349 A.2d 245, 250-51 (Md. 1975).
[55] Goldman v. Bosco, 120 F.3d 53, 55 (5th Cir. 1997) ("In 1985, in Hall v. Hilbun, the Mississippi Supreme Court abandoned the local standard of care and adopted a resource-based national standard of care"); Cortes-Irizarry v. Corporacion Insular De Seguros, 111 F.3d 184, 190 (1st Cir. 1997) ("a health care provider has 'a duty to use the same degree of expertise as could reasonably be expected of a typically competent practitioner in the identical specialty under the same or similar circumstances, regardless of regional variations in professional acumen or level of care'").
[56] RESTATEMENT (SECOND) OF TORTS § 299A (AM. LAW INST. 1965) ("Allowance must be made also for the type of community in which the actor carries on his practice. A country doctor cannot be expected to have the equipment, facilities, experience, knowledge or opportunity to obtain it, afforded him by a large city. [However,] a physician who holds himself out as a specialist in certain types of practice is required to have the skill and knowledge common to other specialists" without regard to geographic location.")
[57] *E.g.*, Reeg v. Shaughnessy, 570 F.2d 309, 314 (10th Cir. 1978) ("Oklahoma law . . . holds specialists to a higher standard of care than that required of general practitioners"); Myles v. Laffitte, 986 F.2d 1414, at *1 (4th Cir. 1993) ("specialists are held to a higher standard of care than that required of general practitioners"); Cross v. Huttenlocher, 440 A.2d 952, 955 (Conn. 1981) (testimony by two specialists in pediatric neurology did not establish the standard of care of a general pediatrician).
[58] *Reeg*, 570 F.2d at 314-15 ("[I]t would have been improper to hold [plaintiff] to a standard of an orthopedic surgeon, inasmuch as he was not board certified in that specialty. . . . [Plaintiff] had performed more than half of the orthopedic operations for the Fetzer Clinic. He was not, however, a board certified surgeon in either the general or orthopedic fields.").

expertise, regardless of where they are located, while generalists' obligations are often limited to treating routine conditions and recognizing when a referral to a specialist is necessary.[59] However, it does not follow that a referring generalist's responsibility for a patient's wellbeing is any less than that of a specialist.[60] On the contrary, the former retains the primary responsibility unless it is officially transferred to the latter.[61]

Therefore, generalists and specialists play different but equally important roles that help explain their different standards of care. Because generalists treat routine issues, identify cases requiring referrals to specialists, and coordinate care provided by specialists, that branch of the medical profession focuses on promoting access to generalists, who then determine which patients must be referred to specialists for further treatment. The locality rule helps achieve that goal by encouraging generalists to practice in new and rural areas where they cannot and do not have to provide the same level of care as in urban centers. Conversely, because specialists must serve as the final authority in diagnosing and treating conditions within their areas of specialty, that branch of the medical profession focuses on applying the latest medical advances and ensuring that patients, who may have to travel to reach a specialist, do not have to second-guess the specialist's competence. The national standard of care helps achieve that goal by requiring all doctors within a specialty to provide the same level of care regardless of location.

2. Ethics Rules for Accounting Professionals

The ethics rules promogulated by the American Institute of Certified Public Accountants Code of Professional Conduct (AICPA Code) recognize two categories of services performed by

---

[59] Steven Pearson, Principles of Generalist–Specialist Relationships, J. OF GEN. INTERNAL MED. (1999), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1496875/ (last visited on Nov. 2, 2022) ("[p]hysicians should obtain consultation when they feel a need for assistance in caring for a patient").
[60] *Id.* ("[u]nless authority has been formally transferred, the ultimate responsibility and corresponding authority for a patient's care lies with the referring physician").
[61] *Id.*

accountants: attest and non-attest services.[62] Attest services involve reviewing or auditing a company's financial statements and issuing an opinion about their reliability.[63] Non-attest services include the accountant's other services and relationships, such as management consulting, bookkeeping, tax preparation, and personal financial planning.[64]

The AICPA Code distinguishes the two categories of services because audit opinions—which accountants issue as part of an attest engagement—are vitally important to the users of the company's financial statements, such as its creditors, its stockholders, and the investing public, who rely on audit opinions to make investment decisions and protect their interests.[65] Therefore, the AICPA Code requires auditors to render unbiased opinions even if doing so contradicts their client's assertions about the accuracy of its financial statements.[66] To prevent bias, the AICPA Code further requires accountants performing attest services to maintain independence by avoiding influences that compromise their professional judgment and avoiding the appearance

---

[62] AICPA CODE OF PROFESSIONAL CONDUCT § 0.400.04 (AICPA 2014), https://pub.aicpa.org/codeofconduct/ethics.aspx?targetdoc=et-cod&targetptr=et-cod0.400.21# (last visited on Nov. 2, 2022) ("Attest engagement. An engagement that requires independence"); Plain English Guide to Independence, AICPA PROFESSIONAL ETHICS DIVISION (2021), https://us.aicpa.org/content/dam/aicpa/interestareas/professionalethics/resources/tools/downloadabledocuments/plain-english-guide.pdf (last visited on Nov. 2, 2022) ("The AICPA Code of Professional Conduct (the code) requires you to remain independent of affiliates of any financial statement attest client.").

[63] STATEMENTS ON STANDARDS FOR ATTESTATION ENGAGEMENTS § 101.01, AICPA AUDITING STANDARDS BOARD (2016), https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/at-00101.pdf (last visited on Nov. 2, 2022) ("This section applies to engagements . . . in which a certified public accountant in public practice . . . is engaged to issue or does issue an examination, a review, or an agreed-upon procedures report on subject matter . . . that is the responsibility of another party."); Will Kenton, *Attest Service*, Investopedia (June 29, 2021), https://www.investopedia.com/terms/a/attest-function.asp (last visited on Nov. 2, 2022) ("An attest service, or attestation service, is an independent review of a company's financial statement conducted by a certified public accountant (CPA). The CPA delivers an attestation report with conclusions about the reliability of the data.").

[64] AICPA CODE OF PROFESSIONAL CONDUCT §§ 1.220.020.06, 1.210.010.15 (AICPA 2014), https://pub.aicpa.org/codeofconduct/ethics.aspx?targetdoc=et-cod&targetptr=et-cod0.400.21# (last visited on Nov. 2, 2022) ("nonattest services [include] tax, personal financial planning, and management consulting . . . [m]anagement participation threat [is] [t]he threat that a member will take on the role of attest client management or otherwise assume management responsibilities for an attest client.").

[65] United States v. Arthur Young & Co., 465 U.S. 805, 806 (1984) ("An independent certified public accountant performs a different role from an attorney whose duty, as his client's confidential adviser and advocate, is to present the client's case in the most favorable possible light. In certifying the public reports that depict a corporation's financial status, the accountant performs a public responsibility transcending any employment relationship with the client, and owes allegiance to the corporation's creditors and stockholders, as well as to the investing public.").

[66] *Id*.

that their judgment is compromised.[67] The Sarbanes-Oxley Act codifies the rule by prohibiting independent auditors of publicly traded companies from contemporaneously providing both attest and non-attest services to the same company.[68]

The independence rule does not apply to accountants performing non-attest services.[69] Furthermore, the AICPA Code acknowledges that "in-house" accountants cannot be independent of their employers because employment automatically creates the appearance that an accountant's judgment is compromised.[70] Nonetheless, in-house accountants play various vital roles ranging from financial and IT analysts to controllers and CFOs for companies ranging from family-owned businesses to Fortune 500 companies.[71] Although they must rely on their independent counterparts for attest services, they can, either on their own or in collaboration with

---

[67] AICPA CODE OF PROFESSIONAL CONDUCT § 0.400.04 (AICPA 2014), https://pub.aicpa.org/codeofconduct/ethics.aspx?targetdoc=et-cod&targetptr=et-cod0.400.21# (last visited on Nov. 2, 2022) ("Attest engagement. An engagement that requires independence"); AICPA CODE OF PROFESSIONAL CONDUCT § 0.400.21 (AICPA 2014), https://pub.aicpa.org/codeofconduct/ethics.aspx?targetdoc=et-cod&targetptr=et-cod0.400.21# (last visited on Nov. 2, 2022) ("Independence. Consists of two elements, defined as follows: a. Independence of mind . . . b. Independence in appearance . . .")

[68] *Strengthening the Commission's Requirements Regarding Auditor Independence*, SECURITIES AND EXCHANGE COMMISSION (Mar. 3, 2003), https://www.sec.gov/rules/final/33-8183.htm ("Section 201(a) of the Sarbanes-Oxley Act adds new Section 10A(g) to the Securities Exchange Act of 1934. Except as discussed below, this section states that it shall be unlawful for a registered public accounting firm that performs an audit of an issuer's financial statements (and any person associated with such a firm) to provide to that issuer, contemporaneously with the audit, any non-audit services . . . .").

[69] *Plain English Guide to Independence*, AICPA PROFESSIONAL ETHICS DIVISION (2021), https://us.aicpa.org/content/dam/aicpa/interestareas/professionalethics/resources/tools/downloadabledocuments/plain-english-guide.pdf (last visited on Nov. 2, 2022) ("You and your firm are not required to be independent to perform services that are not attest services (for example, financial statement preparation, tax preparation or advice, or consulting services, such as personal financial planning) if they are the only services your firm provides for a client.").

[70] AICPA CODE OF PROFESSIONAL CONDUCT § 0.300.050.05 (AICPA 2014), https://pub.aicpa.org/codeofconduct/ethics.aspx?targetdoc=et-cod&targetptr=et-cod0.300# (last visited on Nov. 2, 2022) ("members not in public practice cannot maintain the appearance of independence, they nevertheless have the responsibility to maintain objectivity in rendering professional services").

[71] *Positions in Business and Industry Accounting*, AICPA, https://us.aicpa.org/career/careerpaths/corporateaccounting (last visited on Nov. 2, 2022); *Occupational Outlook Handbook: Accountants and Auditors*, U.S. BUREAU OF LABOR STATISTICS (Sept. 8, 2022), https://www.bls.gov/ooh/business-and-financial/accountants-and-auditors.htm#tab-2 (last visited on Nov. 2, 2022).

external accountants, help their employers identify and implement proper accounting practices and detect and fix issues.[72]

Despite the significant help from in-house accountants and independent auditors, the company's management bears the ultimate responsibility for the accuracy of the financial statements.[73] For example, a publicly traded company's CEO and CFO must sign a certification attesting that they are responsible for establishing and maintaining internal controls, made appropriate disclosures to the company's independent auditors, and are not aware of any untrue or misleading information contained in the financial statements.[74] Consequently, courts hold accountants liable for inaccuracies in a company's financial statements when they knowingly help the company's management conceal those inaccuracies.[75] Furthermore, a company's management is responsible for setting up appropriate monitoring and controls to ensure that they are reasonably informed about the company's operations.[76]

3. Rules of Professional Conduct for Lawyers

Lawyers' conduct is subject to state-specific rules of professional conduct that are based on the America Bar Association's Model Rules of Professional Conduct.[77] A violation of the ethics rules can lead to sanctions against a lawyer, such as suspension from legal practice or

---

[72] *See id*.
[73] 15 U.S.C. § 7241(a) (a publicly traded company's CEO and CFO must certify, among other things, that they "are responsible for establishing and maintaining internal controls," made appropriate disclosures to the company's independent auditors, and are not aware of any untrue or misleading information contained in the financial statements).
[74] *Id.*
[75] In re Rent-Way Sec. Litig., 209 F. Supp. 2d 493, 505 ("it is sufficient for plaintiffs to plead scienter by alleging 'facts "establishing a motive and an opportunity to commit fraud, or by setting forth facts that constitute circumstantial evidence of either reckless or conscious behavior"'").
[76] In re Caremark International Inc. Derivative Litig., 698 A.2d 959, 970 (Del. Ch. 1996) ("a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by noncompliance with applicable legal standards").
[77] *American Bar Association Model Rules of Professional Conduct*, WIKIPEDIA, https://en.wikipedia.org/wiki/American_Bar_Association_Model_Rules_of_Professional_Conduct ("All fifty states and the District of Columbia have adopted legal ethics rules based at least in part on the MRPC.")

disbarment.[78] Besides sanctions, a lawyer may also be subject to a malpractice action.[79] Violation of the ethics rules does not by itself establish a *prima facie* case of legal malpractice.[80] Similarly, establishing a *prima facie* case of legal malpractice does not by itself prove ethical misconduct.[81]

Some of the ethics rules most transferable to other professions include Rule 7.2(c), stating that a lawyer must advertise as a specialist unless a lawyer is certified in that specialty, and Rules 1.1 and 1.3, requiring a lawyer to provide competent and diligent representation.[82] Notably, Rules 1.1 and 1.3 do not contain an exception to competence and diligence when serving a client who would otherwise be worse off.[83] For example, a lawyer violates the ethics rules by providing a less-than-competent or less-than-diligent representation to an asylum seeker who would otherwise be unrepresented and face certain deportation.[84] Furthermore, a lawyer may fail to act with diligence even if the lawyer's actions do not prejudice the client.[85] In other words, a client should not have to second-guess the lawyer's competence and diligence.

A *prima facie* case of legal malpractice requires showing "(1) the existence of an attorney-client relationship; (2) acts constituting negligence or breach of contract; (3) that such

---

[78] MODEL RULES FOR LAWYER DISCIPLINARY ENFORCEMENT r. 10 (AM. BAR ASS'N 2020), https://www.americanbar.org/groups/professional_responsibility/resources/lawyer_ethics_regulation/model_rules_for_lawyer_disciplinary_enforcement/rule_10/ (last visited on Nov. 2, 2022) ("Misconduct shall be grounds for one or more of the following sanctions: (1) Disbarment by the court. (2) Suspension by the court for an appropriate fixed period of time not in excess of three years.").

[79] Ball v. Kotter, 723 F.3d 813, 815 (7th Cir. 2013) ("[t]he other count was . . . for legal malpractice, alleging that she failed to recognize certain conflicts of interest in the two transactions").

[80] *Id*. at 823.

[81] In re Aug., 2010-1546 (La. 10/15/10), 45 So.3d 1019, 1024 ("acts of legal malpractice do not necessarily constitute ethical misconduct").

[82] MODEL RULES OF PROF'L CONDUCT r. 7.2, 1.1, 1.3 (AM. BAR ASS'N 2020).

[83] MODEL RULES OF PROF'L CONDUCT 1.1, 1.3 (AM. BAR ASS'N 2020).

[84] Lisa G. Lerman, Ethical Problems in the Practice of Law 120 (Rachel E. Barkow, et al. eds., 5th ed. 2020).

[85] In re Lewellen, 56 F. App'x 663, 667 (6th Cir. 2003) ("Despite Lewellen's explanations for his conduct, and his assertion that the situation did not prejudice his client's interests, this court cannot say that the district court's conclusion that Lewellen was not acting with diligence and promptness in representing his client is an abuse of discretion."); In re Mills, No. 15-11766, 2018 WL 10323376, at *21 (Bankr. W.D. Tenn. July 24, 2018) ("A court is well within its discretion to determine that an attorney has violated this rule even if the lack of diligence did not prejudice the client's interests.").

acts were the proximate cause of the plaintiff's damages; and (4) that but for defendant's conduct, the plaintiff would have been successful in the prosecution or defense of the action."[86] Therefore, legal malpractice parallels the objective standard in negligence cases, which requires showing the existence of a duty, breach of duty, but-for causation, proximate cause, and injury.[87]

DEVELOPING AND APPLYING A STANDARD OF CARE IN THE CYBERSECURITY CONTEXT

C. What Is Reasonable?

1. What Is Reasonable Varies by Company

As discussed previously, negligence is the prevalent cause of action by data subjects who seek remedies from a business after a data breach.[88] Statutory requirements also play a significant and growing role in shaping companies' behavior.[89] Both legal theories' common theme is that businesses must employ reasonable care and cybersecurity controls, but neither theory defines what constitutes reasonable care and controls. At common law, the court's imposition of a duty of reasonable care requires a fact-specific inquiry that "involves identifying, weighing, and balancing several factors—the relationship of the parties, the nature of the attendant risk, the opportunity and ability to exercise care, and the public interest in the proposed

---

[86] Ryan Contracting Co. v. O'Neill & Murphy, LLP, 883 N.W.2d 236, 242 (Minn. 2016).
[87] Novak v. Cap. Mgmt. & Dev. Corp., 452 F.3d 902, 907 (D.C. Cir. 2006) ("In the District of Columbia, as elsewhere, '[t]o establish negligence a plaintiff must prove a duty of care owed by the defendant to the plaintiff, a breach of that duty by the defendant, and damage to the interests of the plaintiff, proximately caused by the breach.'").
[88] Daniel M. Filler et. al., Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data, 54 Conn. L. Rev. 105, 117 (2022) ("negligence is currently the predominant theory under which data breach class action plaintiffs seek recovery. In 2017, sixty-five percent of all federal data breach class actions alleged negligence as their primary theory of liability, and ninety-five percent of such complaints included it as a cause of action.").
[89] *Id*. at 115 ("The CCPA has changed the dialogue in the United States, with many states looking to California as an example of how to protect privacy"); Joseph J. Lazzarotti, *2023 New Year's Resolution: Don't Get "Whacked" By A State AG for Cybersecurity Compliance*, NATIONAL LAW REVIEW (Jan. 1, 2023), https://www.natlawreview.com/article/2023-new-year-s-resolution-don-t-get-whacked-state-ag-cybersecurity-compliance (last visited on Jan. 21, 2023) ("It usually happens after a reported data breach. . . . Not long thereafter, the organization receives an inquiry from one or more government agencies. . . . On December 16, Pennsylvania's Attorney General and soon to be Governor, Josh Shapiro, announced a settlement with a company that experienced a data incident . . . .").

solution."[90] Therefore, in the cybersecurity context, a court hearing a data breach case must determine whether a defendant company's actions and cybersecurity controls are reasonable based on a fact-specific inquiry.

The starting point of this analysis is that a company cannot reasonably be expected to do the impossible, and what is possible for one company may be impossible for another. Parameters impacting a company's ability to invest in cybersecurity include its sector, size, and the type of data it handles.[91] For example, financial utility companies spend twice as much on cybersecurity annually as insurance companies, both as a percentage of revenue (0.8% versus 0.4%) and per-employee cost ($4,375 versus $1,984).[92] While those differences may partly stem from some companies' unwillingness—rather than inability—to spend more on cybersecurity, it is still mathematically impossible for a smaller company willing to spend the same percentage of its revenue on cybersecurity as its larger counterpart to match the latter's total investment. Therefore, one should not judge the reasonableness of a company's actions in absolute terms, e.g., its total investment in cybersecurity or whether it suffers a data breach. Instead, one should consider whether those involved in crafting the company's cybersecurity strategy acted reasonably, regardless of whether the strategy successfully thwarts a cyberattack.

2. Core Controls Groups

At a high level, three core control groups are chiefly responsible for framing a company's cybersecurity strategy: internal cybersecurity professionals, external cybersecurity professionals,

---

[90] *E.g.*, Alloway v. Bradlees, Inc., 157 N.J. 221, 723 A.2d 960 (1999) ("the determination of such a duty 'involves identifying, weighing, and balancing several factors—the relationship of the parties, the nature of the attendant risk, the opportunity and ability to exercise care, and the public interest in the proposed solution'").

[91] Alessandra Peters, *How Much Should a Business Spend on Cybersecurity?*, SENSEON (July 14, 2022), https://www.senseon.io/resource/how-much-should-a-business-spend-on-cybersecurity/ (last visited on Nov. 2, 2022).

[92] *Reshaping the Cybersecurity Landscape*, DELOITTE (July 24, 2020), https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html (last visited on Nov. 2, 2022) [hereinafter *Deloitte Report*].

and the company's management.[93] A closer examination of a company may reveal variations from this model, e.g., internal information technology (IT) professionals play an essential role in cybersecurity decisions, or the company does not employ external cybersecurity professionals. These nuances are nonetheless the result of the decisions of the core groups. For example, if the internal IT's influence eclipses that of the cybersecurity professionals, it is up to the company's management to elevate the status of the latter group. Similarly, the decision not to employ external cybersecurity professionals rests with the internal cybersecurity professionals for failing to engage outside help or with the company's management for refusing to authorize the necessary expenditures. As an extreme example, a company may lack any cybersecurity professionals, internal or external, but that decision still rests with the company's management. In sum, while a particular company's situation may differ, three core control groups craft a company's cybersecurity strategy, and deviations from this model result from the decisions made by one or more of those groups. Therefore, to establish a reasonableness standard, one must first review each control group's role in crafting a company's cybersecurity strategy.

3. Internal Cybersecurity Professionals

Aspects of internal cybersecurity professionals' responsibilities make them akin to both in-house accountants and medical generalists. They are like in-house accountants because both groups possess specialized knowledge but may be restricted in exercising their knowledge due to the lack of independence from their employer. For example, both groups are susceptible to budgetary constraints, which have been cited as an insurmountable impediment to establishing

[93] Cybersecurity Is Everyone's Job, NAT'L INST. OF STANDARDS AND TECH. (Oct. 15, 2018) ("The organization's leaders set the tone. Leadership is the most important factor to influencing awareness and mindset. Leaders must embrace cybersecurity education, awareness and best practices"); *NIST Cybersecurity Framework*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Apr. 16, 2018) ("3.2 Establishing or Improving a Cybersecurity Program . . . It is important that organizations identify emerging risks and use cyber threat information from *internal* and *external* sources to gain a better understanding of the likelihood and impact of cybersecurity events") (emphasis added).

internal controls.[94] Both groups' processes and procedures are susceptible to management override, rendering internal controls less effective.[95] Therefore, internal cybersecurity professionals are inevitably restricted in what they can do for their employers. For example, like in-house accountants, they cannot perform functions requiring independence and must rely on their external colleagues for such tasks as ISO 27001 certification audits.[96]

Internal cybersecurity professionals are like medical generalists because both groups must respond to diverse concerns—whether health- or cybersecurity-related—but do not specialize in any one area of concern. For example, small- and medium-sized companies may have only a handful of internal cybersecurity professionals who must therefore rely on IT or external vendors for specialized knowledge.[97] As with medical services in rural and other underserved areas, there is a societal interest in promoting the employment of cybersecurity professionals by companies who traditionally eschewed doing so.[98] In 2020, direct global monetary losses from cybercrime were $945 billion, almost double from $522 billion in 2018.[99]

---

[94] *Mimecast Report*, *supra* note 15 ("[w]hen asked what portion of their company's IT budget was allocated to cyber resilience versus how much should be allocated, the respondents, on average, indicated that 14% of their organization's IT budget was set aside for cybersecurity but that a 17% allocation would be optimal . . . of this year's SOES respondents with a budget shortfall were nearly united (95%) in agreeing that their organization's cyber resilience has been impaired as a result").

[95] *See, e.g.*, In re Yahoo! Inc. Customer Data Sec. Breach Litig., 16-MD-02752-LHK, 2017 WL 3727318, at *2 (N.D. Cal. Aug. 30, 2017) ("requests made by Yahoo's security team for new tools and features such as strengthened cryptography protections were, at times, rejected on the grounds that the requests would cost too much money, were too complicated, or were simply too low a priority").

[96] *What Is Involved in an ISO 27001 Audit?*, ALLIANTIST, https://www.isms.online/iso-27001/whats-involved-in-an-audit/ (last visited on Nov. 2, 2022).

[97] *CISA Cybersecurity Awareness Program Small Business Resources*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Nov. 29, 2021), https://www.cisa.gov/resources-tools/resources/cisa-cybersecurity-awareness-program-small-business-resources (last visited on March 8, 2023) ("In some ways, small businesses are at a higher risk of cyber attacks than larger businesses because they often have fewer resources dedicated to cybersecurity.").

[98] *Data Protection Report*, SHRED-IT (2021), https://www.shredit.com/en-us/data-protection-report-2021 (last visited on Nov. 2, 2022) ("Nearly 70% of U.S. consumers surveyed have been personally impacted by a data breach in 2021 . . . Over 80% of consumers surveyed an extremely high level of importance in personal information security . . .").

[99] Macmillan Keck et. al, The role of cybersecurity and data security in the digital economy, United Nations Capital Development Fund (Feb. 2022), https://policyaccelerator.uncdf.org/policy-tools/brief-cybersecurity-digital-economy (last visited on Jan. 21, 2023) ("The global direct monetary losses from cybercrime in 2020 were estimated to have nearly doubled to USD 945 billion from USD 522.5 billion in 2018").

That same year, the total economic cost of data breaches globally was $4 to $6 trillion, or 4% to 6% of the global GDP.[100] In other words, the humankind suffers a greater indirect cost from data breaches than the direct cost born by the immediate victims. The additional, indirect costs come from such externalities as "opportunity cost, downtime, lost efficiency, brand disparagement, loss of trust, intellectual property infringement, and damage to employee morale."[101] Therefore, the society has an interest in preventing data breaches that goes beyond the interest of each member of the society in preventing data breaches affecting that member.

To prevent data breaches by promoting wider employment of internal cybersecurity professionals, one must introduce the locality standard applicable to medical generalists into the cybersecurity context by evaluating the reasonableness of internal cybersecurity professionals' actions in light of their employer's business environment. As it encourages medical professionals to serve rural and other underserved areas, the locality standard also encourages cybersecurity professionals to accept positions at smaller companies without mature cybersecurity programs by not holding them liable for unavoidable constraints imposed by their employers.

Importing the standards applicable to in-house accountants and medical generalists, one can construct the reasonableness standard for internal cybersecurity professionals as requiring them to identify and relay recommendations to management concerning cybersecurity risks, mitigation strategies, and the need to involve external cybersecurity professionals.

---

[100] *Id*. ("The economic cost of information and technology asset security breaches in 2020 was a staggering USD 4-6 trillion, equivalent to about 4-6% of global GDP").
[101] *Id*.

4. External Cybersecurity Professionals

Aspects of external cybersecurity professionals' responsibilities make them akin to independent accountants, medical specialists, and lawyers. They are like independent accountants because they are not employees of the companies to which they provide services.[102] That is not to say that both groups do not develop a financially-driven business relationship with the company—neither accountants nor cybersecurity professionals provide their services for free.[103] However, because financial compensation does not automatically taint an accounting auditor's independence,[104] external cybersecurity professionals can also remain independent and provide unbiased advice.

External cybersecurity professionals are like medical specialists because they can acquire deep expertise by focusing on a narrow subject matter, e.g., data loss prevention systems or email security. As such, like medical specialists and medical generalists, [105] external cybersecurity specialists must be held to a higher standard than technology generalists and are expected to serve as the final authority in their area of expertise. Therefore, one must introduce the national standard applicable to medical generalists into the cybersecurity context and apply it to external cybersecurity professionals by evaluating the reasonableness of external cybersecurity professionals' actions without regard to individual companies' business environments. As it

---

[102] AICPA CODE OF PROFESSIONAL CONDUCT, *supra* note 64 ("Management participation threat [includes situations when] A member serves as an officer or a director of the attest client. A member accepts responsibility for designing, implementing, or maintaining internal controls for the attest client. A member hires, supervises, or terminates the attest client's employees.").

[103] AICPA CODE OF PROFESSIONAL CONDUCT § 1.210.010.18 (AICPA 2014), https://pub.aicpa.org/codeofconduct/ethics.aspx?targetdoc=et-cod&targetptr=et-cod0.400.21# (last visited on Nov. 2, 2022) ("Undue influence threat. . . . Management pressures the member to reduce necessary audit procedures in order to reduce audit fees.").

[104] *Id*.

[105] *E.g.*, Reeg v. Shaughnessy, 570 F.2d 309, 314 (10th Cir. 1978) ("Oklahoma law . . . holds specialists to a higher standard of care than that required of general practitioners"); Myles v. Laffitte, 986 F.2d 1414, at *1 (4th Cir. 1993) ("specialists are held to a higher standard of care than that required of general practitioners"); Cross v. Huttenlocher, 440 A.2d 952, 955 (Conn. 1981) (testimony by two specialists in pediatric neurology did not establish the standard of care of a general pediatrician).

encourages medical professionals to serve as the final authority in their respective areas of specialization, the national standard also encourages cybersecurity professionals to become experts in their respective areas.

There are also reasons to apply elements of legal ethics to cybersecurity providers. First, although cybersecurity is a specialized field, cybersecurity services are often offered by companies that provide other information technology services.[106] Applying Model Rule 7.2(c), which requires that lawyers advertising a particular specialty be certified in that specialty,[107] satisfies clients' reasonable expectation that an information technology company advertising cybersecurity services is indeed capable of providing them rather than engaging in a clever marketing ploy. Second, many clients seek a "reset" of their cybersecurity practice when contracting with a new cybersecurity vendor.[108] Applying Model Rules 1.1 and 1.3, which require competence and diligence rather than a mere improvement of a client's condition over the alternatives,[109] ensures that clients receive the reset they desire rather than a mere incremental improvement over their prior practices.

Importing the standards applicable to independent accountants, medical specialists, and lawyers, one can construct the reasonableness standard for external cybersecurity professionals by requiring companies that offer cybersecurity services to serve as the final authority in their

---

[106] *See, e.g.*, PRESIDIO, https://www.presidio.com/ (last visited on Nov. 2, 2022) (offering cybersecurity services in addition to other services such as managed services, implementation services, procurement services, etc.).
[107] MODEL RULES OF PROF'L CONDUCT r. 7.2 (AM. BAR ASS'N 2020) ("A lawyer shall not state or imply that a lawyer is certified as a specialist in a particular field of law, unless . . . the lawyer has been certified as a specialist . . .").
[108] *See e.g., Are you ready for the great cybersecurity RESET?*, ZSCALER (Oct. 4, 2021), https://revolutionaries.zscaler.com/insights/are-you-ready-great-cybersecurity-reset (last visited on Nov. 2, 2022) ("Technology leaders are demanding a plan that incorporates everything that we have learned so far. It is as if the world is taking stock and approaching this time as an opportunity to RESET. Reset the thinking, the design, the coverage, the spending patterns, the maintenance costs, the complexity, the partners engaged, and the effectiveness of integration."); *The Cybersecurity Reset Starts With Zero Trust*, CIO MAGAZINE (Nov 3, 2021), https://www.cio.com/article/189524/the-cybersecurity-reset-starts-with-zero-trust.html (last visited on Nov. 2, 2022) ("The reset is a new wave of activity and an emerging global trend centered around cybersecurity planning.").
[109] MODEL RULES OF PROF'L CONDUCT r. 1.1, 1.3 (AM. BAR ASS'N 2020).

respective areas of specialization, preserve independence, and deliver advice untainted by their relationship with their clients.

5. Company's Management

A company's management's role in the cybersecurity context essentially mimics its role in the accounting context: take appropriate actions based on advice from internal and external cybersecurity professionals. As in the accounting context, the company's management bears the ultimate responsibility for the company's cybersecurity systems.[110] Management can affect the company's cybersecurity posture in multiple ways, including budgetary allocations, management override, and business strategy. For example, a company whose management frequently overrides established cybersecurity practices and procedures is likely to have a weaker cybersecurity posture than a company whose management observes established cybersecurity protocols.[111] Similarly, a company whose management allocates less budget than cybersecurity professionals find optimal is likely to suffer from impaired cybersecurity controls.[112]

A company's management—particularly its board of directors—also bears a fiduciary duty to ensure the adequacy of the company's internal controls.[113] While the board does not have to implement a corporate system of espionage to identify every instance of wrongdoing, it

---

[110] 15 U.S.C. § 7241(a) (a publicly traded company's CEO and CFO must certify, among other things, that they "are responsible for establishing and maintaining internal controls," made appropriate disclosures to the company's independent auditors, and are not aware of any untrue or misleading information contained in the financial statements).

[111] *See, e.g.*, In re Yahoo! Inc. Customer Data Sec. Breach Litig., 16-MD-02752-LHK, 2017 WL 3727318, at *2 (N.D. Cal. Aug. 30, 2017) ("requests made by Yahoo's security team for new tools and features such as strengthened cryptography protections were, at times, rejected on the grounds that the requests would cost too much money, were too complicated, or were simply too low a priority").

[112] *Mimecast Report*, *supra* note 15 ("[w]hen asked what portion of their company's IT budget was allocated to cyber resilience versus how much should be allocated, the respondents, on average, indicated that 14% of their organization's IT budget was set aside for cybersecurity but that a 17% allocation would be optimal . . . of this year's SOES respondents with a budget shortfall were nearly united (95%) in agreeing that their organization's cyber resilience has been impaired as a result").

[113] In re Caremark International Inc. Derivative Litig., 698 A.2d 959, 969-70 (Del. Ch. 1996) (directors have "duty to attempt in good faith to assure that [an adequate] corporate information and reporting system exists" but they do not have to install a "corporate system of espionage to ferret out wrongdoing").

must ensure an adequate flow of information to keep itself informed.[114] Failure to implement or monitor internal controls is a violation of directors' duty of care or good faith and exposes directors to personal liability for the consequences.[115] In the cybersecurity context, management must ensure, at the very least, that internal and external cybersecurity professionals have a way of reporting cybersecurity risks and recommendations to keep management informed and allow it to make informed decisions.

Implementing adequate internal controls can exculpate management from liability for subsequent data breaches in two ways. First, management is not liable if cybersecurity professionals fail to inform it despite its good-faith effort to remain informed.[116] Second, management's informed decisions are subject to the business judgment rule, which creates a rebuttable presumption that management acted appropriately even if its decision turns out to be wrong.[117] Rebutting a business judgment rule presumption requires a showing of fraud or illegality, conflict of interest, or lack of informed process—a high bar to satisfy.[118] The reason for the high deference to management's informed decisions is that management is most familiar with the company's circumstances and business strategy, not just the external factors such as its sector and size.[119]

---

[114] *Id*.
[115] *Id*.
[116] *Id*.
[117] Shlensky v. Wrigley, 237 N.E.2d 776, 779 (Ill. App. Ct. 1968) ("The judgment of the directors of corporations enjoys the benefit of a presumption that it was formed in good faith and was designed to promote the best interests of the corporation they serve").
[118] *Id*. at 781 ("courts will not step in and interfere with honest business judgment of the directors unless there is a showing of fraud, illegality or conflict of interest").
[119] *Id*. at 781 ("Furthermore, it cannot be said that directors, even those of corporations that are losing money, must follow the lead of the other corporations in the field. Directors are elected for their business capabilities and judgment and the courts cannot require them to forego their judgment because of the decisions of directors of other companies").

Therefore, while management carries the ultimate responsibility for failure to follow cybersecurity professional's recommendations that result in a data breach, management is not *per se* liable for a data breach if cybersecurity professionals failed to inform management despite the latter's good-faith effort to remain informed or if management made an informed but incorrect judgment call.

D. Applying the New Reasonableness Standard

To flesh out the new reasonableness standard, it is helpful to apply it to the facts of several real-life cybersecurity incidents discussed in this section. While courts applied other prevailing legal standards, this section aims to recast the conversation in terms of the new reasonableness standard.

1. Yahoo's Data Breaches

The Yahoo case dealt with several data breaches at Yahoo.[120] The first data breach occurred in 2012 and involved the disclosure of users' passwords.[121] External cybersecurity professionals were befuddled by Yahoo's decision to store users' passwords in plain text instead of encrypting them per the accepted security principles of the time.[122] Worse, even the hackers commented that Yahoo's systems contained egregious security vulnerability and left a note saying the data breach was meant "as a wake-up call, and not as a threat."[123] Even if Yahoo was unaware of its cybersecurity systems' deficiencies, the 2012 breach put it on notice.

---

[120] In re Yahoo! Inc. Customer Data Sec. Breach Litig., 16-MD-02752-LHK, 2017 WL 3727318, at *2 (N.D. Cal. Aug. 30, 2017) ("[i]n 2012, Yahoo admitted that more than 450,000 user accounts were compromised through an SQL injection attack—with the passwords simply stored in plain text. . . . [s]ecurity experts were befuddled ... as to why a company as large as Yahoo would fail to cryptographically store the passwords in its database. Instead, [the passwords] were left in plain text, which means a hacker could easily read them.").
[121] *Id.*
[122] *Id.*
[123] *Id.*

Nonetheless, Yahoo seemingly continued its deficient cybersecurity practices unabated.[124] For example, Yahoo repeatedly rejected requests for tools to address its cybersecurity shortcomings.[125] Although the court's opinion does not specify who rejected these requests, the reasons cited for the rejection resemble the reasons a company's management uses: budgetary constraints, complexity, and overriding priorities.[126] Even if Yahoo's management rejected the requests coming from Yahoo's internal or external cybersecurity professionals, the management's failure to prevent subsequent data breaches is not *per se* unreasonable because the management's actions must be considered in the context of two sets of factors (1) the company's sector, size, and the type of data it handles, and (2) internal and external cybersecurity professionals' efforts to inform management of the cybersecurity risks.[127]

Yahoo is part of the information sector.[128] Its market capitalization fluctuated between $20 and $40 billion in the years surrounding the 2012 data breach.[129] Unlike Yahoo, other companies in the information sector realized the importance of cybersecurity and took appropriate measures and a hard stance against data breaches.[130] For example, Google publicly

---

[124] *Id.* ("Yahoo's internal culture actively discouraged emphasis on data security").
[125] *Id*. ("requests made by Yahoo's security team for new tools and features such as strengthened cryptography protections were, at times, rejected on the grounds that the requests would cost too much money, were too complicated, or were simply too low a priority").
[126] *Cf.* In re Yahoo!, 2017 WL 3727318, at *2 ("the requests would cost too much money, were too complicated, or were simply too low a priority") *with Mimecast Report*, *supra* note 15 ("[w]hen asked what portion of their company's IT budget was allocated to cyber resilience versus how much should be allocated, the respondents, on average, indicated that 14% of their organization's IT budget was set aside for cybersecurity but that a 17% allocation would be optimal . . . of this year's SOES respondents with a budget shortfall were nearly united (95%) in agreeing that their organization's cyber resilience has been impaired as a result").
[127] Peters, *supra* note 91.
[128] Yahoo Inc. Company Profile, DUN & BRADSTREET, https://www.dnb.com/business-directory/company-profiles.yahoo_inc.d5a8bcd4a4e65ba60541963146cf8a52.html (last visited on Nov. 2, 2022) ("HOME / BUSINESS DIRECTORY / *INFORMATION* / DATA PROCESSING, HOSTING, AND RELATED SERVICES") (emphasis added).
[129] Myles Udland, *Yahoo's Market Cap*, BUSINESS INSIDER (July 25, 2016), https://www.businessinsider.com/yahoo-market-cap-over-time-2016-7 (last visited on Nov. 2, 2022).
[130] Michael Arrington, *Google Defends Against Large Scale Chinese Cyber Attack: May Cease Chinese Operations*, TECH CRUNCH (Jan. 12, 2010), https://techcrunch.com/2010/01/12/google-china-attacks/ (last visited on Nov. 2, 2022) ("Should the Chinese government decide that an uncensored engine is illegal, then Google may cease

threatened to cease its operations in China within a month after attacks seeking access to Chinese human rights activists' Gmail accounts, even though those attacks were largely unsuccessful.[131] Although Google's market capitalization was several times greater than Yahoo's,[132] that difference alone is unlikely to explain the sharp contract between Google's actions and Yahoo's alleged inaction: the latter's internal cybersecurity professionals allegedly knew of a similar attack perpetrated by Russian and Canadian hackers in 2015 and 2016 but did nothing to stop it.[133]

The allegations against the internal cybersecurity professionals pertain to the second set of factors that must be considered when evaluating the reasonableness of Yahoo's management's actions or lack thereof. In other words, if Yahoo's internal cybersecurity professionals failed to identify and relay recommendations to management concerning cybersecurity risks, mitigation strategies, and the need to involve external cybersecurity professionals, Yahoo's management's inaction may not be unreasonable. Unfortunately, the court's opinion does not explore whether Yahoo's internal cybersecurity professionals informed the company's management about the ongoing attack or whether their inaction resulted from the management's decision to ignore the risk. If Yahoo's internal cybersecurity professionals informed the company's management, the management's subsequent inaction was unreasonable. On the other hand, if Yahoo's internal cybersecurity professionals failed to inform management, the reasonableness of management's

---

operations in China entirely. . . . [A] primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists . . . . Only two Gmail accounts appear to have been accessed, and that activity was limited to account information . . . rather than the content of emails themselves.").

[131] *Id*.

[132] Jay Yarow, *Apple, Google Market Cap*, BUSINESS INSIDER (Oct. 18, 2013), https://www.businessinsider.com/apple-google-market-cap-chart-2013-10 (last visited on Nov. 2, 2022).

[133] In re Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, at *4 (N.D. Cal. Aug. 30, 2017) ("an independent committee of Yahoo's Board of Directors had determined that Yahoo's information security team knew, at a minimum, about the Forged Cookie Breach as it was happening, 'but took no real action in the face of that knowledge.'")

response turns on whether management satisfied its fiduciary duty to implement internal controls and remain informed.[134] If management satisfied that duty and made an informed decision to limit or forego remedial actions, that decision is subject to the business judgment rule presumption of propriety.[135] If management remained uninformed due to its failure to implement adequate internal controls, management bore the responsibility for the subsequent data breach.[136]

2. Kaspersky's Fall from Grace

The Kaspersky case dealt with the United States Department of Homeland Security's ban on the U.S. Federal Government's use of Kaspersky's cybersecurity products.[137] The court correctly addressed the issue presented by Kaspersky—whether the prohibition constituted an impermissible legislative punishment—and concluded that it did not.[138] However, the case presents a good opportunity to test the application of the new reasonableness standard to external cybersecurity professionals by asking whether Kaspersky can satisfy the new standard if the government does not block the use of the company's product.

Kaspersky is one of the world's leading cybersecurity vendors.[139] It is headquartered in Moscow and argues that its ties with Russia and other countries where many cyber threats

---

[134] In re Caremark International Inc. Derivative Litig., 698 A.2d 959, 969-70 (Del. Ch. 1996) (directors have "duty to attempt in good faith to assure that [an adequate] corporate information and reporting system exists" but they do not have to install a "corporate system of espionage to ferret out wrongdoing").
[135] Shlensky v. Wrigley, 237 N.E.2d 776, 779 (Ill. App. Ct. 1968) ("The judgment of the directors of corporations enjoys the benefit of a presumption that it was formed in good faith and was designed to promote the best interests of the corporation they serve").
[136] In re Caremark International Inc. Derivative Litig., 698 A.2d 959, 969-70 (Del. Ch. 1996) (directors have "duty to attempt in good faith to assure that [an adequate] corporate information and reporting system exists" but they do not have to install a "corporate system of espionage to ferret out wrongdoing").
[137] Kaspersky Lab, Inc. v. United States Dep't of Homeland Sec., 909 F.3d 446, 452-53 (D.C. Cir. 2018) ("No department, agency, organization, or other element of the Federal Government may use . . . any hardware, software, or services . . . by Kaspersky Lab").
[138] *Id*. at 450 ("Kaspersky sued, arguing that the prohibition constitutes an impermissible legislative punishment—what the Constitution calls a bill of attainder").
[139] *Id*. ("Ranking among the world's top four cybersecurity vendors, Kaspersky 'has successfully investigated and disrupted" cyberattacks by "Arabic-, Chinese-, English-, French-, Korean-, Russian-, and Spanish-speaking' hackers.")

originate make it uniquely positioned to help its customers thwart cyberattacks.[140] However, the U.S. government viewed Kaspersky's Russian ties differently.[141] In the aftermath of Russia's efforts to influence the 2016 presidential election, government officials, including Congresspersons, began voicing concerns about the U.S. government's use of Kaspersky's products.[142] The court summarized these concerns by describing Kaspersky as "a proverbial fox in the government's cyber-henhouse: a threat to the very systems it is meant to protect."[143]

According to the new reasonableness standard, external cybersecurity professionals such as Kaspersky must serve as the final authority in their respective areas of specialization, preserve independence, and deliver advice untainted by their client relationship. Therefore, the question of Kaspersky's ability turns primarily on whether it can maintain independence and provide untainted advice. Like accounting professionals, independence for cybersecurity professionals requires avoiding influences that compromise a cybersecurity professional's judgment and avoiding the appearance that their judgment is compromised.[144] Even if Kaspersky can avoid undue influence from the Russian government, it cannot avoid the appearance that its judgment is compromised based on the "chorus of concern" highlighted by the court.[145] Therefore, even if

---

[140] *Id*. ("Founded by a Russian national and headquartered in Moscow, Kaspersky boasts that its 'presence in Russia and its deployment in areas of the world in which many sophisticated cyber-threats originate . . . makes it a unique and essential partner in the fight against such threats,' including hacker groups with suspected connections to Russian intelligence services.")
[141] *Id*. at 451 ("But the U.S. government has come to disagree.").
[142] *Id*. at 451 ("The chorus of concern about Kaspersky began to swell in the spring of 2017. Between March and July of that year, Kaspersky garnered attention in at least five committee hearings before both houses of Congress.").
[143] *Id*.
[144] AICPA CODE OF PROFESSIONAL CONDUCT § 0.400.21 (AICPA 2014), https://pub.aicpa.org/codeofconduct/ethics.aspx?targetdoc=et-cod&targetptr=et-cod0.400.21# (last visited on Nov. 2, 2022) ("Independence. Consists of two elements, defined as follows: a. Independence of mind . . . b. Independence in appearance . . .").
[145] Kaspersky Lab, Inc. v. United States Dep't of Homeland Sec., 909 F.3d 446, 451 (D.C. Cir. 2018) ("The chorus of concern about Kaspersky began to swell in the spring of 2017.").

Kaspersky can continue unrestricted sales of its products, it cannot fulfill its duties as an external cybersecurity vendor based on the new reasonableness standard.

3. The Grey Area of the Cloud

The Capital One case dealt with a 2019 data breach resulting from Capital One's use of Amazon Web Services (AWS).[146] The lawsuit names both Capital One and Amazon as defendants.[147] Both defendants "were well-aware of the AWS cloud's vulnerabilities to unauthorized access through a SSRF attack."[148] An SSRF attack involves submitting a request to a server to retrieve a resource that the attacker does not have permission to access, but the server does.[149] The defendants were so concerned about AWS's SSRF vulnerability that they decided to jointly develop a new product, called Cloud Custodian, to address it by encrypting Capital One's data.[150] However, the solution was inadequate because it failed to address the problem underlying an SSRF attack: any server within Capital One's AWS environment could access and automatically decrypt any piece of Capital One's data.[151] On the contrary, the implemented safeguards made an SSRF attack uniquely suited to bypass Capital One and Amazon's defenses because accessing one internal resource through an SSRF attack allowed an attacker to automatically decrypt any piece of data.[152]

---

[146] In re Cap. One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 388 (E.D. Va. 2020).
[147] *Id*. at 387 ("Defendants Capital One and Amazon have filed Motions to Dismiss . . .").
[148] *Id*. at 389.
[149] *Server-side request forgery (SSRF)*, PORTSWIGGER, https://portswigger.net/web-security/ssrf (last visited on Nov. 2, 2022) ("[i]n a typical SSRF attack, the attacker might cause the server to make a connection to internal-only services within the organization's infrastructure").
[150] In re Cap. One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 389 (E.D. Va. 2020) ("in an attempt to protect against this vulnerability, Capital One and Amazon jointly developed a product called Cloud Custodian, whose purpose was to address the SSRF threat by encrypting data on the AWS servers").
[151] *Id*. ("if an unauthorized individual were able to gain access to a credential in the AWS cloud environment, known technically as an "Identity Access Management" role, the credential would allow the unauthorized individual broad access beyond the firewall protecting the cloud and automatic decryption of the data stored in the cloud").
[152] *Id*.

Applying the new reasonableness standard first turns on whether Amazon can be considered an external cybersecurity vendor. AWS offers diverse products and services focusing on cloud computing and hosting services, making it an information technology but not necessarily a cybersecurity vendor.[153] Nonetheless, security is one of AWS's offerings.[154] Besides standalone security features, AWS also highlights security as a core design principle for all its offerings.[155]

AWS is not the only cloud services provider with a significant focus on cybersecurity.[156] Microsoft Azure, one of AWS's main competitors, also boasts that cybersecurity underpins its cloud services.[157] Google Cloud similarly highlights its security-by-design approach as one of the reasons to use its cloud services.[158] The cloud providers' message resonates with industry observers and businesses alike.[159] Industry observers repeatedly cite enhanced cybersecurity as one of the top reasons businesses move to the cloud, with some citing it as the top reason.[160]

---

[153] *AWS Cloud Products*, AMAZON, https://aws.amazon.com/products/ (last visited on Nov. 2, 2022).
[154] *Id*. (listing the following top offerings: Compute; Storage; Database; Networking & Content Delivery; Analytics; Machine Learning; and Security, Identity, & Compliance).
[155] *AWS Cloud Security*, AMAZON, https://aws.amazon.com/security/ (last visited on Nov. 2, 2022) ("AWS is designed to help you build *secure*, high-performing, resilient, and efficient infrastructure for your applications") (emphasis added).
[156] *Azure Security*, MICROSOFT, https://azure.microsoft.com/en-us/explore/security/ (last visited on Nov. 2, 2022) ("Start with a secure foundation . . . Take advantage of multi-layered security provided by Microsoft across physical datacenters, infrastructure, and operations in Azure. Gain from the state-of-art security delivered in Azure data centers globally.").
[157] *Id*.
[158] *Your security transformation: safer with Google technology and expertise*, GOOGLE CLOUD, https://cloud.google.com/security (last visited on Nov. 2, 2022) (As you move to the cloud, . . . Google Cloud provides a secure-by-design foundation.").
[159] See, e.g., Sean Blake, 5 reasons why you need to move to the cloud, EASY AGILE (Apr. 22, 2022), https://www.easyagile.com/blog/5-reasons-to-move-to-cloud/ (last visited on Nov. 2, 2022) (citing enhanced security as the second top reason to move to the cloud); Top Reasons to Move to the Cloud, LOFFLER (Feb. 27, 2019) https://www.loffler.com/blog/top-reasons-to-move-to-the-cloud (last visited on Nov. 2, 2022) (citing enhanced security as the sixth top reason to move to the cloud); Greg Williams, 7 Urgent Reasons to Move to the Cloud in 2022, WESTERN COMPUTER (Feb. 17, 2022), https://resources.westerncomputer.com/blog/7-urgent-reasons-to-move-to-the-cloud-in-2022 (last visited on Nov. 2, 2022) (citing enhanced security as the top reason to move to the cloud).
[160] *Id*.

Among businesses, even the traditional holdouts such as law firms have embraced the cloud, often citing security concerns.[161]

In sum, cloud providers are more akin to external cybersecurity vendors than traditional information technology companies such as colocation vendors. A colocation vendor provides physical data center space and environmental controls, such as power, cooling, and physical security.[162] Using a colocation vendor allows a company to avoid the capital expenditures needed to build its own data center, but each customer must still purchase, install, and configure its own servers, network devices, and firewalls.[163] In other words, while colocation providers provide physical security, their customers must implement their own network security.[164] Cloud providers, on the other hand, boast about their ability to improve customers' cybersecurity posture.[165] As doctors holding themselves out as experts in a particular area must follow the

---

[161] *See, e.g.*, Isha Marathe, *Firms' Cloud Migration Plows Ahead, as Vendors Force Transition*, LAW.COM (Oct. 5, 2022), https://www.law.com/legaltechnews/2022/10/05/firms-cloud-migration-plows-ahead-as-vendors-force-transition/ (last visited on Nov. 2, 2022) ("[o]nce held back by fears of exorbitant expenses and security concerns, many law firms have become comfortable with cloud technology over the last few years"); *Why Law Firms are Switching to the Cloud*, PRACTICE PANTHER, https://www.practicepanther.com/blog/law-firms-are-switching-to-the-cloud-heres-why/ (last visited on Nov. 2, 2022) ("law firms switching from on-site data management to the cloud has become the norm due to rapid advancements in cybersecurity").

[162] *What is Colocation?*, RACKSPACE, https://www.rackspace.com/library/what-is-colocation (last visited on Nov. 2, 2022) ("Colocation . . . is the practice of renting space for your servers and other computing hardware at a third-party provider's data center facility. Typically, colocation services include the building in which everything is housed, as well as networking, physical security, redundant power and redundant cooling components, which then support the servers and storage provided by the customer."); *Colocation Explained*, GLOBALDOTS (April 21, 2021), https://www.globaldots.com/resources/blog/colocation-explained/ (last visited on Nov. 2, 2022) ("Typically, colocation services include the building in which everything is housed, as well as networking, physical security, redundant power and redundant cooling components, which then support the servers and storage provided by the customer.").

[163] *Colocation Explained*, GLOBALDOTS (April 21, 2021), https://www.globaldots.com/resources/blog/colocation-explained/ (last visited on Nov. 2, 2022) ("With colocation, you purchase and own both the hardware (servers) and software that will host your web presence, AND you are responsible for properly setting up and configuring both. Depending upon your needs, you may also purchase a network device or two (switch, router, firewall, vpn appliance, etc) to manage traffic in and out of your servers. Usually these are not sold to you by the colocation provider, nor do they dictate what you can or cannot buy – you are free to choose the combination that best fits your needs.").

[164] *Id*.

[165] E.g., *AWS Cloud Security*, AMAZON, https://aws.amazon.com/security/ (last visited on Nov. 2, 2022) ("AWS is designed to help you build *secure*, high-performing, resilient, and efficient infrastructure for your applications") (emphasis added); *Azure Security*, MICROSOFT, https://azure.microsoft.com/en-us/explore/security/ (last visited on

standards applicable to specialists in that area,[166] so should cloud vendors holding themselves out as cybersecurity experts follow the same standards as cybersecurity vendors.

Alternatively, if cloud vendors holding themselves out as cybersecurity experts do not have the same duty as external cybersecurity professionals, each customer must negotiate every cybersecurity detail in the fine print of its individual contract with a cloud vendor. This approach fails for two reasons: it assumes that customers are sophisticated enough to understand the cybersecurity nuances and that they have bargaining power in negotiations with cloud vendors. First, many cloud customers struggle to understand their responsibilities and liabilities when dealing with a cloud vendor.[167] Second, due to their dominance in the marketplace, many large cloud providers shepherd their customers into adhesion contracts without giving them much ability to negotiate the finer points even if they understand the need to do so.[168] Therefore, private contracts are an insufficient device to address the reasonable expectations that cloud providers holding themselves out as cybersecurity experts act as such.

Nov. 2, 2022) ("Start with a secure foundation . . . Take advantage of multi-layered security provided by Microsoft across physical datacenters, infrastructure, and operations in Azure. Gain from the state-of-art security delivered in Azure data centers globally."); *Your security transformation: safer with Google technology and expertise*, GOOGLE, https://cloud.google.com/security (last visited on Nov. 2, 2022) (As you move to the cloud, . . . Google Cloud provides a secure-by-design foundation.").

[166] *E.g.*, Reeg v. Shaughnessy, 570 F.2d 309, 314-15 (10th Cir. 1978) ("[I]t would have been improper to hold [plaintiff] to a standard of an orthopedic surgeon, inasmuch as he was not board certified in that specialty. . . . [Plaintiff] had performed more than half of the orthopedic operations for the Fetzer Clinic. He was not, however, a board certified surgeon in either the general or orthopedic fields."). *See supra* 58.

[167] Vicki Tambellini, *Reading The Fine Print: Protecting Your Organization From Vendor Cyberattacks*, FORBES (Nov. 29, 2022), https://www.forbes.com/sites/forbesbusinesscouncil/2022/11/29/reading-the-fine-print-protecting-your-organization-from-vendor-cyberattacks/ (last visited on Jan. 21, 2023) ("Many institutions struggled to figure out their related responsibilities and liabilities."). *See also* Patrick Gray, *The "Fine Print" of Cloud Computing*, TechRepublic (Apr. 24, 2011).

[168] Tom Mozingo, *Revisiting the Enforceability of Online Contracts: The Need for Unambiguous Assent to Inconspicuous Terms*, 43 SEATTLE U. L. REV. 1065, 1081 (2020) ("There are many examples of successful, easy to access click-wrap contracts. Amazon Web Services uses a checkbox that users must click before creating an account, coupled with text stating: 'Check here to indicate that you have read and agree to the terms of the AWS Customer Agreement.'"); William Gamble, 9 Point Cloud Contract Check List, LinkedIn (Aug. 8, 2016), https://www.linkedin.com/pulse/9-point-cloud-contract-check-list-william-gamble (last visited on Jan. 21, 2023) ("With such domination there is a greater likelihood of contracts of adhesion").

According to the new reasonableness standard, external cybersecurity professionals must serve as the final authority in their respective areas of specialization, preserve independence, and deliver advice untainted by their client relationship. While the data breach itself does not mean that AWS failed to meet the reasonableness standard, the fact that AWS was aware of the vulnerability leading to the data breach and failed to address it may indicate that AWS lacked the necessary expertise or independence. SSRF is a known attack variety with known methods for mitigating its risk.[169] If AWS was unaware of proper ways to mitigate SSRF, it lacked the necessary expertise to serve as a cybersecurity vendor. On the other hand, if AWS knew the proper ways to mitigate SSRF but failed to advise its client, Capital One, due to the magnitude of their financial relationship, it lacked the independence required of external cybersecurity vendors. In either case, AWS acted unreasonably when judged by the new reasonableness standard for external cybersecurity professionals.

4. Social Engineering Attacks

Social engineering is a set of attack vectors that are among the most prevalent cyber threats.[170] In 2022, hotel group Marriott confirmed a data breach of 20 gigabytes of sensitive information resulting from a cyberattack in which hackers claimed to use social engineering to

---

[169] See, e.g., *Server Side Request Forgery Prevention*, OWASP CHEAT SHEETS SERIES, https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html (last visited on Nov. 2, 2022) ("Several protective measures are possible at the Application and Network layers. To apply the defense in depth principle, both layers will be hardened against such attacks."); Amar Zlojic, *Server Side Request Forgery (SSRF) Attacks & How to Prevent Them*, BRIGHT SECURITY (Apr. 2, 2022), https://brightsec.com/blog/ssrf-server-side-request-forgery/ (last visited on Nov. 2, 2022).

[170] *15 Examples of Real Social Engineering Attacks*, TESSIAN (Feb. 7, 2022), https://www.tessian.com/blog/examples-of-social-engineering-attacks/ (last visited on Nov. 2, 2022) ("[s]ocial engineering attacks are one of the main ways bad actors can scam companies"); *What Is Social Engineering*, IMPERVA, https://www.imperva.com/learn/application-security/social-engineering-attack/ (last visited on Nov. 2, 2022) ("What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.").

trick Marriott employees into giving hackers access to employees' computers.[171] Many similar social engineering attacks resulted in both data breaches and financial losses.[172]

Social engineering differs from other attack vectors because it relies on human error rather than technical vulnerabilities.[173] Whereas other cyberattacks target a company's infrastructure, social engineering targets its people.[174] For example, a threat actor may send phishing emails to a company's employees to try to get them to reveal sensitive information or allow the sender to access their computers to steal sensitive information.[175] Because a social engineering attack does not rely on technical vulnerabilities, the three control groups—internal cybersecurity professionals, external cybersecurity professionals, and the company's management—may conclude that they are not liable for cyber incidents resulting from social engineering attacks. Applying the new reasonableness standard highlights that this view is shortsighted.

It is a well-known fact that a vast majority of breaches—82%, according to some reports—involve a human element.[176] The mitigating measure—employee training—is as well-

---

[171] Carly Page, *Hotel giant Marriott confirms yet another data breach*, TECH CRUNCH (July 6, 2022), https://techcrunch.com/2022/07/06/marriott-breach-again/ (last visited on Nov. 2, 2022) ("Hotel group Marriott International has confirmed another data breach, with hackers claiming to have stolen 20 gigabytes of sensitive data, including guests' credit card information . . . when an unnamed hacking group claimed they used social engineering to trick an employee at a Marriott hotel in Maryland into giving them access to their computer.").

[172] *15 Examples of Real Social Engineering Attacks*, TESSIAN (Feb. 7, 2022), https://www.tessian.com/blog/examples-of-social-engineering-attacks/ (last visited on Nov. 2, 2022) ("$100 Million Google and Facebook Spear Phishing Scam . . . Microsoft 365 phishing scam steals user credentials . . .").

[173] *What Is Social Engineering*, IMPERVA, https://www.imperva.com/learn/application-security/social-engineering-attack/ (last visited on Nov. 2, 2022) ("What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.").

[174] *Common Types of Cybersecurity Attacks*, RAPID7, https://www.rapid7.com/fundamentals/types-of-attacks/ (last visited on Nov. 2, 2022) ("In an SQL injection attack, an attacker goes after a vulnerable website to target its stored data, such as user credentials or sensitive financial data.").

[175] *Id*.

[176] *Verizon Report*, *supra* note 4 ("This year, 82% of breaches in the DBIR14 involved the human element. This puts the person square in the center of the security estate with the Social Engineering pattern capturing many of those human-centric events.").

known as the social engineering attacks themselves.[177] A training program can educate employees about the dangers of clicking on links in suspicious emails and the need to use password keepers.[178] Companies do not have to create their own cybersecurity training curricula—they can partner with one of many training vendors.[179] Many training vendors allow customers to choose from a library of prepackaged training modules to suit each customer's needs.[180]

The new reasonableness standard requires a company's management and internal and external cybersecurity professionals to treat social engineering as any other threat. Internal cybersecurity professionals must alert management about the threat and identify the top categories of social engineering attacks that a company's employees are likely to face. Management must allocate appropriate funds and ensure employees' compliance with the training requirements. External cybersecurity vendors, i.e., training vendors, must offer fresh and accurate content. Therefore, while it may be tempting to treat social engineering attacks differently than other attack vectors, the new reasonableness standard does not mandate this distinction.

IV. CONCLUSION

The new reasonableness standard offers a comprehensive overhaul of the standard of care applicable to the three control groups chiefly responsible for framing a company's cybersecurity

---

[177] *Verizon Report*, *supra* note 4 ("But, we can get better, both at what we do and what we build. To that end, training is a big part of improving.").
[178] *Verizon Report*, *supra* note 4 ("Training can potentially help improve security behaviors, in both day-to-day (such as Don't Click … Stuff, and using a password keeper) as well as in design (such as secure coding, lifecycle management, etc.).").
[179] *KnowBe4 Recognized as a Leader in Security Awareness and Training Solutions by Forrester Research*, KNOWBE4, https://www.knowbe4.com/forrester-wave-security-awareness-training (last visited on Nov. 2, 2022) ("As the provider of the world's largest security awareness training platform, we believe being named a Leader continues to show our success in our ability to enable organizations and their users to make smarter security decisions, improve security culture and mitigate risk using world-class training and simulated phishing.").
[180] *Overview of KnowBe4 Training Module Library*, KNOWBE4, https://www.knowbe4.com/en/knowbe4-training-modules-overview/ (last visited on Nov. 2, 2022).

strategy: internal cybersecurity professionals, a company's management, and external cybersecurity professionals. While it does not preclude the application of other causes of action to data breach cases—including statutory compliance, privacy torts, and negligence—the new standard offers an alternative view of what is expected from the three groups. Internal cybersecurity professionals must identify and relay recommendations to management concerning cybersecurity risks, mitigation strategies, and the need to involve external cybersecurity professionals. External cybersecurity professionals must serve as the final authority in their respective areas of specialization, preserve independence, and deliver advice untainted by their relationship with their clients. A company's management must bear the final responsibility for implementing internal controls and following cybersecurity professionals' advice but is not *per se* liable for a data breach if cybersecurity professionals failed to inform management despite the latter's good-faith effort to remain informed or if management made an informed but incorrect judgment call.