"REASONABLE [CYBERSECURITY] MEASURES" FOR DIGITAL TRADE SECRETS: LESSONS FROM MARKETING

RAJ SACHDEV[**]

The loss of digital trade secrets in marketing and beyond, often the source of competitive advantage, can have disastrous impacts on brands and companies. Bad actors want to get their digital hands on digital trade secrets, and other actors and factors may also cause a risk to their secrecy. The Defend Trade Secrets Act (DTSA) makes clear that "reasonable measures" must be taken to maintain the secrecy of a trade secret. Likewise, the Uniform Trade Secrets Act (UTSA) requires "*reasonable steps.*" *However, in a digital age, the definition of what is "reasonable" is even more unclear than in offline settings. Here, cybersecurity plays a key role, albeit not the only role. What cybersecurity measures could be put in place to meet the*

---

* *MSc (Oxford), LLM, LLM(IP), MBA, DBA, PCM, CIPP/US*; Assistant Facilitator (Cornell Law), Assistant Professor (PSU), Adjunct Faculty (UNH Law); researcher, speaker, licensed attorney (CA), licensed solicitor (England/Wales). Forthcoming author of Digital Marketing Law and Regulation in the US, UK and EU (Edward Elgar) and author of Digital Marketing (McGraw Hill). In full disclosure, the author proposed and created the Legal Control in the Cloud Security Alliance IoT Security Controls Framework Version 2.

*This article has undergone a peer review process through IDEA. IDEA thanks the peer reviewers for their valuable input during the process. The author thanks many reputed scholars, Ryan Vacca for extensive review and feedback, intellectual property scholars at WIPIP 2025 for their feedback during a session where a draft of this article was presented, Kasper Rasmussen and Sriharsha Mallapuram for feedback on cybersecurity aspects, and Jon Cavicchi for his helpful guidance. The author also thanks the IDEA Editor-in-Chief and other law students for their impeccable editing and formatting. Opinions expressed are not necessarily of those named, and any shortcomings are the author's own.

"reasonable measures" or equivalent standard is the subject matter of this article. A Reasonable [Cybersecurity] Measures Framework is developed to assist judges and juries in determining reasonableness of cybersecurity measures, practitioners and organizations when considering such measures, legal scholars, and faculty teaching trade secrets. This is especially crucial as technical aspects of cybersecurity have important nuances that, it is argued, may make a considerable difference when applying them to a legal analysis of "reasonable." At the same time, failing to consider key technical angles may result in a flawed analysis or interpretation of this requirement. While drawing on lessons from marketing, it is anticipated that much of this discussion will apply to any digital trade secret.

I. INTRODUCTION

The loss of trade secrets in marketing, such as algorithms, product plans, innovations, and formulas, often the source of competitive advantage, can have disastrous impacts on brands and companies. In a digital age, trade secrets may be kept in digital formats, referred to as digital trade secrets, and bad actors have an insatiable appetite to access and profit from such secrets. However, it is not only the bad actors who might compromise the trade secret; there are also other actors and factors to consider. Federal U.S. trade secret law, under the 2016 Defend Trade Secrets Act (DTSA), makes clear that "reasonable measures" must be taken to maintain the secrecy of a trade secret. The Uniform Trade Secrets Act (UTSA) requires "reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret." However, in a digital environment, defining "reasonable" is challenging in comparison with offline settings because of the ever-evolving nature of cybersecurity. This creates a lack of certainty, and ample confusion may result, including wide differences in interpretation.

Cybersecurity, therefore, plays an ever-increasing role, even if it is not the only type of measure that may be required to protect a trade secret. The specific cybersecurity measures that will meet the "reasonable measures" or equivalent standard is the subject matter of this article. A *Reasonable [Cybersecurity] Measures Framework* is developed for various stakeholders. First, it is envisioned to assist courts in determining reasonableness of cybersecurity measures, including when interacting with expert witnesses. This is especially important as technical aspects of cybersecurity make a considerable difference when applying them to a legal analysis of "reasonable." At the same time, failing to consider key technical angles may result in a flawed analysis or interpretation of this requirement. Second, courts may use the framework to instruct juries. In the case of a jury, as recommended by Menell et al., jury instructions should include the "meaning of 'reasonable measures' to protect information."[1] However, as they also recognize, there are few sources to use as guidance to instruct juries, and they propose some very helpful model jury instructions.[2] To further assist judges in providing the meaning of such requirement to juries, it is helpful to consider the proposed framework in this article. This is especially helpful as "jurors cannot be expected to understand the specific information security risk environment of most businesses and what options might be available to reduce risk."[3] Third, it may be informative to

---

[1] PETER S. MENELL ET AL., TRADE SECRET CASE MANAGEMENT JUDICIAL GUIDE 10-
14 (2023), available at https://www.fjc.gov/sites/default/files/materials/08/Trade%20Secret%20final.pdf [https://perma.cc/G6MM-AZDT].
[2] *Id.*
[3] *Id.* at 8-4.

legal practitioners of trade secrets when considering cybersecurity measures as part of the "reasonable measures" requirement, either in litigation or to advise clients about the measures they intend to take or are taking. Fourth, it may be used by businesses and organizations to help assess what may be reasonable cybersecurity measures for their digital trade secrets in particular situations. Fifth, it may be used by legal scholars researching this area to consider various technical elements that play a role in cybersecurity for trade secrets. Sixth, faculty teaching trade secrets courses, or related courses with trade secret topics may find this article and the proposed framework a useful teaching tool. In this way, this article and the proposed framework attempt to remedy the gap of knowledge between technical cybersecurity measures and the requirement of "reasonable measures" for various stakeholders in the trade secret process.

It has been recognized that "[t]he biggest challenge for trade secret protection is maintaining secrecy."[4] Cundiff, in 2009, recognized that trade secret owners must realize the "new circumstances"[5] in which trade secrets in digital environments exist, and the "increased availability of digital tools to remove them"[6] must be taken into consideration if they are to meet the "reasonable measures" standard.[7] Likewise, Rowe, in 2009, recognized that "[t]he digital world complicates this problem and indeed vastly increases the likelihood of destroying the trade secret status of

[4] Elizabeth A. Rowe, *The Challenge of Protecting Trade Secret Information in a Digital World*, *in* INTELLECTUAL PROPERTY PROTECTION OF FACT-BASED WORKS: COPYRIGHT AND ITS ALTERNATIVES 269, 270 (Robert F. Brauneis ed., 2009).
[5] Victoria A. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, 49 IDEA 359, 359 (2009).
[6] *Id.*
[7] *Id.*

misappropriated information.”[8] In fact, “modern technological . . . methods allow . . . information to be easily accessed, reproduced, and disseminated.”[9] Rowe, in 2016, recognized that “[m]any companies do not invest sufficiently in cybersecurity and protecting their trade secret information” and that “to the extent that a company’s network may be interconnected with others, vulnerability can be shared ”[10]

Fast forward to the present, and these challenges not only remain, but the proliferation of technology and breaches alike have made the playing field even more complicated, requiring continuous analysis into how that standard might be interpreted or met. This is further complicated by the fact that there are a multitude of methods for keeping or storing digital trade secrets, such as in the cloud, on private servers, and on external storage devices. Additionally, trade secrets may be properly or improperly disseminated through text messages, emails, file transfers, the cloud, numerous cloud services, and inputting into generative artificial intelligence (GenAI) systems or services.[11] Thus, as technology evolves and changes, as marketers and organizations increasingly rely on digital means to maintain and use trade secrets, as we inch closer to

---

[8] Rowe, *supra* note 4.
[9] *Id.*
[10] Elizabeth A. Rowe, *RATs, TRAPs, and Trade Secrets*, 57 B.C. L. REV. 381, 413 (2016).
[11] R. Mark Halligan, *Trade Secrets 2.0*, ASIS INT’L (Feb. 1, 2017), https://www.asisonline.org/security-management-magazine/articles/2017/02/trade-secrets-2.0/ [https://perma.cc/4LCP-Y7UY]; Nicholas Gowen, *Protecting Trade Secrets in the Cloud,* NAT’L L. REV. (Oct. 20, 2014), https://natlawreview.com/article/protecting-trade-secrets-cloud [https://perma.cc/XG8T-RXZH]; *Generative AI Navigating Intellectual Property*, WIPO (Feb. 28, 2024), https://www.wipo.int/export/sites/www/about-ip/en/frontier_technologies/pdf/generative-ai-factsheet.pdf [https://perma.cc/RP75-2MWM].

a decade of the DTSA (in 2026), and as the demand for cybersecurity skills grows unprecedentedly within organizations,[12] what constitutes "reasonable measures" naturally evolves.[13] However, organizations seek legal certainty, which challenges these notions.

In Part II, this article discusses the increasing importance of digital trade secrets in marketing. Part III discusses the "reasonable measures" or the equivalent requirement. Part IV covers the role of cybersecurity in meeting such "reasonable measures" requirements. Part V proposes the *Reasonable [Cybersecurity] Measures Framework* to better assess "reasonable measures," including the three factors to review when conducting a reasonable risk assessment prior to determining which of the various specific cybersecurity measures are envisioned to meet the said requirement. Finally, Part VI concludes the article.

II. THE INCREASING IMPORTANCE OF DIGITAL TRADE SECRETS IN MARKETING

A trade secret, means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether and how stored, compiled, or memorialized

[12] World Economic Forum, *Bridging the Cyber Skills Gap*, https://initiatives.weforum.org/bridging-the-cyber-skills-gap/home [https://perma.cc/CU7B-TG7W].
[13] *See* David G. Majdali, *Trade Secrets Versus the Internet: Can Trade Secret Protection Survive in the Internet Age?*, 22 WHITTIER L. REV. 125, 144, 155–56 (2000).

physically, electronically, graphically, photographically, or in writing ."[14]

In marketing, digital trade secrets may include some types of digital objects,[15] client lists, algorithms,[16] product plans, marketing plans and strategies,[17] marketing processes, code,[18] pricing strategies, marketing innovation,[19] formulas, marketing "know-how,"[20] and much more, all kept in a digital format.

Competitive advantage[21] is often a key consideration for digital trade secrets in marketing. This is the case when organizations choose to maintain certain eligible protectable

---

[14] 18 U.S.C. § 1839(3).
[15] *WIPO Guide to Trade Secrets and Innovation Part VII: Trade Secrets and Digital Objects*, WIPO, https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/part-vii-trade-secrets-and-digital-objects.html [https://perma.cc/2JTK-ZT96].
[16] *Id.*
[17] *Intellectual Property Toolkit – Trade Secrets*, USPTO, https://www.uspto.gov/sites/default/files/documents/tradesecretsiptoolkit.pdf [https://perma.cc/P7C2-NAWZ].
[18] *Trade Secrets and Digital Objects*, *supra* note 15.
[19] Nicola Searle, *The Economic and Innovation Impacts of Trade Secrets*, U.K. INTELL. PROP. OFF. (Apr. 19, 2021), https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets/the-economic-and-innovation-impacts-of-trade-secrets#economic-construction [https://perma.cc/92JR-VFBU].
[20] *Trade Secrets*, DMLP (Sept. 9, 2024), https://www.dmlp.org/legal-guide/trade-secrets [https://perma.cc/RM26-ZYED].
[21] Oleksandra Ozcan et al., *A Trade Secrets Framework and Strategic Approaches*, 71 IEEE TRANSACTIONS ON ENG'G MGMT. 10200, 10202 (2024);
Eur. Innovation Council & SMEs Exec. Agency, *Trade Secrets as a Competitive Advantage in the Internationalisation Process*, EUR. COMM'N (July 31, 2024), https://intellectual-property-helpdesk.ec.europa.eu/document/download/39e2ba33-499a-4cf2-9df1-e04ad0430359_en?filename=10%20Infographic%20Trade%20secrets%20as%20competitive%20advantage%20when%20internationalising.pdf [https://perma.cc/5J3M-26ZD].

information as a trade secret "by avoiding the disclosure" required by other intellectual property forms.[22]

A digitally held client list within a customer relationship management (CRM) platform, if qualified as a trade secret, may also include customer preferences, behaviors, and actions taken. This could be the source of great marketing efforts to reach consumers with offerings that are relevant, interesting, and more likely to result in purchases based on the information contained in the CRM, which is tied to specific customers.

Also, algorithms are increasingly relevant in marketing, and major technology companies, such as Google, have historical beginnings in algorithms like its "search algorithm *PageRank*."[23] Algorithms are also used in marketing, such as to "generate predictions for marketing decisions, such as which consumers to target with which offers,"[24] including helping "make marketing more intelligent, efficient, consumer-friendly, and, ultimately, more effective."[25] While some algorithms may be protected under other forms of intellectual property, certain algorithms can be kept a secret and protected as trade secrets.

Certain plans and documented strategies may also be trade secrets. Marketing plans,[26] product plans, pricing plans and strategies, and others may qualify as trade secrets

---

[22] Searle, *supra* note 19.
[23] LUC DESAUNETTES-BARBERO, TRADE SECRETS LEGAL PROTECTION: FROM A COMPARATIVE ANALYSIS OF US AND EU LAW TO A NEW MODEL OF UNDERSTANDING 3 (Josef Drexl et al. eds., 2023).
[24] Dennis Herhausen et al., *Machine Learning in Marketing: Recent Progress and Future Research Directions*, 170 J. OF BUS. RSCH. 114254, 114254 (2024).
[25] *Id.*
[26] *Trade Secrets*, *supra* note 17.

under certain circumstances and may be significant sources of competitive advantage.[27]

In today's digital environment, many trade secrets are often kept in digital formats, such as the cloud, due to the many benefits this provides, including "efficiency,"[28] "accessibility,"[29] "scalability,"[30] "security,"[31] and "transmission."[32] Many services used by organizations and marketers are also digitally available and administered through the cloud, such as CRMs, digital marketing systems, storage services, and many others.[33] Trade secrets may also be kept on servers within an organization, tied to or separate from organizational computer networks.[34] Trade secrets may also be kept on individual user-level computers or laptops, be backed up onto organizational computing resources, and be stored on external storage devices such as a Universal Serial Bus (USB) drive[35] or external hard

---

[27] Ozcan et al., *supra* note 21; Eur. Innovation Council & SMEs Exec. Agency, *supra* note 21.

[28] *Trade Secrets and Digital Objects*, *supra* note 15.

[29] *The Benefits of Cloud Storage*, ORACLE (June 17, 2022), https://www.oracle.com/cloud/storage/what-is-cloud-storage/benefits/ [https://perma.cc/W5R2-3S9G].

[30] *Id.*

[31] *Id.*

[32] *Trade Secrets and Digital Objects*, *supra* note 15.

[33] *Gartner Says Cloud Will Become a Business Necessity by 2028*, GARTNER (Nov. 29, 2023), https://www.gartner.com/en/newsroom/press-releases/2023-11-29-gartner-says-cloud-will-become-a-business-necessity-by-2028 [https://perma.cc/KXV2-LGEF].

[34] Amy Candido et al., *Trade Secrets: How to Protect These Increasingly Important Assets,* WILSON SONSINI (Mar. 21, 2024), https://www.acc.com/sites/default/files/program-materials/upload/WILSON%20ACC%20Bay%20SFBA%20Life%20Sciences%20Conference%20Protecting%20Trade%20Secrets%20March2024_FINAL2.pdf [https://perma.cc/FM9E-8VK6].

[35] Also known as a flash, jump, thumb drive, etc.

drives.[36] The practical benefits of each of these digital formats have resulted in an increased use of these methods; however, they also raise various security issues.

III. TRADE SECRET REQUIREMENT OF REASONABLE MEASURES OR EQUIVALENT: WHAT IS REASONABLE ANYWAY?

Under the DTSA, a trade secret is conditioned on the requirement that the trade secret be kept a secret. Specifically, this means that:

> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.[37]

The focus of this article is on the phrase "reasonable measures" under 18 U.S.C. § 1839(3)(A). However, even though "U.S. trade secret law has seen several statutory initiatives, the precise meaning and definitional parameters of the trade secret concept remain elusive."[38] The DTSA

---

[36] *Portable Storage Device*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/portable_storage_device [https://perma.cc/KF7H-HW9S].
[37] 18 U.S.C. § 1839(3).
[38] Suzana Nashkova, *Defining Trade Secrets in the United States: Past and Present Challenges–A Way Forward?*, 54 IIC 634, 636 (Mar. 28, 2023) https://link.springer.com/content/pdf/10.1007/s40319-023-01310-1.pdf [https://perma.cc/CZW4-6PH7].

does not define[39] and "gives scant guidance"[40] with respect to what "reasonable measures"[41] means. This is especially challenging in an ever-evolving cybersecurity environment where what this means will necessarily and continuously change. It should be recognized that there is an interstate or foreign commerce requirement to institute a civil proceeding under the DTSA,[42] although trade secrets may otherwise be afforded protection under state or other law.

As Rowe and Sandeen note, "[r]easonableness is a relative term that depends on the particular circumstances."[43] Milgrim states that factors such as the "size and character of the enterprise," "location," and even the "nature and character of the enterprise's staff," may play a role.[44] In the context of non-digital trade secrets, it has always been important to implement reasonable physical measures, such as security guards, cameras, and other measures to protect physical boxes of trade secrets left in an office environment.[45] Cundiff recognizes that "[t]he digital world is no friend to trade secrets," while also recognizing the trackability available with technology and the added security that may be available in digital environments.[46] For digital trade secrets, malicious theft may occur by employees or ex-employees, by outside professional attackers, by competitors, or even by recreational or amusement hackers. Other disclosures may be accidental or innocent. Also,

---

[39] Wwmap, LLC v. Midwifery, 711 F. Supp. 3d 1313, 1321 (N.D. Fla. 2024).

[40] Turret Labs USA, Inc. v. CargoSprint, LLC, No. 21-952, 2022 U.S. App. LEXIS 6070, at *4–5 (2d Cir. Mar. 9, 2022).

[41] 18 U.S.C. § 1839(3).

[42] 18 U.S.C § 1836; 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.01.

[43] ELIZABETH A. ROWE & SHARON K. SANDEEN, TRADE SECRETS LAW: CASES AND MATERIALS 188 (2d ed. 2017).

[44] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.04.

[45] *See* Cundiff, *supra* note 5, at 369.

[46] *Id.* at 361.

various methods, approaches, measures, and levels of cybersecurity may be applied to digital trade secrets in marketing to counter or mitigate the multitude of types of attacks and accidents. This makes the requirement of "reasonable measures" a difficult and evolving concept.

As also recognized by Rowe and Sandeen, "whether or not a company took adequate steps to protect confidential information is often used as evidence of the information holder's subjective belief that the information was a trade secret and thus worthy of legal protection."[47] It is here that an interplay between what the value of the trade secret is and what measures are used to protect it are important. For example, the cost of the measures to protect a trade secret may be related to its value.[48] However, as Hrdy and Lemley correctly note, some "secrecy precautions can be very cheap"[49] and courts should be cautious about whether they use the amount of monies expended to ascertain whether reasonable measures were taken. For example, "nondisclosure agreements or confidentiality stamps . . . are cheap to draft, and yet courts frequently accept them ."[50] Likewise, marking something as *confidential* or *trade secret* may be a low-cost measure. As the District Court of the District of Puerto Rico noted, "simply implemented, minimally expensive security measures . . ." may have "disproportionately large benefits."[51] Thus, reasonable

[47] ROWE & SANDEEN, *supra* note 43.
[48] R. Mark Halligan, *Reasonable Measures to Protect Trade Secrets*, REUTERS (Oct. 10, 2022), https://www.reuters.com/legal/legalindustry/reasonable-measures-protect-trade-secrets-2022-10-10/ [https://perma.cc/765R-Q4ZU].
[49] Camilla A. Hrdy & Mark A. Lemley, *Abandoning Trade Secrets*, 73 STAN. L. REV. 1, 34 (2021).
[50] *Id.*
[51] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.04; TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo, No. 15-2121 (BJM), 2018 U.S. Dist. LEXIS 168546, at *51 (D.P.R. Sept. 28, 2018).

measures may certainly be impacted by the value of the trade secret; however, the amount of money spent on it may not always be dispositive.

Further, beyond the DTSA, there are other potential ways to protect trade secrets under other laws, such as state or foreign laws. While this article focuses on the cybersecurity aspect of the "reasonable measures" requirement under the DTSA, it also references relevant state-specific case law under the particular state version of the UTSA. Further, it is anticipated that much of the discussion and the framework presented can also substantially apply to most state matters. In fact, federal courts may even "rely on the decisional trade secret law of the state in which they sit to construe the DTSA."[52] However, some states may notably differ, as Menell et al. note.[53] For example, Nevada law incorporates a presumption that if the words "Confidential" or "Private," or other similar "indication of secrecy" are used in "a reasonably noticeable manner," then "reasonable effort" will be presumed rebuttable by "clear and convincing evidence" otherwise, of not having taken "reasonable efforts."[54] Nevertheless, "substantive elements of many state law trade secret claims closely track the DTSA requirements."[55]

A brief review of state and foreign requirements is helpful for putting the DTSA in context. Section 4(2) of the Uniform Trade Secrets Act (UTSA), dating well before the DTSA, states that a trade secret:

"is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[56]

---

[52] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.01.
[53] PETER S. MENELL ET AL., *supra* note 1, at 3-15.
[54] Nev. Rev. Stat. § 600A.032.
[55] PETER S. MENELL ET AL., *supra* note 1, at 3-15.
[56] Uniform Trade Secrets Act § 4(2) (amended 1985).

Likewise, Article 39(2)(c) of the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement states that a trade secret:

"has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."[57]

The European approach uses slightly different language. Under Article 2(1)(c) of the EU Trade Secrets Directive states:

"it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."[58]

The UK, under Section 2 of the Trade Secrets (Enforcement, etc.) Regulations 2018, uses language similar to that in the EU Trade Secrets Directive, as the Directive was implemented in the UK prior to Brexit and has continued in force thereafter.[59] Given that the EU Trade Secrets Directive[60] was adopted in 2016,[61] the UK Regulation came into force in 2018,[62] and the DTSA was enacted in 2016,[63] all of these will continue to be subject to interpretation over time, as they cover angles of

---

[57] Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 33 I.L.M. 81, 98 (1994).
[58] Directive 2016/943, of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, 2016 O.J. (L 157) 1, 9 [hereinafter Directive 2016/943].
[59] *See* The Trade Secrets (Enforcement, etc.) Regulations 2018, No. 597 (U.K.).
[60] Directive 2016/943, *supra* note 58.
[61] *Id.*
[62] The Trade Secrets (Enforcement, etc.) Regulations 2018.
[63] 18 U.S.C. § 1836.

technological purview such as those related to cybersecurity measures.

As noted by Milgrim, various terminology may be used to describe the requirement, including "reasonable efforts," "reasonable precautions," "reasonable measures," "reasonable safeguards," or "precautions reasonable under the circumstances."[64]

While the UTSA, TRIPS, and the stated foreign requirements all use the terminology of "the circumstances,"[65] it appears that such circumstances will generally be considered on a case-by-case basis under the DTSA without having to incorporate that specific language.[66] Importantly, there are "near infinite" techniques available to protect trade secrets and the "environment and circumstances in which the trade secret is maintained" is most relevant.[67]

IV. THE ROLE OF CYBERSECURITY IN "REASONABLE MEASURES" OR EQUIVALENT

Cybersecurity is not a static concept. It is important to understand that as technology evolves, cybersecurity must evolve, creating ongoing novel challenges. This evolving nature, along with the harmonious yet confused relationship

---

[64] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.01.
[65] TRIPs (1994); Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, art. 39(2)(c), 1869 U.N.T.S. 299; Uniform Trade Secrets Act § 4(2); Directive 2016/943; The Trade Secrets (Enforcement, etc.) Regulations 2018.
[66] *See* James Pooley, *Addressing the "Reasonable Efforts" Requirement through Expert Testimony*, *in* ADVANCED TRADE SECRETS 2022: NEW RISKS, NEW CHALLENGES, NEW IDEAS § 3 (Practising Law Institute, 2022).
[67] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.04; Cundiff, *supra* note 5, at 369.

between trade secrets and cybersecurity, will now be discussed.

A. Evolving Nature of Cybersecurity

"Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."[68] Such "confidentiality, integrity, and availability of information"[69] are known in the cybersecurity industry as the "CIA triad"[70] and may be "extended with the AAA triad,"[71] which represents "[a]uthorization, [a]uthentication and [a]uditing."[72] It is important to define these terms to put cybersecurity into context.

Confidentiality is concerned with "unauthorized disclosure"[73] to protect proprietary information[74] and trade secrets. Integrity protects against "improper information modification,"[75] such as stored trade secrets. Availability is concerned with ensuring technical resources are available when needed,[76] such as the technical systems on which digital trade secrets are stored. Authorization involves

---

68 *What is Cybersecurity?,* CYBERSEC. & INFRASTRUCTURE SEC. AGENCY (Feb. 1, 2021), https://www.cisa.gov/news-events/news/what-cybersecurity [https://perma.cc/FWV3-ZVYW].
69 *Id.*
70 Jennifer Cawthra et al., *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*, NAT'L INST. OF STANDARDS AND TECH. (Dec. 2020), https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html [https://perma.cc/W5L6-YTQN].
71 *Security Fundamentals*, OWASP, https://owasp.org/www-project-developer-guide/draft/foundations/security_fundamentals/# [https://perma.cc/R22Z-FWMF].
72 *Id.*
73 *Id.*
74 Cawthra et al., *supra* note 70.
75 *Id.*
76 *Security Fundamentals, supra* note 71.

"access rights to secure resources,"[77] such as the authority to sign into systems on which trade secrets are stored or can be used. Authentication is "confirming the identity of the entity that wants to interact with a secure system,"[78] such as before systems containing trade secrets are accessed by specific users. Auditing is tracking what is happening within secure systems,[79] such as to document and trace activity within a system on which trade secrets are stored. Cybersecurity involves the interplay between all of these key concepts, which are important to consider under the DTSA, rather than viewing cybersecurity from a generalized perspective.

While many cybersecurity measures will be technical, not all are. For example, physical measures[80] relevant to cybersecurity are also important and go hand in hand with the technical measures. Furthermore, organizational measures may be relevant to implement.[81] However, this article focuses primarily on key cybersecurity measures, even if briefly discussing related ones.

What is involved in cybersecurity will constantly change as technological innovation evolves. While early cybersecurity involved viruses and, later, cybercrimes,[82] these concerns remain today, along with more recent concerns about cloud security,[83] "quantum computing,"[84] and the security of generative AI.[85] As digital trade secrets

---

77 *Id.*
78 *Id.*
79 *Id.*
80 *Trade Secrets*, *supra* note 17.
81 *See* Pamela Passman, *Eight Steps to Secure Trade Secrets*, WIPO MAG. (Feb. 2016), https://www.wipo.int/wipo_magazine/en/2016/01/article_0006.html [https://perma.cc/8DLQ-B8AT].
82 *The History of Cybersecurity*, MARYVILLE UNIV. (July 24, 2024), https://online.maryville.edu/blog/history-of-cybersecurity/ [https://perma.cc/SN75-29V6].
83 *Id.*
84 *Id.*
85 *Id.*

in marketing interact with these evolving technologies and platforms, what cybersecurity encompasses needs to be constantly reconsidered.

B. The Harmonious Yet Confused Relationship Between Trade Secret Law and Cybersecurity

There appears to be a harmonious yet confused relationship between trade secret law and cybersecurity. While it appears straightforward that cybersecurity should be used to protect digital trade secrets, there are many technical factors involved that could create confusion or may not be adequately considered in a legal analysis.

This is further complicated by the fact that there are many actors in the cybersecurity threat environment including legitimate organizational users, such as authorized employees, third parties accessing trade secrets from remote locations, service providers (and their employees) hosting cloud-based software where trade secrets are stored, as well as malicious attackers seeking financial gain, amusement, and/or self-fulfillment among many others.[86] Beyond actors, there are also many factors that are implicated with digital trade secrets in marketing. Technical cybersecurity know-how and the implementation of secure methods and strategies to protect digital trade secrets can vary widely, in part due to the "cybersecurity workforce shortage,"[87] among many other reasons. A lack of knowledge or inadequate resources dedicated to cybersecurity can result in

[86] *What are the Types of Cyber Threat Actors?*, SOPHOS, https://www.sophos.com/en-us/cybersecurity-explained/threat-actors [https://perma.cc/N438-6JWN].
[87] Vanessa Lyon et al., *Cybersecurity Has a Talent Shortage. Here's How to Close the Gap*, BOS. CONSULTING GRP. (Oct. 2, 2024), https://www.bcg.com/publications/2024/cybersecurity-talent-shortage-close-the-gap [https://perma.cc/L4L2-TKEQ].

insufficient measures. The level of protection for a trade secret can be based on the value the trade secret holder places on it, or a lack of resources (including time and money) may lead to a reduced ability to protect trade secrets adequately. In some cases, carelessness, lack of knowledge, or simple disregard may be the cause of inadequate measures being employed. Of course, all of this assumes that the organization or trade secret holder understands that what they hold and protect is a trade secret that requires reasonable measures.

What is certain in the context of digital trade secrets in marketing is that one key aspect of reasonable measures is employing cybersecurity measures. Although it is recognized that cybersecurity is not the only consideration in taking such measures, it is a "key component of protection"[88] if not the most prominent, and it may be the single most difficult one to interpret in the context of such required measures. For example, employing confidentiality agreements, non-disclosure agreements (NDAs), etc., are often considered an essential part of a reasonable measure analysis. These topics are beyond the scope of this analysis and are well documented in the literature.[89] However, cybersecurity, when used to determine or partly determine whether reasonable measures have been taken, may be the most controversial and the most open to interpretation due to the ever-evolving technical nature of such measures, as well as the risks and threats that make these measures important.

---

[88] Atin Basuchoudhary & Nicola Searle, *Snatched Secrets: Cybercrime and Trade Secrets Modelling a Firm's Decision to Report a Theft of Trade Secrets*, ELSEVIER (Aug. 8, 2019), https://www.sciencedirect.com/science/article/pii/S0167404819300616 [https://perma.cc/R3L8-ZNRP].

[89] *See* Julianne M. Hartzell, *Trade Secrets, Professional Perspective - Non-Disclosure Agreements and Trade Secrets Protection*, BLOOMBERG L. (Mar. 2020), https://www.bloomberglaw.com/external/document/XC859CCS000000/trade-secrets-professional-perspective-non-disclosure-agreements [https://perma.cc/8297-EB4M].

In fact, while certain measures may be reasonable at one "point in time," they may not be at "another time," and a modification of the cybersecurity measures taken may be necessary to meet the reasonableness requirement on an ongoing basis.[90]

V. TOWARDS A FRAMEWORK TO BETTER ASSESS REASONABLE [CYBERSECURITY] MEASURES OR EQUIVALENT

A. Cybersecurity Measures Envisioned to Help Meet "Reasonable Measures" or Equivalent for Digital Trade Secrets in Marketing

A key consideration is that courts generally refer to measures in broad terms. For example, references to a firewall in the general sense may be made; however, as will be further described below, firewalls can vary in type, quality, and the levels of security they provide.[91] Likewise, when storing something in the cloud, due consideration might be had to the various cloud "service models,"[92] "types of cloud architecture,"[93] and the level of protection provided for each.[94] While these may or may not have been the

[90] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.04
[91] *What is a Firewall? - Definition & Explanation*, AO KAPERSKY LAB, https://usa.kaspersky.com/resource-center/definitions/firewall [https://perma.cc/4FWE-YHJR]; *What is a Firewall?*, CISCO SYS., https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html [https://perma.cc/R9D7-37EN].
[92] *What is Cloud Architecture?*, GOOGLE CLOUD, https://cloud.google.com/learn/what-is-cloud-architecture [https://perma.cc/E7GP-V3ZJ].
[93] *Id.*
[94] *See* Raj Sachdev, Legal Issues in Cloud Security and Privacy (2019) (Master's dissertation, Univ. of Oxford) (on file with author); PREETI MISHRA ET AL., CLOUD SECURITY: ATTACKS, TECHNIQUES, TOOLS, AND CHALLENGES 29 (CRC Press 2022).

subject of deep examination, courts may not delve into the technical details of the measures, or they may oversimplify the issue. Juries may not be knowledgeable of specific technical cybersecurity measures and their relation to the reasonableness measure.[95]

The reasonableness of measures taken will likely be a "fact intensive" inquiry by the courts.[96] However, "efforts to maintain secrecy need not be overly extravagant, and absolute secrecy is not required."[97] In the context of trade secrets in a platform, the required secrecy "need not be absolute."[98] In other words, trade secret owners are "not required to employ all possible measures to preserve secrecy"[99] and reasonable measures may still be found "even if they are imperfect or they ultimately fail to thwart misappropriation."[100] This was seen in *Wwmap, LLC v. Midwifery*, which concerned "a list of the costs of administering medical tests; a list of medical professionals who referred patients to Plaintiff; [and] a customer list . . .,"[101] which could be used to compete, and financial information which could be used by competitors to set prices.[102] In fact, only "sufficient secrecy" is required, and this was interpreted by one court as "except by use of improper means, there would be difficulty in acquiring the

---

95 PETER S. MENELL ET AL., *supra* note 1, at 8-4.
96 Synopsys, Inc. v. Risk Based Sec., Inc., No. 3:21cv252, 2022 U.S. Dist. LEXIS 134694, at *32 (E.D. Va. July 28, 2022); 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.01.
97 AvidAir Helicopter Supply, Inc. v. Rolls-Royce Corp., 663 F.3d 966, 974 (8th Cir. 2011).
98 ResMan, LLC v. Karya Prop. Mgmt., LLC, No. 4:19-CV-00402, 2021 U.S. Dist. LEXIS 145462, at *14–15 (E.D. Tex. Aug. 4, 2021).
99 Wwmap, LLC v. Midwifery, 711 F. Supp. 3d 1313, 1321 (N.D. Fla. 2024).
100 *Id.*
101 *Id.* at 1320.
102 *Id.*

information."[103] Under state law, the Colorado UTSA does not require "extreme measures,"[104] the Kansas UTSA does not require "all conceivable efforts,"[105] and the Maryland UTSA (and the DTSA) do not require "the best security measures available"[106] to meet the requisite standard. Overall, this will be a "highly contextual"[107] assessment based on individual circumstances. As Milgrim notes, "it is not inconsistent for a trade secret owner to allege both that it used reasonable efforts under the circumstances to protect the secrecy of its secrets and that defendant successfully misappropriated the secrets."[108] Nevertheless, some common elements are seen in some of the case law.

There is no "exhaustive catalogue"[109] of reasonable measures, and a single measure is often insufficient. Further, there is "no bright-line test to determine what amount or types of safeguards are reasonable to protect the secrecy of proprietary information."[110] Courts, as will be seen below, have often considered a combination of measures to conclude that they were reasonable under the DTSA. At the same time, litigants will attempt to describe how they go beyond the reasonable measures, although not all instances of what they describe will actually be required to meet the standard. As such, parties and their representatives should

---

[103] Houser v. Feldman, 569 F. Supp. 3d 216, 229–30 (E.D. Pa. 2021).
[104] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.04; *see* L-3 Communs. Corp. v. Jaxon Eng'g & Maint., Inc., No. 10-cv-02868-MSK-KMT, 2013 U.S. Dist. LEXIS 139219, at *13 (D. Colo. Sept. 27, 2013).
[105] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.04; *see* All W. Pet Supply Co. v. Hill's Pet Prods. Div., 840 F. Supp. 1433, 1438 (D. Kan. 1993).
[106] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.04; *see* Brightview Grp., LP v. Teeters, 441 F. Supp. 3d 115, 131 (D. Md. 2020).
[107] Pooley, *supra* note 66.
[108] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.01.
[109] MAGDALENA KOLASA, TRADE SECRETS AND EMPLOYEE MOBILITY: IN SEARCH OF AN EQUILIBRIUM 66 (Cambridge Univ. Press 2018).
[110] PETER S. MENELL ET AL., *supra* note 1, at 2-13.

be careful to not assume that all measures accepted by a court may be minimally required. They will often employ expert witnesses to attempt to prove that the measures taken were reasonable.[111] The nature of the measures taken will also depend on a careful balance between "'foreseeability' of misappropriation"[112] and the "cost of effective precautions"[113] that are employed. In fact, this "requires an assessment of the security risks for that information in the business, and the burden of mitigation techniques measured against the value of the information as a secret."[114]

It should be noted that there are key difficulties in ascertaining the meaning of "reasonable measures" under the DTSA, both from legal and technical perspectives. From the legal perspective, as aptly recognized, "given that most [trade secret cases] are decided on summary judgment,"[115] it is difficult to ascertain a specific standard. At such a stage, there may be facts in dispute which may properly be within the area of juries to decide, although the plaintiff will still have to meet the requirement to sufficiently plead their case.[116] Therefore, it is important to consider the available details in such cases which have been included in the discussion below. Further, while the DTSA is a federal law and should, at least theoretically, lead to "national uniformity,"[117] this is not always the case, especially when circuits disagree on the same point.[118] Additionally, while most cases discussed in this article are from the federal

---

[111] Pooley, *supra* note 66.
[112] *Id.*
[113] *Id.*
[114] PETER S. MENELL ET AL., *supra* note 1, at 2-13.
[115] Pooley, *supra* note 66.
[116] PETER S. MENELL ET AL., *supra* note 1, at 7-6.
[117] Christopher T. Zirpoli, *An Introduction to Trade Secrets Law in the United States*, CONG. RSCH. SERV. (Jan. 27, 2023), https://www.everycrsreport.com/reports/IF12315.html [https://perma.cc/JS62-47WH].
[118] *Id.*

courts, claims under the DTSA may, in some cases, be heard in state courts, since the federal courts have "original but not exclusive jurisdiction ."[119]

From the technical perspective, it is important to understand that there are technical differences, nuances, and approaches that must be considered to determine whether a particular measure or set of measures is reasonable. This can vary greatly in different cases, depending on a number of factors, including but not limited to the type of organization, the nature of the trade secrets, the method of maintaining the secrecy, and various other factors.[120] It is not enough to simply say that a trade secret is password-protected or that encryption was used. There are a number of considerations for each of these measures that render poor implementation,[121] primitive or insecure forms of them arguably below the standard of reasonable measures, as will be explained below.

It is proposed that courts and the parties use a framework to better assess reasonable measures in the context of cybersecurity. This will help avoid painting such measures with a broad brush and provide a basis on which to assess this key prong of trade secrets.

---

[119] David S. Levine & Christopher B. Seaman, *The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act*, 53 WAKE FOREST L. REV. 106, 119 (2018); 18 U.S.C. § 1836(c) ("The district courts of the United States shall have original jurisdiction of civil actions brought under this section."); Restaurant Zone LLC v. Myers, No. 45, slip op. (N.Y. Sup. Ct. Aug. 4, 2023) ("Since Congress has not reserved jurisdiction over Defend Trade Secrets Act claims to exclusively federal district courts, this court has concurrent jurisdiction over such claims.").

[120] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.04.

[121] PETER S. MENELL ET AL., *supra* note 1, at 2-16.

B. Proposed Framework

The following *Reasonable [Cybersecurity] Measures Framework* begins with key initial considerations that courts, it is proposed, should evaluate before delving into specific cybersecurity measures and determining whether they collectively constitute reasonable measures. This framework will help courts better assess reasonable measures by first addressing these initial considerations and then providing guiding questions and considerations related to various cybersecurity measures.

Prior to introducing the framework, it is important to note its relevance to the process of litigation. In most cases, at the pleadings stage or in response to a motion to dismiss or a motion for summary judgment, the standards will differ from those expected at trial. As seen from the cases discussed in this article, the courts, when deciding on such motions, have commonly accepted general allegations of reasonable measures without delving into specific technical details. Therefore, generic statements about reasonable cybersecurity measures might be sufficient to withstand a motion. However, if deemed strategic by counsel, it may be prudent for digital trade secret holders to plead with specificity, such as by detailing strong password methods, specific types of encryption, digital markings, cybersecurity training, cloud service responsibilities, the level of security employed, and other cybersecurity measures, while utilizing court procedures to maintain the confidentiality of such measures when needed.[122] Opposing counsel may consider challenging the pled measures as, for example, insufficient or not rising to the relevant standard for purposes of the motion.[123] In the case of either a motion or trial, it is

---

[122] PETER S. MENELL ET AL., *supra* note 1, at 2-16.

[123] Smietana, et al. v. Stephens, et al., No. 22-708, 2024 WL 965178 (N.D. Ill. Mar. 5, 2024); John Baranello et. al, *In Case You Missed It: Federal Court Dismisses Cryptocurrency DTSA Claim Finding*

submitted that the courts should determine the reasonableness of the measures taken based on an analysis of the framework presented below. Even if the standards differ, the overall considerations are expected to remain the same. Within the litigation process, the role of experts is also an important consideration. For example, parties may employ experts to help the court determine whether the measures taken were reasonable. As courts hear from the experts, this framework can provide the court and the parties with guiding considerations to help assess allegations and evidence and better understand the cybersecurity-related considerations at play. Absent expert witnesses, the framework can be used as a guiding document to assess reasonable measures under consideration.

The framework presented in Figure 1 proposes three key initial considerations that a court should understand to set the stage for evaluating measures taken with respect to digital trade secrets while conducting a reasonable risk assessment. It then recommends considering specific cybersecurity measures in line with the discussion in the sections that follow. Cybersecurity standards, best practices, and other related considerations should be applied where relevant. The subsections following the framework below provide an in-depth explanation of the framework.

Plaintiffs Failed to Plead Reasonable Measures Requirement, MOSES & SINGER LLP (Mar. 6, 2024), https://www.mosessinger.com/publications/in-case-you-missed-it-federal-court-dismisses-cryptocurrency-dtsa-claim-finding-plaintiffs-failed-to-plead-reasonable-measures-requirement [https://perma.cc/TS38-UCA7].

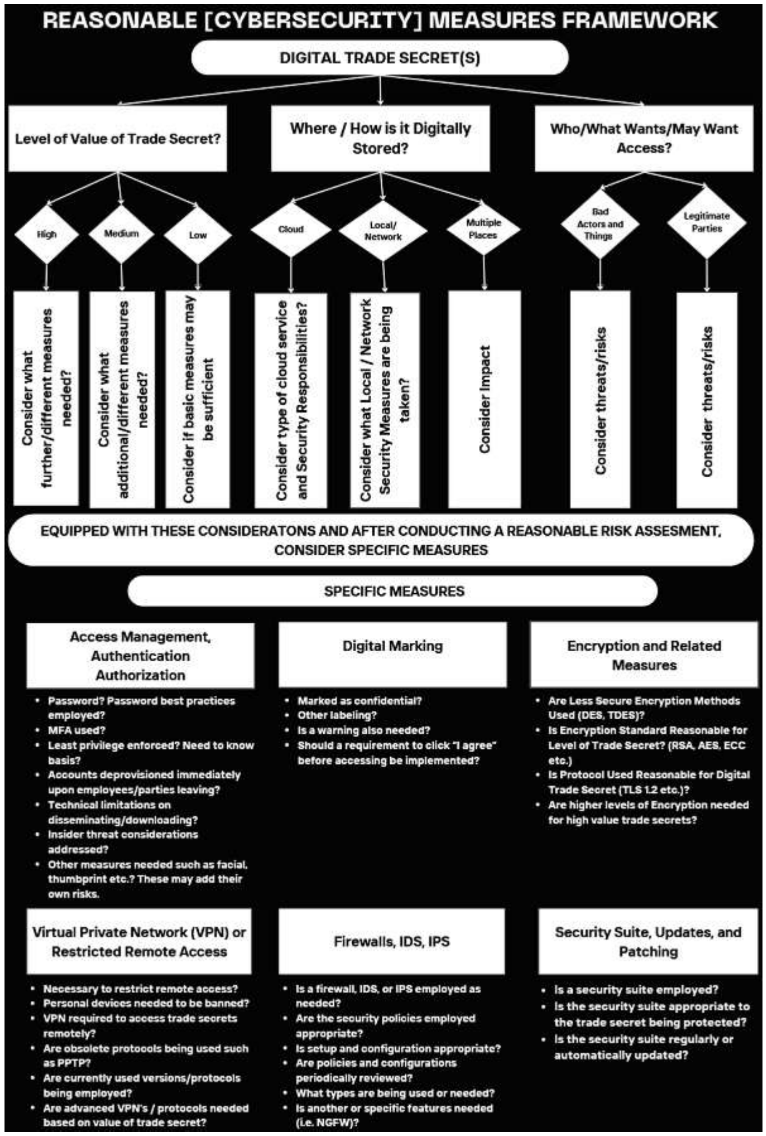
REASONABLE [CYBERSECURITY] MEASURES FRAMEWORK
DIGITAL TRADE SECRET(S)
Level of Value of Trade Secret?
Where / How is it Digitally Stored?
Who/What Wants/May Want Access?
High
Medium
Low
Cloud
Local/ Network
Multiple Places
Bad Actors and Things
Legitimate Parties
Consider what further/different measures needed?
Consider what additional/different measures needed?
Consider if basic measures may be sufficient
Consider type of cloud service and Security Responsibilities?
Consider what Local / Network Security Measures are being taken?
Consider Impact
Consider threats/risks
Consider threats/risks
EQUIPPED WITH THESE CONSIDERATONS AND AFTER CONDUCTING A REASONABLE RISK ASSESMENT, CONSIDER SPECIFIC MEASURES
SPECIFIC MEASURES
Access Management, Authentication Authorization
• Password? Password best practices employed?
• MFA used?
• Least privilege enforced? Need to know basis?
• Accounts deprovisioned immediately upon employees/parties leaving?
• Technical limitations on disseminating/downloading?
• Insider threat considerations addressed?
• Other measures needed such as facial, thumbprint etc.? These may add their own risks.
Digital Marking
• Marked as confidential?
• Other labeling?
• Is a warning also needed?
• Should a requirement to click "I agree" before accessing be implemented?
Encryption and Related Measures
• Are Less Secure Encryption Methods Used (DES, TDES)?
• Is Encryption Standard Reasonable for Level of Trade Secret? (RSA, AES, ECC etc.)
• Is Protocol Used Reasonable for Digital Trade Secret (TLS 1.2 etc.)?
• Are higher levels of Encryption needed for high value trade secrets?
Virtual Private Network (VPN) or Restricted Remote Access
• Necessary to restrict remote access?
• Personal devices needed to be banned?
• VPN required to access trade secrets remotely?
• Are obsolete protocols being used such as PPTP?
• Are currently used versions/protocols being employed?
• Are advanced VPN's / protocols needed based on value of trade secret?
Firewalls, IDS, IPS
• Is a firewall, IDS, or IPS employed as needed?
• Are the security policies employed appropriate?
• Is setup and configuration appropriate?
• Are policies and configurations periodically reviewed?
• What types are being used or needed?
• Is another or specific features needed (i.e. NGFW)?
Security Suite, Updates, and Patching
• Is a security suite employed?
• Is the security suite appropriate to the trade secret being protected?
• Is the security suite regularly or automatically updated?

Figure 1. Sachdev's Reasonable [Cybersecurity] Measures Framework[124]

---

[124] Sources: *Access Management*, NATI'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/access_management

[https://perma.cc/G37D-GSK3]; Paul A. Grassi et al., *Digital Identity Guidelines Authentication and Lifecycle Management*, NAT'L INST. OF STANDARDS AND TECH. (June 2017), https://pages.nist.gov/800-63-3/sp800-63b.html [https://perma.cc/4DJ5-9EC3]; *Risks of Default Passwords on the Internet*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY (Oct. 7, 2016), https://www.cisa.gov/news-events/alerts/2013/06/24/risks-default-passwords-internet [https://perma.cc/B78M-CWLA]; *Multi-Factor Authentication*, NAT'L INST. OF STANDARDS AND TECH. (Mar. 12, 2024), https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication [https://perma.cc/D3HZ-CZYB]; *Authorization*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/authorization [https://perma.cc/9XFH-SRW6]; *Least Privilege*, NAT'L INST. OF STANDARDS AND TECH. (last visited Nov. 24, 2024), https://csrc.nist.gov/glossary/term/least_privilege [https://perma.cc/9ZRF-JKEJ]; *WIPO Guide to Trade Secrets and Innovation Part VII: Trade Secrets and Digital Objects*, WIPO, https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/part-vii-trade-secrets-and-digital-objects.html [https://perma.cc/2JTK-ZT96]; Amy Candido et al., *Trade Secrets: How to Protect These Increasingly Important Assets,* WILSON SONSINI (Mar. 21, 2024), https://www.acc.com/sites/default/files/program-materials/upload/WILSON%20ACC%20Bay%20SFBA%20Life%20Sciences%20Conference%20Protecting%20Trade%20Secrets%20March2024_FINAL2.pdf [https://perma.cc/FM9E-8VK6]; *Defining Insider Threats*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats [https://perma.cc/42K5-8FS4]; *Encryption*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/encryption [https://perma.cc/D5YL-GX9X]; *Cryptographic Key*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/cryptographic_key [https://perma.cc/GCB9-H7L7]; *Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations*, NAT'L SEC. AGENCY (Jan. 2021), at 2, https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF [https://perma.cc/6J5F-NQ8W]; Clare Stouffer, *What is Encryption? How It Works + Types of Encryption*, NORTON (July 18, 2023), https://us.norton.com/blog/privacy/what-is-encryption [https://perma.cc/9D5E-WTC3]; *What is Encryption?*, CISCO, https://www.cisco.com/c/en/us/products/security/encryption-explained.html [https://perma.cc/HM4E-VWRA]; *Encryption of Data in Transit*, AMAZON WEB SERVICES (2024), https://docs.aws.amazon.com/whitepapers/latest/efs-encrypted-file-systems/encryption-of-data-in-transit.html [https://perma.cc/Q7U3-FRKR]; *Why use TLS 1.3?*, CLOUDFLARE (last visited Nov. 24, 2024), https://www.cloudflare.com/learning/ssl/why-use-tls-1.3/ [https://perma.cc/9642-7SEA]; *Salesforce Services and Marketing Cloud Supported TLS Cipher Suites*, SALESFORCE (last visited Nov. 24, 2024), https://help.salesforce.com/s/articleView?id=000380977&type=1 [https://perma.cc/SPA8-ZK83]; Brenna Cleary, *VPN Protocols: 7 Types* and Comparisons, NORTON (May 13, 2024), https://us.norton.com/blog/privacy/vpn-protocols [https://perma.cc/DA33-NLE7]; *What Are the Different Types of VPN Protocols?*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/types-of-vpn-protocols#l2tp [https://perma.cc/P5N7-84CF]; *Selecting and Hardening Remote Access VPN Solutions*, NAT'L SEC. AGENCY, https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/csi_selecting-hardening-remote-access-vpns-20210928.pdf [https://perma.cc/3XPG-9BRX]; *What is a Firewall? - Definition & Explanation*, AO KAPERSKY LAB, https://usa.kaspersky.com/resource-center/definitions/firewall [https://perma.cc/4FWE-YHJR]; *What is a Firewall?*, CISCO SYS., https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html [https://perma.cc/R9D7-37EN]; *Keeping Devices and Software Up to Date*, NAT'L CYBER SEC. CENTER, https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date [https://perma.cc/G94A-PZML]; CRYSTAL PANEK, SECURITY FUNDAMENTALS 33–109 (2019); *What is Cloud Architecture?*, GOOGLE CLOUD, https://cloud.google.com/learn/what-is-cloud-architecture [https://perma.cc/E7GP-V3ZJ]; MICROSOFT, *What is a Hybrid Cloud?*, MICROSOFT, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-hybrid-cloud-computing [https://perma.cc/S2FB-C94H]; Raj Sachdev, Legal Issues in Cloud Security and Privacy (2019) (Master's dissertation, Univ. of Oxford) (on file with author); PREETI MISHRA ET AL., CLOUD SECURITY: ATTACKS, TECHNIQUES, TOOLS, AND CHALLENGES 29 (CRC Press 2022); Ejona Preçi & Peter H. Gregory, *SaaS Security Risk and Challenges*, ISACA (July 26, 2022), https://www.isaca.org/resources/news-and-trends/industry-news/2022/saas-security-risk-and-challenges [https://perma.cc/CAE3-

1. The Value of the Trade Secret

Because of a "very wide band of discretion, the trade secret owner is to consider the value of the secret, the nature of the threat to disclosure, and the cost of any particular security mechanism."[125] It should first be considered, for all relevant trade secrets involved, what their value is. A mechanism should be used to assign a relative value to the trade secrets such as *High*, *Medium*, or *Low*. If needed, more specific methods may be adopted. For example, a specific monetary value would be ideal, although this may not always be necessary. This assignment of value, or level of value, is

---

PQZR]; Robert Ackerman, *The Critical Intersection of AI and Cybersecurity is Moving Briskly*, RSA CONFERENCE (Sept. 5, 2024), https://www.rsaconference.com/library/blog/the-critical-intersection-of-ai-and-cybersecurity-is-moving-briskly [https://perma.cc/S8PE-EZ7U]; *What Is Generative AI in Cybersecurity?*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/generative-ai-in-cybersecurity [https://perma.cc/XJ32-QBNV]; ELIZABETH A. ROWE & SHARON K. SANDEEN, TRADE SECRETS LAW: CASES AND MATERIALS 188 (2d ed. 2017); 1-4 TRADE SECRET LAW AND CORPORATE STRATEGY § 4.03 *Risk Assessment*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/risk_assessment [https://perma.cc/LYN8-GGMH]; *Physical Security*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/physical-security [https://perma.cc/ES6H-R92L]; *Layering Network Security Through Segmentation*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY (Jan. 2022), https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf [https://perma.cc/XX39-T7XN]; *Portable Storage Device*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/portable_storage_device [https://perma.cc/KF7H-HW9S]; Peter S. Menell, David S. Almeling, Victoria A. Cundiff, James Pooley, Elizabeth Rowe, Peter J. Toren, Rebecca Wexler, Federal Judicial Center, Trade Secret Case Management Judicial Guide, 2023, https://www.fjc.gov/sites/default/files/materials/08/Trade%20Secret%20final.pdf; RESTATEMENT (THIRD) UNFAIR COMPETITION § 43.

[125] PETER S. MENELL ET AL., *supra* note 1, at 2-14.

important because the reasonableness of the measures may be impacted by the value. As noted by Rowe and Sandeen, the "[e]fforts to protect the secrecy of information are also related to the economic value requirement."[126] In fact, the "guiding principles seem to boil down to simple cost-benefit analysis."[127] Specifically, the trade secret holder should "perform a cost-benefit analysis of possible information security measures to adopt an information security plan that is reasonable under the circumstances to maintain the secrecy of any information that gives the company a competitive advantage."[128] Therefore, "efforts need not be impregnable."[129] For low-value trade secrets, such as a trade secret worth a few thousand dollars or less, basic cybersecurity measures may be reasonable.[130] As will be seen in the specific measures in subsection 4 below, the most extensive firewalls, Virtual Private Networks (VPNs), and the most elaborate measures are unlikely to be needed to constitute reasonable measures, as historically, "neither extravagance nor absolute secrecy" are required.[131] In general, for medium-value trade secrets, some additional measures beyond the basic should be considered.[132] For high-value trade secrets, such as those worth millions or more, it is expected that more advanced protective measures

[126] ROWE & SANDEEN, *supra* note 43.
[127] JAMES POOLEY, TRADE SECRETS (ALM) § 4.04 (2024).
[128] 1 DAVID W. QUINTO ET AL., TRADE SECRETS: LAW AND PRACTICE § 4.03.
[129] See PETER S. MENELL ET AL., *supra* note 1.
[130] *Trade Secrets and Digital Objects*, *supra* note 15.
[131] Rachael Rodman, *Trade Secrets, Professional Perspective - Reasonable Measures Under the DTSA*, BLOOMBERG L. (Jan. 2020), https://www.bloomberglaw.com/external/document/X2QG2S4K000000/trade-secrets-professional-perspective-reasonable-measures-under [https://perma.cc/4SME-ZGX5].
[132] Candido et al., *supra* note 34; *Trade Secrets and Digital Objects*, *supra* note 15.

would be required.[133] As will also be discussed in subsection 4, this does not always mean a higher cost, but for some cybersecurity measures, it certainly will. The key consideration here is that the greater the value of the digital trade secret, the greater the level of measures that may be needed to constitute reasonable.[134] Therefore, an organization "should implement security measures that are roughly proportionate to the value of the information protected."[135]

2. Where and How the Digital Trade Secret is Stored

Where and how the digital trade secret is stored must be considered. If stored in the cloud, the type of cloud service should be considered. For example, Software as a Service (SaaS) is a common form of service available through the cloud, through which technical means for storing or accessing digital trade secrets may be provided.[136] It is important to consider not only the security of the cloud service but also the security of the devices and locations from which the cloud service is accessed. To this end, who has what security responsibilities should be considered, and the level of security provided by the cloud provider is also relevant. If the digital trade secret is stored locally, the courts should consider where it is stored, such as on-

---

[133] *Id.*
[134] *Id.*
[135] 1-4 DAVID S. ALMELING & DARIN W. SNYDER, TRADE SECRET LAW AND CORPORATE STRATEGY § 4.03.
[136] Nikhil Pradhan, *How Intellectual Property Fits in Cloud Computing and SaaS Business Models*, NAT'L L. REV. (Nov. 8, 2022), https://natlawreview.com/article/how-intellectual-property-fits-cloud-computing-and-saas-business-models, [https://perma.cc/FNZ3-AAP8]; Jane Song, *Intellectual Property Due Diligence: Acquisition of a Software-as-a-Service Business*, BLOOMBERG L. (Dec. 1, 2017), https://news.bloomberglaw.com/esg/intellectual-property-due-diligence-acquisition-of-a-software-as-a-service-business [https://perma.cc/KK58-NPNM].

premises servers or computers, and how those are being secured. If multiple methods of storage are used, including both cloud and local storage, various factors will need to be considered for all storage methods.

3. Who or What Wants/May Want Access to the Digital Trade Secret

Who or what may want access to the digital trade secret is an important consideration. For example, specific legitimate and authorized individuals may want access, such as legitimate employees and service providers in the course of and within their employment. However, bad actors could also attempt to gain access for any given reason, including monetary gain, competitive advantage, or simply for the enjoyment of breaching security.[137] Beyond individuals, things such as bots or malicious software may also want access.[138] Assessing these actors and factors is important in determining how much and what kinds of protection would be reasonable under the given circumstances.

It is important to consider the threats and risks associated with digital trade secrets and to conduct, at least, a reasonable risk assessment. For example, some common types of cybersecurity threats may include malware, a type of malicious software attack to gain access to digital trade secrets.[139] A "man-in-the-middle" attack permits

---

[137] *Id.*
[138] Christian B. Hecht, *Man vs. Machine: Court Examines Bot's Data Scraping as Improper Means of Appropriating Trade Secrets*, JD SUPRA, https://www.jdsupra.com/legalnews/man-vs-machine-court-examines-bot-s-7793801/ [https://perma.cc/KN5Q-94K9]; *Bot Attack Security Risks*, IDENTITY MANAGEMENT INSTITUTE, https://identitymanagementinstitute.org/bot-attack-security-risks/ [https://perma.cc/99JH-6KT9].
[139] Sameer Somal, *The Increasing Threat of Cyber Espionage and Its Impact on Trade Secret Protection*, IP WATCHDOG (Jan. 3, 2025), https://ipwatchdog.com/2025/01/03/the-increasing-threat-of-cyber-

eavesdropping "on a network connection to intercept and relay messages between two parties,"[140] which could be used to take digital trade secrets. A "social engineering"[141] attack is where a bad actor uses "human interaction (social skills)"[142] to trick someone to provide digital trade secrets and includes "phishing" where emails, text messages, or calls may be used to obtain that information.[143] An "insider threat" is defined "as the threat that an insider, such as an employee, will use their authorized access, intentionally or unintentionally, to do harm" to the organization, including, but not limited to, taking digital trade secrets.[144] "Advanced persistent threats" (APTs) are such attacks where a bad actor "carries out a prolonged attack"[145] against an organization, such as by using a variety of different attacks and may go unnoticed for a relatively long period of time.[146] Attacks may also happen through suppliers and service providers, which include cloud services.[147] A number of other cybersecurity threats are possible, and the risk these threats

---

espionage-and-its-impact-on-trade-secret-protection/ [https://perma.cc/NXW5-THYV].

140 IBM Cloud Team, *Types of Cyberthreats*, IBM (Mar. 25, 2024), https://www.ibm.com/think/topics/cyberthreats-types [https://perma.cc/3GYY-GU9R].

141 *Avoiding Social Engineering and Phishing Attacks*, CYBERSEC. & INFRASTRUCTURE SECURITY AGENCY (Jan. 2022), https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks [https://perma.cc/MUY6-N6UA].

142 *Id.*

143 IBM Cloud Team, *supra* note 140.

144 *Defining Insider Threats*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats [https://perma.cc/42K5-8FS4]; Somal, *supra* note 139.

145 *Advanced Persistent Threat (APT) Buyer's Guide*, GEN. SERVS. ADMIN. (July, 2022), https://www.gsa.gov/system/files/APT_Buyers_Guide_v2_July_2022.pdf [https://perma.cc/YY8H-JHZ4].

146 *Id.*

147 Somal, *supra* note 139.

cause may include substantial business loss, impact on "competitive advantage," "reputation," and financial costs.[148] However, some threats may not be from bad actors. For example, employees may accidentally or unknowingly release trade secrets.[149]

4. Specific Reasonable Cybersecurity Measures

After assessing the three considerations above and conducting a reasonable risk assessment,[150] specific reasonable cybersecurity measures should be assessed. For example, all of the cybersecurity measures in place for a digital trade secret should be reviewed in light of these factors. The various specific measures outlined in the framework will now be considered; however, they should not be viewed as measures that will or will not meet the reasonableness requirement, as all matters will be decided based on the circumstances, and each measure may be coupled with other measures. Further, which and how many of these specific measures may be considered reasonable will depend on the circumstances, and there is no formula for determining exactly which measures would be required. Each of the specific measures below show relevant considerations for each cybersecurity measure, and it is recommended that courts consider the technical aspects of

---

[148] R. Mark Halligan, *The Current Trade Secret Conundrum: The Cart Before the Horse*, REUTERS (July 6, 2021), https://www.reuters.com/legal/legalindustry/current-trade-secret-conundrum-cart-before-horse-2021-07-06/ [https://perma.cc/F4KZ-2NMT].

[149] Stephen Vaughn, *The Big Oops: Planning for Inadvertent Disclosures of Trade Secrets*, LAW.COM (Apr. 3, 2019), https://www.law.com/dailyreportonline/2019/04/03/the-big-oops-planning-for-inadvertent-disclosures-of-trade-secrets/?slreturn=20250130151931, [https://perma.cc/8BF4-4436].

[150] PETER S. MENELL ET AL., *supra* note 1, at 8-4; RESTATEMENT (THIRD) UNFAIR COMPETITION § 43.

each, as introduced below, prior to concluding whether reasonable measures were taken. Further, as the Montana District Court noted, it is important that measures taken are "consistently enforced" which, if not, may raise "a question as to whether plaintiff had in fact used reasonable measures."[151] In fact, "[s]loppy implementation of sensible security measures can destroy trade secrecy."[152]

a. *Access Management, Authentication, and Authorization (Need-to-Know Basis)*

Access management, according to the National Institute of Standards and Technology (NIST), includes a "set of practices that enables only those permitted the ability to perform an action on a particular resource."[153] Password protection is one common aspect of access management and simply involves requiring a "secret authenticator."[154]

Several cases have recognized password protection among the measures that may be taken to collectively reach the level of reasonable measures under the DTSA. In *Houser v. Feldman*, trade secrets in models and data which might be used to create "treatments and therapies"[155] in the future were under consideration. As just one among the measures to prove reasonable measures, it was acceptable that the contents of the trade secret "were kept only in . . . [a]

[151] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.04; *see* GTAT Corp. v. Fero, No. CV 17-55-M-DWM, 2017 U.S. Dist. LEXIS 80511, at *10 (D. Mont. May 25, 2017).
[152] PETER S. MENELL ET AL., *supra* note 1, at 2-16.
[153] *Access Management*, NATI'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/access_management [https://perma.cc/G37D-GSK3].
[154] Paul A. Grassi et al., *Digital Identity Guidelines Authentication and Lifecycle Management*, NAT'L INST. OF STANDARDS AND TECH. (June 2017), https://pages.nist.gov/800-63-3/sp800-63b.html [https://perma.cc/4DJ5-9EC3].
[155] Houser v. Feldman, 569 F. Supp. 3d 216, 221 (E.D. Pa. 2021).

lab or . . . office and were either locked or password protected."[156] The platform, which was a trade secret or included trade secrets in *ResMan, LLC v. Karya Prop. Mgmt., LLC*, was password protected.[157] In *Inv. Sci., LLC v. Oath Holdings Inc.*, the court recognized, in general, that password protection may be one acceptable measure.[158]

Requiring "limits and obligations of anyone given access to [its] system, [as well as] password and security controls that require verification of each user's identity . . ."[159] is a basic aspect of access management. This was recognized in *WalkMe Ltd. v. Whatfix, Inc.* in the context of a motion to dismiss for alleged trade secrets comprising "uniquely designed tables, columns, account number structures, methods of populating table data, and [a] combination or interrelation thereof "[160]

While various courts have accepted passwords among reasonable measures, simply stating that password protection will meet this requirement could be a faulty conclusion by a court. For example, simple or poorly implemented password protection may be considered insufficient, and best practices for passwords may be recommended or even enforced through password policies that require users to select strong passwords.[161] Breaches can occur when organizations fail to change the "default passwords" that come with hardware or systems, allowing attackers easy access because they can look these up or

[156] *Id.* at 230.
[157] ResMan, LLC v. Karya Prop. Mgmt., LLC, No. 4:19-CV-00402, 2021 U.S. Dist. LEXIS 145462, at *17 (E.D. Tex. Aug. 4, 2021).
[158] Inv. Sci., LLC v. Oath Holdings Inc., 20 Civ. 8159 (GBD), 2021 U.S. Dist. LEXIS 151076, at *7 (S.D.N.Y. Aug. 11, 2021).
[159] WalkMe Ltd. v. Whatfix, Inc., No. 23-cv-03991-JSW, 2024 U.S. Dist. LEXIS 120331, at *7 (N.D. Cal. July 9, 2024).
[160] *Id.*
[161] Grassi et al., *supra* note 154, at § 2.

obtain them from the product or published sources.[162] Further, passwords "need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value."[163] However, recent recommendations show that "lengthy" or "complex" passwords may not necessarily be more secure, especially if these are documented physically or "stored electronically in an unsafe manner".[164] Passwords may also be required to be changed periodically in order to reduce the chance of attack. However, whether any of the above would be required is unclear.

Despite the general acceptability of password protection,[165] in *Inv. Sci., LLC v. Oath Holdings Inc.*,[166] this "cyber-security" measure was not considered a sufficient pleading of reasonable measures for purposes of a motion to dismiss for two reasons.[167] First, the measure was insufficient because an employee provided a "hardcopy" of a "Trading Plan" to the other party, who retained it "for his records," rendering the measure useless.[168] Second, the alleged trade secrets were disclosed by presenting them through a phone "using the password and login of his work email," which was not distinguished from "a protective measure that is used to safeguard any other corporate

---

162 *Risks of Default Passwords on the Internet*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY (Oct. 7, 2016), https://www.cisa.gov/news-events/alerts/2013/06/24/risks-default-passwords-internet [https://perma.cc/B78M-CWLA].
163 Grassi et al., *supra* note 154, at § 5.1.1.
164 *NIST SP 800-63 Digital Identity Guidelines*, NAT'L INST. OF STANDARDS AND TECH., https://pages.nist.gov/800-63-4/sp800-63b.html#appA [https://perma.cc/R3P4-P4XP].
165 *ResMan, LLC*, 2021 U.S. Dist. LEXIS 145462, at *17; *Inv. Sci., LLC*, 2021 U.S. Dist. LEXIS 151076, at *7.
166 *Inv. Sci., LLC*, 2021 U.S. Dist. LEXIS 151076, at *7.
167 *Id.* at *9–10.
168 *Id.* at *10.

information”[169] that might signify the enhanced protection afforded to a trade secret. Recently, in *Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC*, “[u]ser password management which specifies password complexity, length, and change requirements including automatic password suspension after a certain number of failed login attempts” was acceptable.[170] For those trade secrets in marketing that can derive significant value for an organization, strong password protection may be expected. However, it is unclear whether courts will always examine such details, which may require the parties to raise these considerations. The Alabama District Court, in *Physiotherapy Assocs., Inc. v. ATI Holdings, LLC*, found “that Physiotherapy’s password-protection system reflects little more than a ‘normal business practice’”[171] and declined to afford this measure reasonable measure status, especially because, as it concluded, a “system-wide password” allowed all employees to access all information.[172]

At the same time, some courts have recognized further related measures. As the *Wwmap, LLC v. Midwifery* court recently described it, reasonable measures can include “access control policies or measures—such as passwords, thumbprints, or iris scans—to protect computers, documents, and files that contain secrets.”[173] This case recognizes additional specific modern methods of protection, as password protection and access management methods have evolved.

---

[169] *Id.*
[170] Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC, 22 CVS 4285, 2024 NCBC 46, 166 (N.C. Super. Ct. 2024).
[171] Physiotherapy Assocs., Inc. v. ATI Holdings, LLC, 592 F. Supp. 3d 1032, 1042 (N.D. Ala. 2022); 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.01.
[172] *Id.*
[173] Wwmap, LLC v. Midwifery, 711 F. Supp. 3d 1313, 1322 (N.D. Fla. 2024).

Multi-factor Authentication (MFA) is "an important security enhancement that requires a user to verify their identity by providing more than just . . . something you know," which is the category under which a "username and password" falls.[174] For example, "something you have," such as a "smart card or pin" might be used in addition.[175] Alternatively, this may be "something you are," such as a "fingerprint or face" recognition system.[176] In *ResMan, LLC v. Karya Prop. Mgmt.*, *LLC*, a two-factor authentication of the subject matter platform was one of the various measures considered reasonable.[177] *Centurum Info. Tech. Inc. v. Geocent* recognized "password protection and multi-factor authentication, restricted access, and other means" as sufficient to constitute reasonable efforts.[178] MFA is rapidly becoming the norm for protecting important information.[179] In *Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC*, MFA was "required for employees in order to gain access to the Company network" and was considered, among other measures, a reasonable measure.[180]

Account deprovisioning is another aspect of access management.[181] This involves the removal of access to those no longer needing access or should no longer have access to

---

174 *Multi-Factor Authentication*, NAT'L INST. OF STANDARDS AND TECH. (Mar. 12, 2024), https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication [https://perma.cc/D3HZ-CZYB].

175 *Id.*

176 *Id.*

177 ResMan, LLC v. Karya Prop. Mgmt., LLC, No. 4:19-CV-00402, 2021 U.S. Dist. LEXIS 145462, at *16 (E.D. Tex. Aug. 4, 2021).

178 Centurum Info. Tech. Inc. v. Geocent, LLC, No. 21-0082, 2021 U.S. Dist. LEXIS 27661, at *41 (E.D. La. Feb. 12, 2021).

179 *Multi-Factor Authentication*, *supra* note 174.

180 Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC, 22 CVS 4285, 2024 NCBC 46, 166, 170 (N.C. Super. Ct. 2024).

181 Belle Wong, *Deprovisioning: Definition & Best Practices (2024)*, FORBES (Apr. 28, 2024, 6:37 PM), https://www.forbes.com/advisor/business/deprovisioning/# [https://perma.cc/6VBF-3B88].

specific resources, such as digital trade secrets.[182] For example, when an employee leaves an organization, their access should immediately be terminated. In *Wwmap, LLC v. Midwifery*, "prompt revocation of information technology access upon termination of employment" was considered as one reasonable measure sufficiently pleaded in the context of a motion to dismiss. [183]

Authorization is "[t]he right or a permission that is granted to a system entity to access a system resource."[184] In other words, once a user is within a system, there may be limitations on what they are able to do within the system. In the field of cybersecurity, the concept of "least privilege" is relevant, and "a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks."[185] Courts have recognized, alongside other measures, that limiting authorization to a "need-to-know"[186] basis can help meet the reasonable measures standard.[187] In other words, a trade secret may be revealed to one "who has a need to know it and who knows it is confidential."[188]

---

[182] *Id.*
[183] Wwmap, LLC v. Midwifery, 711 F. Supp. 3d 1313, 1322 (N.D. Fla. 2024).
[184] *Authorization*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/authorization [https://perma.cc/9XFH-SRW6].
[185] *Least Privilege*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/least_privilege [https://perma.cc/9ZRF-JKEJ].
[186] *Trade Secrets and Digital Objects*, *supra* note 15, at § 6.1; Candido et al., *supra* note 34.
[187] UrthTech LLC v. GOJO Indus., No. 22-cv-6727 (PKC), 2023 U.S. Dist. LEXIS 125555, at *31 (S.D.N.Y. July 20, 2023); Inv. Sci., LLC v. Oath Holdings Inc., 20 Civ. 8159 (GBD), 2021 U.S. Dist. LEXIS 151076, at *7 (S.D.N.Y. Aug. 11, 2021); AD Lightning Inc. v. Clean.io, Inc., No. 19-CV-7367 (JPO), 2020 U.S. Dist. LEXIS 141311, at *6 (S.D.N.Y. Aug. 7, 2020).
[188] JAMES POOLEY, TRADE SECRETS (ALM) § 4.04 (2024).

UrthTech LLC v. GOJO Indus. recognized such a "need-to-know" basis as a part of reasonable measures.[189] This followed from the general recognition in *Inv. Sci., LLC v. Oath Holdings Inc.* of such basis as one measure.[190] Further, *Wwmap, LLC v. Midwifery* recognized the "compartmentalization of information,"[191] borrowing from cybersecurity terminology[192] and grounded in the "need to know" principle.[193] Restricting certain trade secret information to be accessible only to an "administrator" has also been recognized as part of reasonable measures, as seen in *WalkMe Ltd. v. Whatfix, Inc.*[194] Likewise, in *Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC*, the court recognized "[r]ole-based permissions allowing access to [c]ompany data only on a need-to-know basis."[195] These restrictions also help mitigate an "insider threat."[196] If such restrictions are employed, employees who do not have access to certain resources because they do not need them to perform their duties will not be able to cause such harm. However, "limited disclosure of certain information to a small group of people" may not necessarily result in a finding of reasonable, such as where the Southern District of New York found that the limited disclosure "may have been due to the

---

[189] *UrthTech LLC*, 2023 U.S. Dist. LEXIS 125555, at *31.
[190] *Inv. Sci., LLC*, 2021 U.S. Dist. LEXIS 151076, at *7.
[191] Wwmap, LLC v. Midwifery, 711 F. Supp. 3d 1313, 1322 (N.D. Fla. 2024).
[192] *Compartmentalization*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/compartmentalization [https://perma.cc/2Y5X-J54N].
[193] *Wwmap, LLC*, 711 F. Supp. 3d at 1322.
[194] WalkMe Ltd. v. Whatfix, Inc., No. 23-cv-03991-JSW, 2024 U.S. Dist. LEXIS 120331, at *7 (N.D. Cal. July 9, 2024).
[195] Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC, 22 CVS 4285, 2024 NCBC 46, 166 (N.C. Super. Ct. 2024).
[196] *Defining Insider Threats*, *supra* note 144.

nature of the work rather than an affirmative step to preserve secrecy."[197]

Restriction of data transmission, limiting the ability or access to forward, copy, or otherwise disseminate trade secrets through technical means, may also support a finding of reasonable measures.[198] For example, a document containing trade secrets may, in some cases, be prevented from being attached to an email, forwarded by technical means,[199] or from being copied, downloaded,[200] printed (such as "without managerial approval"),[201] or captured through a screenshot[202] or similar mechanism. It should be noted that there are methods that may overcome these restrictions, which are difficult to prevent, such as taking a picture of a monitor screen on which a trade secret may be displayed, instead of a screenshot, unless a technology is

---

[197] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.04; *see* Pauwels v. Deloitte LLP, No. 19-CV-2313 (RA), 2020 U.S. Dist. LEXIS 28736, at *18 (S.D.N.Y. Feb. 19, 2020).

[198] Laura Alaniz & Derek Forinash, *New Year, New Employment: Trade Secret Mishaps and Best Practices*, PORTER HEDGES (Jan. 18, 2022), https://www.porterhedges.com/assets/htmldocuments/2022.01.18%20New%20Year%20New%20Employment.pdf [https://perma.cc/A62L-Z8DJ].

[199] DES Support Center, *Prevent Email From Being Forwarded*, DES, https://desitsupport4u.des.wa.gov/hc/en-us/articles/4406921820695-Prevent-Email-from-being-Forwarded [https://perma.cc/6LLX-MUPS].

[200] *Block Downloads for View-Only Files in SharePoint and OneDrive*, MICROSOFT, https://support.microsoft.com/en-us/office/block-downloads-for-view-only-files-in-sharepoint-and-onedrive-6051184b-62ac-4149-b874-13dcd40ef91e [https://perma.cc/6YWM-CMK5]; *How to Set or Change Shared Link Permissions*, DROPBOX (Jan. 16, 2025), https://help.dropbox.com/share/set-link-permissions [https://perma.cc/7T9M-7WC9].

[201] Ingram v. Cantwell-Cleary Co., 260 Md. App. 122, 169 (2023); 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.01.

[202] Mark Hachman, *Microsoft Edge Will Start Blocking Screenshots on the Job*, PCWORLD (May 23, 2024), https://www.pcworld.com/article/2336462/microsoft-edge-will-start-blocking-screenshots-on-the-job.html [https://perma.cc/SSS8-EPN8].

used to try and prevent this.[203] However, as noted earlier, "absolute" secrecy is not required.[204]

Holders of digital trade secrets in marketing will likely be expected to employ sufficient access management measures, including strong password protection, MFA, authentication, and authorization limited to a "need-to-know"[205] basis, as noted above.

b. Digital Marking

As noted in Part III, some measures may be low-cost, yet effective. Digitally marking a trade secret as "confidential," or using a "label, footer, digital watermark or electronic tag" through a variety of technical means, may be helpful in establishing reasonable measures[206] and could also be a low-cost measure. For example, when accessing a program or document containing trade secrets, a prominent banner or watermark may be displayed to remind users that this information should not be disclosed. In some cases, a warning may be appropriate to accompany the marking, which may serve as a reminder of the trade secret. In advanced cases, there may be a prominent warning requiring acceptance each time it is accessed.

c. Encryption or Related Methods

According to NIST, encryption involves "[c]ryptographic transformation of data (called 'plaintext')

---

[203] *A Hidden Blind Spot in Data Security*, FASOO, https://en.fasoo.com/strategies/screen-security/ [https://perma.cc/S4WE-RG65].

[204] ResMan, LLC v. Karya Prop. Mgmt., LLC, No. 4:19-CV-00402, 2021 U.S. Dist. LEXIS 145462, at *14–15 (E.D. Tex. Aug. 4, 2021); Chmura Econs. & Analytics, LLC v. Lombardo, No. 3:19-cv-813, 2021 U.S. Dist. LEXIS 143009, at *43 (E.D. Va. July 29, 2021); AvidAir Helicopter Supply, Inc. v. Rolls-Royce Corp., 663 F.3d 966, 974 (8th Cir. 2011).

[205] Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC, 22 CVS 4285, 2024 NCBC 46, 166 (N.C. Super. Ct. 2024).

[206] *Trade Secrets*, *supra* note 17, at 5; Candido et al., *supra* note 34, at 12.

into a form (called 'ciphertext') that conceals the data's original meaning to prevent it from being known or used."[207] Essentially, "cryptography uses mathematical techniques to transform data and prevent it from being read or tampered with by unauthorized parties," such as to secure communication in "e-commerce transactions, mobile device conversations and other exchanges of data."[208] The process of decryption takes the "ciphertext" and decodes it into readable "plaintext."[209] In other words, encrypting the contents of a trade secret will allow it to not be read in plain language, and decrypting it allows authorized individuals to access it in a readable form. Trade secrets in marketing may be stored using encryption as one method of trying to secure this information.

There are a number of types and methods of encryption, a detailed description of which is beyond the scope of this article, although a summary is helpful. The two main types of encryption are "symmetric" encryption and "asymmetric" encryption.[210] Symmetric encryption uses the same "key,"[211] which is a "parameter used in conjunction with a cryptographic algorithm that determines its

[207] *Encryption*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/encryption [https://perma.cc/D5YL-GX9X].
[208] *Cryptography*, NAT'L INST. OF STANDARDS AND TECH., https://www.nist.gov/cryptography [https://perma.cc/LP4Q-7ZXV].
[209] Grassi et al., *supra* note 154.
[210] *What is Encryption?*, CISCO, https://www.cisco.com/c/en/us/products/security/encryption-explained.html [https://perma.cc/HM4E-VWRA].
[211] *Id.*

operation"[212] to "encrypt" and "decrypt" information.[213] Asymmetric encryption uses a "public key" to encrypt, but instead of the same key, it uses a "private key" to decrypt.[214] Only specific pre-determined users would be provided access to the "private key" in this method, providing enhanced security over "symmetric" methods.[215] The National Security Agency (NSA) warns that "obsolete encryption provides a false sense of security," and data may not actually be protected.[216]

Beyond this, it is important to understand specific data encryption standards that are utilized in security today. Data Encryption Standard (DES) and Triple Data Encryption Standard (TDES/3DES) are older methods of encryption that are prone to attacks and not considered suitable for "sensitive data."[217] The Rivest-Shamir-Adleman (RSA) encryption employs "asymmetric cryptography" described above and uses "prime factorization," although it has been considered by some as "increasingly inefficient at higher security levels."[218] The currently popular Advanced

---

212 *Cryptographic Key*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/cryptographic_key [https://perma.cc/GCB9-H7L7]; *Symmetric Key*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/symmetric_key [https://perma.cc/5VZ9-UJWX].

213 *What is a Firewall?*, *supra* note 91.

214 *Id.*

215 *Id.*

216 *Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations*, NAT'L SEC. AGENCY (Jan. 2021), at 2, https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF [https://perma.cc/6J5F-NQ8W].

217 *Id.* at 3; Clare Stouffer, *What is Encryption? How It Works + Types of Encryption*, NORTON (July 18, 2023), https://us.norton.com/blog/privacy/what-is-encryption [https://perma.cc/9D5E-WTC3].

218 Stouffer, *supra* note 217; *What is a Firewall?*, *supra* note 91.

Encryption Standard (AES) uses "symmetric encryption and a substitution permutation network (SPN) algorithm to apply multiple rounds of encryption,"[219] which enhances the security and is much harder to decrypt. For example, it "uses three separate keys: AES-128, AES-192, and AES-256" and has been used to "protect classified government information and sensitive data."[220]

However, a "protocol" is used to encrypt data, and data "in transit," such as that used by certain Amazon Cloud Services, may be "encrypted in transit using Transport Layer Security 1.2 (TLS) with an industry-standard AES-256 cipher."[221] TLS 1.2 is commonly employed in these circumstances, although TLS 1.3 is available, and TLS 1.2 or higher has been recommended for certain data.[222] As the NSA and industry recommend moving away from TLS lower than 1.2,[223] this might not be adequate for reasonable measures, subject to court discretion and the circumstances in a case-by-case analysis. However, a court may or may not reach this level of technical detail.

A much more advanced encryption is Elliptic Curve Cryptography (ECC), which "based on a common public key

---

[219] Stouffer, *supra* note 217.
[220] *What is a Firewall*?, *supra* note 91.
[221] *Encryption of Data in Transit*, AMAZON WEB SERVICES (2024), https://docs.aws.amazon.com/whitepapers/latest/efs-encrypted-file-systems/encryption-of-data-in-transit.html [https://perma.cc/Q7U3-FRKR].
[222] *See Why use TLS 1.3?*, CLOUDFLARE, https://www.cloudflare.com/learning/ssl/why-use-tls-1.3/ [https://perma.cc/9642-7SEA]; *Salesforce Services and Marketing Cloud Supported TLS Cipher Suites*, SALESFORCE, https://help.salesforce.com/s/articleView?id=000380977&type=1 [https://perma.cc/SPA8-ZK83].
[223] *Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations*, *supra* note 216, at 3; *Why use TLS 1.3?*, *supra* note 222; *Salesforce Services and Marketing Cloud Supported TLS Cipher Suites*, *supra* note 222.

algorithm, ECC combines elliptic curves and number theory to encrypt data."[224] Further, NIST recently released encryption standards for quantum computers,[225] devices that "deliver huge leaps forward in processing power" and have the "ability to generate and manipulate quantum bits, or qubits," which are "typically subatomic particles such as electrons or photons."[226] These stand in stark contrast to traditional computers, which use "bits—a stream of electrical or optical pulses representing *1*s or *0*s"[227] and consequently do not use as much power. These newer encryption standards are likely unnecessary for purposes of most of today's trade secrets but may become more relevant in the future.

Courts have referred to encryption as one measure among others that could lead to reasonable measures. In *Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC*, "[f]ull disk encryption on Company-issued portable devices (e.g., laptops)" and "encryption of Company Data" was reasonable alongside other measures.[228] However, in *PPEX v. Buttonwood, Inc.*, a customer list for an online marketplace that used blockchain was "stored on PPEX's client database" and was described as being "secured via SSH which uses public-key cryptography—a military-grade encryption with 256-bit keys requiring users to have one of

---

[224] *What is Encryption?*, *supra* note 210.
[225] *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*, NAT'L INST. OF STANDARDS AND TECH. (Aug. 13, 2024), https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards [https://perma.cc/D9RG-LZ5Z].
[226] Martin Giles, *Explainer: What is a Quantum Computer?*, MIT TECH. REV. (Jan 29, 2019), https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/ [https://perma.cc/3KBN-GQGH].
[227] *Id.*
[228] Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC, 22 CVS 4285, 2024 NCBC 46, 166 (N.C. Super. Ct. 2024).

these keys to access the database."[229] Despite the described level of cryptography, which might, on the face of it, be considered among reasonable measures, the court declined to issue a preliminary injunction because there were no "steps to ensure that persons within PPEX knew or treated those lists as secret or confidential to PPEX."[230] Therefore, digital trade secret holders should consider other measures alongside encryption.

In *Houser v. Feldman*, the plaintiff "coded" the contents of the trade secret "so that they were intelligible to only Houser or his lab members," which was considered a part of the sufficiently pled reasonable measures taken for purposes of a motion to dismiss.[231] While the specific type of coding used was not outlined in this decision, even if not a recognized encryption method, this appears to have supported reasonable measures under the circumstances.

Digital trade secrets in marketing, depending on the nature of the trade secrets, might be sufficiently encrypted for better security, and older methods of encryption should not be relied on. While a specific encryption type may not be required, selecting an appropriate one should be carefully considered. For example, DES and TDES are unlikely reasonable.[232] Likewise, TLS 1.2 or a higher encryption might be reasonable for some trade secrets, and other methods may be needed for others.[233]

d. Virtual Private Network (VPN) or Restricted Remote Access

[229] PPEX v. Buttonwood, Inc., No. 21-CV-53-F, 2021 U.S. Dist. LEXIS 254584, at *27 (D. Wyo. Sept. 7, 2021).
[230] *Id.* at *27, *40.
[231] Houser v. Feldman, 569 F. Supp. 3d 216, 230 (E.D. Pa. 2021).
[232] *Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations*, *supra* note 216, at 3.
[233] *Id.*

Restricting remote access might be one measure taken to enhance security. However, this may not be feasible in many virtual environments or where such restriction might itself be impracticable given the nature of remote work in today's employment context. Therefore, utilized measures may include a ban on the use of personal devices or a requirement to use VPNs for remote access to trade secrets.[234]

Some organizations use a VPN to enhance security.[235] A VPN "establishes a digital connection" between a "computer and a remote server," which establishes "a point-to-point tunnel that encrypts . . . personal data, masks . . . [an] IP address" and permits "sidestep[ping] website blocks and firewalls on the internet."[236] This common method employed by organizations gives employees remote access to organizational technical resources.[237]

While VPNs have clear security benefits, not all VPNs are the same, nor do they have the same features: some work for certain systems and devices, some are more broadly compatible, and others are geared toward sensitive corporate traffic.[238] For example, the Point-to-Point Tunneling Protocol (PPTP) is rendered "obsolete for enterprises concerned with protecting sensitive data" by enhanced

---

[234] Candido et al., *supra* note 34.
[235] *Id.*
[236] *What is a VPN?*, MICROSOFT, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn [https://perma.cc/EY3U-F5NK].
[237] *Id.*
[238] Brenna Cleary, *VPN Protocols: 7 Types and Comparisons*, NORTON (May 13, 2024), https://us.norton.com/blog/privacy/vpn-protocols [https://perma.cc/DA33-NLE7]; *What Are the Different Types of VPN Protocols?*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/types-of-vpn-protocols#l2tp [https://perma.cc/P5N7-84CF].

encryption methods.[239] Internet Key Exchange version 2 (IKEv2), which operates with IPsec (Internet Protocol Security)—collectively referred to as IKEv2/IPsec—is another, more secure option for VPNs.[240] Likewise, Layer 2 Tunneling Protocol (L2TP), an older protocol that may be used alongside IPSec (referred to as L2TP/IPsec), is widely used for creating VPN connections and employs a commonly implemented AES-256 encryption.[241] Another example is OpenVPN, which employs strong encryption and security but may be slower and have a more complex setup.[242] A relatively recent option, WireGuard, is positioned to be a fast and reliable choice.[243] However, it is still in the development stages.[244] The choice of the most suitable VPN will depend on particular circumstances and needs, although some older VPNs and approaches may not provide the relevant security.

In addition, it is important to reduce the remote access to a VPN's attack surface by employing measures to update and apply patches, thereby reducing the chance of attacks.[245] Further, access to and from the VPN should be protected.[246]

Cases have considered VPNs in the context of reasonable measures that parties have or could have taken to protect their data. In *Brown & Root Indus. Servs., LLC v. Brown*, in the context of a motion to dismiss, "requiring

---

[239] *What Are the Different Types of VPN Protocols?*, *supra* note 238.
[240] Cleary, *supra* note 238.
[241] *Id.*; *What Are the Different Types of VPN Protocols?*, *supra* note 238.
[242] *Id.*
[243] *What Are the Different Types of VPN Protocols?*, *supra* note 238.
[244] Cleary, *supra* note 238.
[245] *Selecting and Hardening Remote Access VPN Solutions*, NAT'L SEC. AGENCY, https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/csi_selecting-hardening-remote-access-vpns-20210928.pdf [https://perma.cc/3XPG-9BRX].
[246] *Id.*

remote access to Plaintiffs' databases only through Plaintiffs' virtual private network" was part of a number of measures considered allegedly reasonable at the pleading stage for protecting trade secret information.[247] Likewise, in *Hedgeye Risk Mgmt., LLC v. Dale*, in the context of contact lists, a "price volume volatility file," and other alleged trade secrets, a VPN was required for remote access, along with various other measures that were considered sufficient for purposes of the pleadings.[248] Similarly, in *Tri-State Floors, Inc. v. Old Rule Servs., Ltd. Liab. Co.*, where pricing structures, customer lists, and other alleged trade secrets were considered, a VPN set up, along with other measures, met sufficiently pled and reasonable measures to defeat a motion for summary judgment.[249] Likewise, in *Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC*, "[r]estrictions on remote user access to the Company's network (e.g., requiring access through the Company's . . . (VPN))"[250] were considered, amongst other measures, as reasonable.

Therefore, digital trade secret holders should consider the type of VPN, whether it suits their needs, and whether it can be argued that the use of that specific VPN would be considered a reasonable measure of data protection if the court reaches that level of technical discussion. For example, VPNs based on obsolete methods will likely be insufficient, and those offering many more advanced features or protections may only be needed for very high value trade secrets, depending on the storage environment and purpose of the VPN.

---

[247] Brown & Root Indus. Servs., LLC v. Brown, No. 21-291-JWD-SDJ, 2022 U.S. Dist. LEXIS 174537, at *23–25 (M.D. La. Sept. 9, 2022).
[248] Hedgeye Risk Mgmt., LLC v. Dale, No. 21-cv-3687 (ALC)(RWL), 2023 U.S. Dist. LEXIS 177181, at *11, *20 (S.D.N.Y. Sept. 29, 2023).
[249] Tri-State Floors, Inc. v. Old Rule Servs., Ltd. Liab. Co., No. 19-CV-707-JFH-JFJ, 2022 U.S. Dist. LEXIS 178356, at *23, *27–28 (N.D. Okla. Sept. 30, 2022).
[250] Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC, 22 CVS 4285, 2024 NCBC 46, 166 (N.C. Super. Ct. 2024).

e. Firewalls, Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS)

A firewall is a commonly used network security[251] mechanism that "regulates incoming and outgoing network traffic based on preset security rules."[252] It is considered a "first line of defense."[253] In other words, a firewall can block specific traffic into the network or prevent certain activity within a network.[254] However, while some features will block unwanted traffic, a firewall needs to be configured and will implement security policies, meaning it will follow the rules and setup from its configuration.[255] As outlined by NIST, such configuration is essential to properly securing the network segments.[256] This setup and configuration needs to be periodically reviewed, otherwise it may fail to meet its purpose.[257] Further, a firewall may have a "log" that documents activity within the network, allowing preventative or reactive action to take place, assisting in determining what happened within a network following an incident or attack in progress.[258]

There are a number of different firewalls, and simply alluding to a firewall without also describing its type, features, configuration, and other details does not itself discern the level of security the firewall may provide. A stateful inspection firewall is a traditional firewall that

---

[251] *What is a Firewall?*, *supra* note 91.
[252] *Id.*
[253] *Id.*
[254] *Id.*
[255] *Id.*
[256] Keith Stouffer et al., *Guide to Operational Technology (OT) Security*, NAT'L INST. OF STANDARDS AND TECH. (Sept. 2023), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf [https://perma.cc/655K-5PMF].
[257] *What is a Firewall?*, *supra* note 91.
[258] *Id.*

monitors network activity based on how it is configured and learns from past "connections," which may be blocked based on previous activity.[259] Another type, a proxy firewall, is a gateway from one network to another for a specific application and essentially functions as a potential block at the door of the application.[260] Yet another type is a next-generation firewall (NGFW), which provides enhanced security beyond traditional firewalls, including control of applications, an IPS that helps prevent attacks, and filtering based on geolocation, reputation, and threat intelligence.[261] Further, AI-powered firewalls are also making their way into the industry.[262] However, one should not simply compare firewalls without also assessing further details as noted above, and employing two firewalls may not necessarily be better than employing one appropriate firewall that is "well-maintained" and "well-configured."[263]

Further, a firewall is not, and does not necessarily (but may) come with an IDS.[264] An IDS, depending on its features and configuration, may monitor and detect all traffic, both internal and external, as employed.[265] An IPS, as referred to above, can "detect multiple types of cyber-attacks," and its goal is to "block them."[266] While all three—firewalls, IDS, and IPS—are security measures, they differ, but may be provided through one service provider and must be properly configured and deployed. Each will have similar

---

[259] *Id.*
[260] *Id.*
[261] *Id.*
[262] *Id.*
[263] *Security architecture anti-patterns*, NAT'L CYBER SEC. CENTRE (May 22, 2019), https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns [https://perma.cc/VV3R-XE6L].
[264] AN INTERDISCIPLINARY APPROACH TO MODERN NETWORK SECURITY 72–73 (Sabyasachi Pramanik et al. eds., CRC Press 2022).
[265] *Id.*
[266] *Id.* at 77.

or different features and may be geared towards certain types of networks or protection needs.[267]

Firewalls have regularly been considered by the courts. In *ResMan, LLC v. Karya Prop. Mgmt.*, *LLC*, a firewall was a considered reasonable measure among a host of other measures.[268] Likewise, in *Iacovacci v. Brevet Holdings, Ltd. Liab. Co.*, allegations of utilizing a firewall and log-in and password protection were among other measures which were considered adequately pled.[269]

Holders of digital trade secrets in marketing should consider the types of firewalls, features, and the necessary configurations needed to reasonably protect such secrets alongside other measures. For example, it is unlikely that an AI-powered firewall would be required to constitute a reasonable measure at this time. As long as a reasonable firewall that suits the purpose based on the trade secret and its value is in place, a court may accept that the firewall was sufficient.[270]

f. Security Suite, Updates, and Patching

Outdated software may open the door to further security concerns and is a key consideration for digital trade secrets.[271] A security suite is a combination of protection measures, including protection against viruses, malware, ransomware, and other threats, sometimes commonly

---

[267] IPS. vs. IDS vs. Firewall: What Are the Differences?, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/firewall-vs-ids-vs-ips [https://perma.cc/QD7H-N27U].
[268] ResMan, LLC v. Karya Prop. Mgmt., LLC, No. 4:19-CV-00402, 2021 U.S. Dist. LEXIS 145462, at *16–17 (E.D. Tex. Aug. 4, 2021).
[269] Iacovacci v. Brevet Holdings, Ltd. Liab. Co., 437 F. Supp. 3d 367, 381 (S.D.N.Y. 2020).
[270] *Id.*
[271] *Keeping Devices and Software Up to Date*, NAT'L CYBER SEC. CENTER, https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date [https://perma.cc/G94A-PZML].

referred to simply as anti-virus software (although it normally goes beyond this function).[272] These are offered by a variety of vendors, including consumer products, corporate vendors, and advanced customized services.[273] They come in various grades and supply various potential basic and advanced features, which may be designed for consumer use or specially designed suites or features exclusively for corporate use to protect the most sensitive information, such as digital trade secrets.[274] However, any claims by companies to do so should be verified. Some are equipped with other security mechanisms, discussed elsewhere in this article, such as specific types of firewalls or VPN's.[275] In some cases, software is provided by a third party, who may or may not undertake security responsibilities, as will be seen in section H below.

In *Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC*, the alleged use of "[a]nti-virus software, patch management, and network firewall maintenance" among other measures were considered sufficiently pled.[276] However, it is important to specifically consider the type of security suite and whether it is adequate to secure the digital trade secrets held. Further, whether the security suite itself is being kept updated is important to consider. For example, as new threats emerge and a security suite requires a technical update to keep it current, this update could be set to occur automatically, or it may require manual steps to enforce.[277]

---

[272] Neil J. Rubenking, *The Best Security Suites for 2024*, PC MAG (Nov. 12, 2024), https://www.pcmag.com/picks/the-best-security-suites [https://perma.cc/BA2U-BM9D].
[273] *Id.*
[274] *Id.*; *Sage 300 Security*, NORMING, https://www.norming.com/channel?pCateId=9 [https://perma.cc/LS94-JG44].
[275] *Id.*
[276] Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC, 22 CVS 4285, 2024 NCBC 46, 166 (N.C. Super. Ct. 2024).
[277] *Security Suite: What is it and How Can it Protect Your Business?*, AVG BUS., https://www.avg.com/en/signal/security-suite

If not updated, the security suite may be less effective and may not protect against the latest threats. If commercially deployed, a security suite may be set to perform automatic updates to get current protection.[278] In many instances, this may be considered a basic measure.[279]

Beyond the security suite, software also needs to be kept updated. For example, updates and patches may be available for different types of software, or applications may need updates to protect against the latest threats. When software vendors provide updates, these may be applied automatically or centrally, or they may require action or permissions.[280]

g. Logging, Accounting, and Reasonable Review

Logging is keeping "a record of the events occurring within an organization's systems and networks."[281] As discussed earlier, accounting is the concept related to "keeping track of a user's activity while accessing network resources."[282] These measures help track and potentially

[https://perma.cc/2EH4-4FAH]; *Configuring Automatic Updates for Trend Vision One Security Agents*, TREND MICRO INC. (May, 13, 2024), https://success.trendmicro.com/en-US/solution/KA-0016584 [https://perma.cc/AF3K-GSE8]; *Keep Your Norton Device Security Up to Date*, NORTON, https://support.norton.com/sp/en/us/norton-security-suite/current/solutions/v2035127 [https://perma.cc/38F9-NZEV].

[278] *Id.*

[279] *Information Services: Updates & Anti-Virus*, UNIV. OF STRATHCLYDE, https://www.strath.ac.uk/professionalservices/informationservices/cybersecurity/updatesanti-virus/ [https://perma.cc/TJT2-UX5V].

[280] *What is SaaS (Software as a Service)?*, AMAZON, https://aws.amazon.com/what-is/saas/ [https://perma.cc/6Q4E-YUU8].

[281] Karen Kent & Murugiah Souppaya, *Guide to Computer Security Log Management*, NIST (Sept. 2006), https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf [https://perma.cc/SF4A-S9AX].

[282] CRYSTAL PANEK, SECURITY FUNDAMENTALS 33–109 (2019).

even stop an attack in progress, allowing the organization to decide how to proceed under the given circumstances.[283] However, having logs and enabling accounting is less useful if an analysis of the information is not conducted or acted upon.[284] For example, if an employee downloads documents containing trade secrets, an alert may be generated depending on the settings. However, these alerts should reasonably be acted upon, and emergency alerts may be set for suspicious activity so that action can be taken as needed.

In *WalkMe Ltd. v. Whatfix, Inc.*, "operational controls that monitor and record usage" of the platform were considered part of the alleged reasonable measures taken, in part, to establish a trade secret's existence.[285] Likewise, in *Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC*, the audit log records maintained for information systems were sufficiently pled as reasonable measures, among others.[286]

Holders of digital trade secrets should implement logging and accounting measures and conduct a reasonable review of these in line with the trade secret's value and where it is stored. For example, periodic review for anomalies or events can provide a way for digital trade secret holders to monitor their systems and security. It can also help to disclose cybersecurity incidents after they have taken place, which, while not ideal, can still help to counter future incidents.

h. Cloud Storage and Third-Party Cloud Services

Digital trade secrets in marketing are commonly stored in the cloud. For example, various providers offer

[283] Kent & Souppaya, *supra* note 281.
[284] *Id.*
[285] WalkMe Ltd. v. Whatfix, Inc., No. 23-cv-03991-JSW, 2024 U.S. Dist. LEXIS 120331, at *7 (N.D. Cal. July 9, 2024).
[286] Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC, 22 CVS 4285, 2024 NCBC 46, 166 (N.C. Super. Ct. 2024).

cloud-based services such as Salesforce Marketing Cloud,[287] Oracle Marketing,[288] HubSpot CRM,[289] Google Marketing Platform,[290] and many others, which can be used for a variety of dedicated marketing purposes—some of which may include trade secrets. Also, digital trade secret holders may use cloud services such as Microsoft Azure,[291] Dropbox,[292] Google Cloud,[293] and Amazon Web Services (AWS),[294] among many others, to store such secrets (as opposed to, for example, computers and servers on the premises of the organization or elsewhere). Many such services provide a level of security as outlined in their marketing materials and service level agreements (SLAs), essentially transferring some or much of the security responsibility to the provider.

However, it is important to understand that services in the cloud may be provided through different service models, including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS).[295] SaaS is a common method of providing software via the cloud, as opposed to, for example, software installed

---

[287] *Marketing*, SALESFORCE, https://www.salesforce.com/marketing/ [https://perma.cc/5E6G-RCC7].
[288] *Oracle Marketing*, ORACLE, https://www.oracle.com/cx/marketing/ [https://perma.cc/EM5M-8Z3R].
[289] *Free CRM Software & Tools for Your Whole Team*, HUBSPOT, https://www.hubspot.com/products/crm [https://perma.cc/4GPW-Q8DQ].
[290] *Google Marketing Platform*, GOOGLE, https://marketingplatform.google.com/about/ [https://perma.cc/4V66-WK44].
[291] *Storage*, MICROSOFT, https://azure.microsoft.com/en-us/products/category/storage [https://perma.cc/6FX9-REU4].
[292] DROPBOX, https://www.dropbox.com/ [https://perma.cc/E778-R2N7].
[293] *Cloud Storage*, GOOGLE, https://cloud.google.com/storage [https://perma.cc/346G-D3XB].
[294] *Cloud Storage on AWS*, AMAZON WEB SERVICE, https://aws.amazon.com/products/storage/ [https://perma.cc/LX47-F5MS].
[295] *What is Cloud Architecture?*, *supra* note 92.

locally on a computer.[296] SaaS is a very popular method of providing marketing platforms, communication software, and other relevant software-based services to marketers.[297] PaaS permits access to necessary tools in the cloud to develop, run, and manage applications.[298] IaaS provides infrastructure, such as servers, storage, and networking through the cloud, helping to avoid the need to purchase such infrastructure.[299]

There are also various types of cloud architecture, including a public cloud, which is shared amongst customer organizations.[300] Alternatively, trade secret holders may contract a private cloud, which is dedicated to a customer organization, although usually at a much higher cost, with the potential for (but not guarantee of) enhanced security due to its private nature.[301] A hybrid cloud is a mix of the above architectures, offering certain benefits and drawbacks from the different architectures.[302] For example, organizations may select certain services to be contracted through public cloud services while maintaining their own physical servers on their premises and deciding where to store what information.[303] Practically, many organizations will commonly employ different architectures and even employ what is known as a multi-cloud environment, utilizing the cloud services of various organizations.[304]

---

[296] *Id.*
[297] *Google Marketing Platform*, *supra* note 290.
[298] *What is Cloud Architecture?*, *supra* note 92.
[299] *Id.*
[300] *Id.*
[301] *Id.*
[302] *Id.*
[303] *What is a Hybrid Cloud?*, MICROSOFT, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-hybrid-cloud-computing [https://perma.cc/S2FB-C94H].
[304] *Id.*; Satish Govindappa, *Secrets of Securing Intellectual Property (IP) in the Cloud*, CLOUD SEC. ALL. (Aug. 8, 2023), https://cloudsecurityalliance.org/blog/2023/08/08/secrets-of-

It is not accurate to generally label cloud use or storage as secure or insecure.[305] Each of these service models and types of architecture raises different security and legal considerations.[306] For example, SaaS, which might include eligible customer lists or other trade secrets, must be protected against loss or theft of data, unauthorized access, malware, and a number of other threats and risks.[307] There may be varying levels of security employed, with responsibilities assigned to different parties and interactions occurring with or through different systems. For example, some SaaS providers will contractually take on key security responsibilities, and the software service may include specific security services, such as updates for security vulnerabilities, to help keep the service secure.[308] However, accessing cloud services through insecure devices can result in a lapse in security, even if the cloud service employs a reasonable level of security.

Courts have considered cloud services and storage in trade secret settings. In *ResMan, LLC v. Karya Prop. Mgmt., LLC*, the information in question was stored in Microsoft

---

securing-intellectual-property-ip-in-the-cloud [https://perma.cc/FM93-EK5T].

305 *The Top 10 Cloud Myths*, GARTNER (Nov, 5, 2019), https://www.gartner.com/smarterwithgartner/the-top-10-cloud-myths [https://perma.cc/YBH3-46J5].

306 *What is Cloud Architecture?*, *supra* note 92; Sachdev, *supra* note 94; PREETI MISHRA ET AL., *supra* note 94, at 21–22.

307 Ejona Preçi & Peter H. Gregory, *SaaS Security Risk and Challenges*, ISACA (July 26, 2022), https://www.isaca.org/resources/news-and-trends/industry-news/2022/saas-security-risk-and-challenges [https://perma.cc/CAE3-PQZR]; *Get Ready for Today’s SaaS Explosion*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/network-security/saas-security [https://perma.cc/6MHT-HJFX].

308 H. Ward Classen*, SaaS Agreements: Key Contractual Provisions*, AM. BAR ASSOC. (Nov. 2, 2021), https://businesslawtoday.org/2021/11/saas-agreements-key-contractual-provisions/ [https://perma.cc/JRM6-VKCJ].

Azure's Cloud architecture, which has various certifications and is subject to various security and other measures under its contractual offering. The court considered this to be sufficiently reasonable, among a host of other measures.[309] In *Wwmap, LLC v. Midwifery*, the court decided that reasonable measures were sufficiently pled, which included "storage of the trade secrets in secure accounts—not accessible to the general public—with third-party service providers such as HubSpot, American Esoteric Laboratories, Quickbooks, and Poynt."[310] In *Harley Marine NY, Inc. v. Moore,* allegations that the information was in a password-protected Dropbox account were considered sufficiently pled alongside other measures taken.[311] However, in some instances, others go further. The plaintiff in *Corp. Synergies Grp., LLC v. Andrews* prohibits the use of public cloud storage, such as Dropbox, and instead keeps its confidential information on password-protected servers and devices that can only be accessed using appropriate credentials.[312]

However, in *PPEX v. Buttonwood, Inc.*, discussed above, a customer list was stored on PPEX's Mailchimp® account, a cloud service that provides email and other marketing services[313] and uses application-layer security, along with multifactor authentication.[314] While such measures might normally be considered a part of cybersecurity efforts leading to reasonable measures, the

---

309 ResMan, LLC v. Karya Prop. Mgmt., LLC, No. 4:19-CV-00402, 2021 U.S. Dist. LEXIS 145462, at *16 (E.D. Tex. Aug. 4, 2021).
310 Wwmap, LLC v. Midwifery, 711 F. Supp. 3d 1313, 1322 (N.D. Fla. 2024).
311 Harley Marine NY, Inc. v. Moore, 716 F. Supp. 3d 21, 29 (N.D.N.Y. 2024).
312 Corp. Synergies Grp., LLC v. Andrews, No. 18-13381, 2019 U.S. Dist. LEXIS 135293, at *9 (D.N.J. Aug. 12, 2019).
313 INTUITMAILCHIMP, https://mailchimp.com/ [https://perma.cc/A26Z-9YUP].
314 PPEX v. Buttonwood, Inc., No. 21-CV-53-F, 2021 U.S. Dist. LEXIS 254584, at *8 (D. Wyo. Sept. 7, 2021).

court, in declining a preliminary injunction, reasoned that "PPEX does not point to *any* step it took to inform its employees . . . that the Customer and Supplier Lists were trade secrets."[315] Thus, trade secret holders may consider digitally marking, as discussed in subsection ii above, or providing training on trade secrets beyond the cloud security measures available or employed. Further, under Puerto Rico's version of the UTSA, the District Court for the District of Puerto Rico, using a "short cost-benefit analysis," found that the alleged trade secret holder "used only the basic default settings on Dropbox, but the Dropbox enables further protections that went unused."[316]

Not all digital trade secrets held by marketers will need to employ the most secure versions of the cloud, only those deemed reasonable. Where needed, it is also possible to impose restrictions on the use of cloud services to store trade secrets, which may only be stored in specific locations, using specific cloud architectures, or with specific providers. These choices may be influenced by the types of trade secrets and the nature and frequency of access to them.

i. Human Oversight

Human oversight is the management of security systems and measures by one or more people with the relevant authority and/or duty.[317] Having human oversight of security measures has been cited by a court as a reasonable measure, among others, as seen in *ResMan, LLC v. Karya Prop. Mgmt., LLC*, where the Chief Technology Officers, "vice-presidents, [and] other executives" were responsible

---

[315] *Id.* at *29.
[316] TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo, No. 15-2121 (BJM), 2018 U.S. Dist. LEXIS 168546, at *51 (D.P.R. Sept. 28, 2018).
[317] *See* Sarah Sterz et al., *On the Quest for Effectiveness in Human Oversight: Interdisciplinary Perspectives*, FAccT '24 (June 5, 2024), https://dl.acm.org/doi/fullHtml/10.1145/3630106.3659051 [https://perma.cc/6BR7-JJ7L].

"to ensure that the security of the platform [was] up to par."[318] The level of human oversight will likely be required to be commensurate with where the digital trade secret is stored, the threats and vulnerabilities involved, and the value of the trade secret.

It remains to be seen how much further artificial intelligence (AI) may change the field of cybersecurity. However, as of now, human oversight appears to be an acceptable aspect of reasonable measures, whether or not AI is used.[319]

j. Cybersecurity and Other Training

Cybersecurity training may range from watching a video, taking a quiz,[320] annual training, tabletop exercises,[321] internal or external training,[322] or other "specialized training" requirements based on the "level of disclosure" to trade secrets.[323] Not only might such training be required, recommended, or optional, the difference in types and extent

---

[318] ResMan, LLC v. Karya Prop. Mgmt., LLC, No. 4:19-CV-00402, 2021 U.S. Dist. LEXIS 145462, at *17 (E.D. Tex. Aug. 4, 2021).

[319] *See* Robert Ackerman, *The Critical Intersection of AI and Cybersecurity is Moving Briskly*, RSA CONFERENCE (Sept. 5, 2024), https://www.rsaconference.com/library/blog/the-critical-intersection-of-ai-and-cybersecurity-is-moving-briskly [https://perma.cc/S8PE-EZ7U]; *What Is Generative AI in Cybersecurity?*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/generative-ai-in-cybersecurity [https://perma.cc/XJ32-QBNV].

[320] *Cybersecurity Quizzes*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz [https://perma.cc/FBV2-RBZ2].

[321] *Cybersecurity Tabletop Exercise Tips*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/sites/default/files/publications/Cybersecurity-Tabletop-Exercise-Tips_508c.pdf [https://perma.cc/4SCG-X29K].

[322] *Offer tailored cyber security training to your employees - ITSAP.10.093*, CAN. CENTRE CYBER SEC. (Sept. 2024), https://www.cyber.gc.ca/en/guidance/offer-tailored-cyber-security-training-your-employees-itsap10093 [https://perma.cc/J9TZ-RCVG].

[323] Candido et al., *supra* note 34.

of such training may be relevant to the implementation of reasonable measures.

In *Asset Planning Servs., Ltd. v. Halvorsen*, in the context of a motion to dismiss, the court described "training . . . on information security risks and responsibilities" as one of the many extensive steps taken to protect the trade secrets including "client lists . . . proprietary software . . . and . . . a curated compilation binder of benefits."[324] In *Capital One Fin. Corp. v. Sykes*, Capital One's confidential customer lists and information, marketing plan, and other materials, which defendants emailed to themselves, were the subject matter of a trade secret dispute in which a temporary restraining order and preliminary injunction were requested.[325] Subsequently, some of the customer list information was loaded onto the competitor's Hubspot account, which is a customer relationship management and marketing cloud-based service.[326] The court considered that "Capital One requires annual computer-based training on cybersecurity"[327] and "provides training to employees regarding their obligations to safeguard confidential information."[328] While the court did not reach the issue of reasonable measures, as it arrived at a conclusion regarding the requested injunction on a contract claim, it is important to note that the training referenced here went beyond cybersecurity-specific training and included training on obligations that may be considered as a measure for owners of digital trade secrets in marketing.[329]

[324] Asset Planning Servs., Ltd. v. Halvorsen, No. 21-2021, 2022 U.S. Dist. LEXIS 68073, at *2, *18 (E.D. Pa. Apr. 13, 2022).
[325] Capital One Fin. Corp. v. Sykes, No. 3:20cv763, 2021 U.S. Dist. LEXIS 128617, at *4, *9 (E.D. Va. July 9, 2021).
[326] *Id.* at *9, *20–21.
[327] *Id.* at *13.
[328] *Id.* at *27.
[329] *Id.*

Training employees, vendors, and others with access to digital trade secrets in marketing should be considered as a potential reasonable measure, as it helps to establish that the parties were aware of not only cybersecurity measures but also of their obligations. This should include training on "social engineering"[330] attacks to increase the likelihood of employees being alert to these types of scams.

k. Ongoing Risk Assessments

As Rowe and Sandeen recognize, it is crucial for holders of trade secrets to carefully assess risks, both internal and external.[331] A risk assessment is "[t]he process of identifying risks to organizational operations . . . resulting from the operation of an information system," such as those on which trade secrets may reside.[332] These may vary in nature, extent, or approach, though most involve analyzing potential threats or vulnerabilities and assessing current or future security measures.[333] In addition to the reasonable risk assessment alluded to when considering the three initial factors in this framework, an ongoing risk assessment is likely required.

In *Asset Planning Servs., Ltd. v. Halvorsen*, described as part of extensive steps sufficiently pled, the party engaged in "periodic risk assessments to identify cybersecurity threats and vulnerabilities."[334] Such

---

330 *Avoiding Social Engineering and Phishing Attacks*, *supra* note 141.
331 ROWE & SANDEEN, *supra* note 43, at 199.
332 *Risk Assessment*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/risk_assessment [https://perma.cc/LYN8-GGMH].
333 *See* Volkan Evrin, *Risk Assessment and Analysis Methods: Qualitative and Quantitative*, ISACA (Apr. 28, 2021), https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods [https://perma.cc/6UKZ-SFLN].
334 Asset Planning Servs., Ltd. v. Halvorsen, No. 21-2021, 2022 U.S. Dist. LEXIS 68073, at *2 (E.D. Pa. Apr. 13, 2022).

assessments should take place on a regular basis for digital trade secrets in marketing, not only when a major change in a system or another major event is planned. The extent of the risk assessment, while it can vary greatly, should be in line with the trade secrets held.

l. Physical Measures as Part of Cybersecurity Measures

Physical measures or physical security involve actions such as using traditional locks and keys for devices or servers containing digital trade secrets, restricting physical access to those requiring it, and implementing a system to track access.[335]

Courts have recognized that cybersecurity measures form part of what may be reasonable measures,[336] and in general, courts will look not only to agreements but also to "physical-or cyber-security protections."[337] However, in the field of cybersecurity, these are concepts that go hand in hand. In other words, cybersecurity begins with strong physical security, and physical measures that are taken should be a part of the overall cybersecurity measures.[338] Thus, "or" should not be used; instead, cybersecurity measures *and* related physical measures should be

[335] *See Trade Secrets*, *supra* note 17; *Physical Security*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/physical-security [https://perma.cc/ES6H-R92L].
[336] *See* Cloudera, Inc. v. Databricks, Inc., No. 21-cv-01217-HSG, 2021 U.S. Dist. LEXIS 164033, at *12 (N.D. Cal. Aug. 30, 2021).
[337] Core SWX, LLC v. Vitec Grp. US Holdings, Inc, No. 21-CV-1697 (JMA)(JMW), 2022 U.S. Dist. LEXIS 125198, at *21–22 (E.D.N.Y. July 14, 2022); Turret Labs USA, Inc. v. CargoSprint, LLC, No. 21-952, 2022 U.S. App. LEXIS 6070, at *11 (2d Cir. Mar. 9, 2022).

[338] *Physical Security*, *supra* note 335.

employed.[339] In *Charles Ramsey Co. v. Fabtech-NY LLC*, it was commented that "[m]ost courts in this Circuit look to contractual confidentiality agreements or physical security measures when determining whether a party took reasonable measures,"[340] and the amended complaint failed to plausibly allege the relevant measures.[341] Holders of digital trade secrets should employ physical safeguards where relevant to their cybersecurity posture.

m. Segmented and Segregated Networks

According to NIST, network segmentation involves breaking down a network into sub-networks and protecting them using various measures discussed elsewhere in this article, such as firewalls.[342] For example, if a threat is found in one sub-network, measures may be taken to isolate it, even if there may be some potential for it to affect another sub-network.[343] The Cybersecurity & Infrastructure Security Agency (CISA) states that segmentation provides limited access to "devices, data, and applications and restricts communications between networks."[344] Sometimes a Demilitarized Zone (DMZ) is necessary, which "is a physical or logical subnet that separates a local area network

---

339 *See Core SWX, LLC*, 2022 U.S. Dist. LEXIS 125198, at *21; *Turret Labs USA, Inc.*, 2021 U.S. Dist. LEXIS 27838, at *11.

340 Charles Ramsey Co. v. Fabtech-NY LLC, No. 1:18-CV-0546 (LEK/CFH), 2020 U.S. Dist. LEXIS 9348, at *42 (N.D.N.Y. Jan. 21, 2020).

341 *Id.* at *45.

342 *Network Segmentation*, NAT'L INST. OF STANDARDS AND TECH., https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary#N [https://perma.cc/G6GG-EP2G].

343 *See id.*

344 *Layering Network Security Through Segmentation*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY (Jan. 2022), https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf [https://perma.cc/XX39-T7XN].

from other untrusted networks.”[345] This can help prevent access by a bad actor to high-value assets by shielding the network from unauthorized access, such as digital trade secrets.[346] Relatedly, network segregation involves the configuration of a network into separate parts.[347] In some cases, it may be prudent to isolate trade secrets into specific sub-networks, and when employing these network security mechanisms, digital trade secrets may be further protected.

n. Hardware, Connectivity, and Device Restrictions

Hardware such as USB drives or external hard drives may be used to store, transport, and even steal trade secrets.[348] As Cundiff and others recognize, limiting digital-storage media may be one way to protect trade secrets.[349] In *Progress Eng’g, LLC v. Bennett*, it was alleged that “employees are not permitted to store technical or customer data on any external devices.”[350] In *Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC*, “[r]emovable media management including restricted use of external hard drives and USB drives to, in part, prevent exfiltration of confidential information” was part of various measures considered sufficiently pled as reasonable measures.[351]

In some cases, “very strict access control” on hardware “(e.g., no USB devices allowed, no other connectivity enabling data transfers like Bluetooth)” may be

[345] *Id.*
[346] *Id.*
[347] MICROSOFT, https://learn.microsoft.com/en-us/platform-engineering/playbook/capabilities/network/network-segregation [https://perma.cc/3RG3-YQZM].
[348] *See Portable Storage Device*, *supra* note 36.
[349] Cundiff, *supra* note 5, at 369.
[350] Progress Eng’g, LLC v. Bennett, No. 1:22-cv-00257-LEW, 2022 U.S. Dist. LEXIS 200166, at *6 (D. Me. Nov. 3, 2022).
[351] Rel. Ins., Inc. v. Pilot Risk Mgmt. Consulting, LLC, 22 CVS 4285, 2024 NCBC 46, 166 (N.C. Super. Ct. 2024).

appropriate.[352] Further, connectivity restrictions may be put in place, such as keeping trade secrets on computers that do not have internet access.[353] However, this will not always be practicable, as the trade secrets will need to be regularly accessed for purposes such as managing customer lists and accounts.

Additionally, cybersecurity is as strong as the "weakest link."[354] It is important, therefore, to consider that an unsecure device, such as a personal device or a company device connected to an insecure network, may pose a risk. Measures should be put into place to implement secure procedures or policies regarding these types of instances.[355] Notably, trade secrets are "only as secure as the devices used for storage and access."[356]

o. Security by Design

Digital trade secrets may be stored on, used through, or transmitted from devices and technological products. In the field of cybersecurity, the concept of "secure by design" involves building cybersecurity "into the design and manufacture of technology products."[357] For example, it is

---

[352] *Trade Secrets and Digital Objects*, *supra* note 15.
[353] *See* Cundiff, *supra* note 5; *Trade Secrets and Digital Objects*, *supra* note 15.
[354] Glait Klein & Moti Zwillinig, *Weakest Link: Employee Cyber-Defense Behaviors While Working from Home.* 64 J. COMPUTER INFO. SYS. 3, 408–22 (June 26, 2023), https://doi.org/10.1080/08874417.2023.2221200 [https://perma.cc/VXT8-YVJC]; Julie Haney, *Cybersecurity Awareness Month: Securing Devices at Home and Work*, NAT'L INST. OF STANDARDS AND TECH. (Oct. 13, 2020), https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-awareness-month-securing-devices-home-and-work [https://perma.cc/4BYE-Y7QW].
[355] *Id.*
[356] ALMELING & SNYDER, *supra* note 135.
[357] *Secure by Design*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/securebydesign [https://perma.cc/R39W-KZ5A].

not an add on feature; rather, it is a way of thinking about the design from the beginning, which should allow for more secure technology products.[358] Some methods that may be employed in "secure by design" include secure by default mechanisms, such as when a certain level of security is already employed into the technological product. For example, secure configurations that the customer does not need to complete.[359]

Another method is to avoid using default passwords, where the device manufacturer equips all the devices with the same password and requires the customer to change it. Often, customers will create passwords that open a potential avenue for attackers to gain access.[360] Relatedly, privacy by design principles may be employed to provide some key benefits.[361] Some of these are now considered aspects of security, such as end-to-end security, recognizing that there is some overlap between security and "privacy by design" principles.[362]

Likewise, in the context of software used by organizations, security by design may be implemented into the software design.[363] Where trade secrets in marketing are

---

[358] *Id.*
[359] *See id.*; *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by Design and -Default*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf [https://perma.cc/SCD6-2AK9].
[360] *Id.*
[361] *See* Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*, https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf [https://perma.cc/2DW9-6VBQ].
[362] *Id.*; *Secure by Design*, *supra* note 357; *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by Design and -Default*, *supra* note 359; Cavoukian, *supra* note 361.
[363] *See generally Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by Design and -Default*, *supra* note 359.

held on devices and technological products, which employ security by design, such measures may be argued to be part of reasonable measures taken.[364]

p. Security Contracts and Policies

It is well known that NDAs and confidentiality agreements provide some basis for the implementation of reasonable measures.[365] Incorporating provisions pertaining to cybersecurity may be helpful. For example, employees promising to keep trade secrets secure might provide an added measure. In *Tanium Inc. v. Yago*, an employee agreed that they "w[ould] use reasonable care to protect the confidentiality and security of Proprietary Information and use Proprietary Information only as necessary and [was] authorized to perform . . . duties as an employee of Company."[366] This went beyond mere confidentiality and incorporated security obligations.

Organizations may also create and implement various policies that pertain to cybersecurity. These may cover specific security rules, measures, or obligations and should be put into place to manage the risk associated with digital trade secrets. These should include "storage, retention, and disposal policies"[367] for digital trade secrets. These policies may be incorporated into employment agreements, confidentiality agreements, or NDAs. One court noted that "[e]specially in the digital age, where electronic information is always vulnerable, lacking clear

---

[364] *Id.*
[365] ResMan, LLC v. Karya Prop. Mgmt., LLC, No. 4:19-CV-00402, 2021 U.S. Dist. LEXIS 145462, at *17 (E.D. Tex. Aug. 4, 2021).
[366] Tanium Inc. v. Yago, No. 1:21-CV-1867-MHC, 2019 U.S. Dist. LEXIS 240245, at *8 (N.D. Ga. July 28, 2021).
[367] *Safeguard Your Company's Intellectual Property*, SHRED-IT (Oct. 19, 2021), https://www.shredit.com/en-us/blog/how-to-safeguard-your-companys-trade-secrets [https://perma.cc/TJ4P-M5ES].

policies on confidential information, technology, and digital security is unreasonable."[368]

In *Comet Techs. USA Inc. v. Beuerman*, the court found reasonable measures because the "[p]laintiff ha[d] taken a number of steps to keep the information at issue secret, including requiring employees to sign non-disclosure agreements . . . and establishing internal policies that prohibit[ed] using third party data storage for company information and require[d] high quality passwords."[369] In *Legend Biotech USA Inc. v. Liu*, employees agreed to "confidentiality obligations, a code of conduct, a data protection policy, a data handling policy, and media retention and destruction policies as a condition of their employment."[370] Further, upon termination of the defendant's employment, the defendant agreed to comply with "the Record Management Policy, the Global Data Privacy Policy, the Global Data Handling and Classification Policy, and the Data Handling and Classification Standard Operating Procedures "[371] Further, such policies and agreements, which "implemented contractual controls" for its employees "to limit their use and authorization to use Plaintiff's information beyond that which is necessary for their job duties," were considered—along with other measures—as evidence that the Plaintiff had taken reasonable steps.[372] However, in *Farmers Edge Inc. v. Farmobile*, it was confirmed that reasonable measures were not taken because the party "shared the information with a third-party contractor without a confidentiality

[368] TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo, No. 15-2121 (BJM), 2018 U.S. Dist. LEXIS 168546, at *52 (D.P.R. Sept. 28, 2018).
[369] Comet Techs. USA Inc. v. Beuerman, No. 18-CV-01441-LHK, 2018 U.S. Dist. LEXIS 224356, at *8 (N.D. Cal. Mar. 15, 2018).
[370] Legend Biotech USA Inc. v. Liu, No. 2:23-cv-02965-BRM-LDW, 2024 U.S. Dist. LEXIS 37012, at *2 (D.N.J. Mar. 4, 2024).
[371] *Id.* at *7.
[372] *Id.*

agreement and without other policies or practices for safeguarding secrets."[373] At the same time, a court may decide, as the Norther District of California did, that even though not all employees signed a confidentiality agreement with respect to source code for a video game, those who did not "nonetheless understood the source code to be confidential business information."[374]

Policies related to cybersecurity might specifically address specific jobs or roles, including both internal and external persons where relevant. Digital trade secrets should be explicitly mentioned in such policies, and, alongside other measures considered, help to establish reasonable measures.

q. Secure Destruction of Digital Copies

As with traditional "photocopies of confidential documents,"[375] it is important to securely destroy or delete the information. For example, copies of trade secrets may be required for reasonable business purposes with reasonable measures in place to protect that information. If not required, copies should, of course, not be made. If made, wherever this information is stored—whether on a particular device, media, or in the cloud—any copies should be deleted immediately following their intended use, in a way that prevents the copy from being retrieved. For example, if a file is deleted from a device or cloud service, it may end up in another folder or storage location, and measures should be taken to permanently delete it.[376]

---

[373] Farmers Edge Inc. v. Farmobile, LLC, 970 F.3d 1027, 1033 (8th Cir. 2020).
[374] 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.04; *see* Lilith Games (Shanghai) Co. v. uCool, Inc., No. 15-CV-01267-SC, 2015 U.S. Dist. LEXIS 128619, at *29 (N.D. Cal. Sept. 23, 2015).
[375] PETER S. MENELL ET AL., *supra* note 1, at 11-8.
[376] *Effectively Erasing Files*, CISA, https://www.cisa.gov/news-events/news/effectively-erasing-files [https://perma.cc/5X8C-XYWU]; *Deleting your data from computers, laptops and other devices*, ICO,

r. Generative AI Restrictions

A key form of GenAI today includes machine-learning models that can "learn to make a prediction based on data."[377] These may include OpenAI's ChatGPT[378] and Google Gemini[379] for chat-based AI, Stable Diffusion[380] or Dall▪E 2[381] for image creation, and Pika[382] for generative videos, among many others.

Organizations should exercise caution with the use of GenAI within their organization or by their employees, especially regarding trade secret information.[383] For example, organizations could "inadvertently give away trade secrets or waive confidentiality on commercially sensitive information if such information is used for prompting or training AI tools."[384] Due to the potential for "considerable differences in the terms on which developers are licensing their AI tools, including the approach to trade secrets and other confidential information, the ownership of outputs, . . . and obligations on users to mitigate risks through the implementation of staff monitoring and training," digital

---

https://ico.org.uk/for-the-public/online/deleting-your-data-from-computers-laptops-and-other-devices/ [https://perma.cc/8ABR-HUUG].

377 Adam Zewe, *Explained: Generative AI: How Do Powerful Generative AI Systems Like ChatGPT Work, and What Makes Them Different From Other Types of Artificial Intelligence?*, MIT NEWS (Nov. 9, 2023), https://news.mit.edu/2023/explained-generative-ai-1109 [https://perma.cc/9YKJ-JKXW].

378 CHATGPT, https://openai.com/chatgpt/ [https://perma.cc/9GQG-9ECK].

379 GOOGLE GEMINI, https://gemini.google.com/ [https://perma.cc/TGJ5-4QVJ].

380 STABLE DIFFUSION ONLINE, https://stablediffusionweb.com/ [https://perma.cc/EYR8-HYCQ].

381 OPENAI, *DALL▪E 2*, https://openai.com/index/dall-e-2/ [https://perma.cc/S8LK-GWZB].

382 PIKA, https://pika.art/home [https://perma.cc/8GUE-MU9U].

383 *See Trade Secrets and Digital Objects*, *supra* note 15.

384 *Generative AI: Navigating Intellectual Property*, *supra* note 11.

trade secret holders should implement technical and policy measures to prevent their trade secrets from entering generative AI systems without careful analysis.[385]

It should be noted that some generative AI systems may not use data input into prompts for training, while others do.[386] Some organizations have policies against using generative AI with certain information, and this appears to contribute to reasonable measures with respect to trade secrets, especially in cases where there is a risk of exposure.[387]

C. Cybersecurity Standards, Frameworks, Best Practices, Industry Standards, and Industry Regulation

Various organizations create, publish, or disseminate cybersecurity standards, frameworks, best practices, guidance, or other similar documents. These are also important to assess certain digital trade secrets. It is unlikely that a low-value digital trade secret for a very small business would be required to comply with formal standards or frameworks designed for larger organizations, but it would still need to follow reasonable cybersecurity practices. However, for medium- and high-value trade secrets,

---

385 *Id.*

386 *See* Gonzalo Martínez et al., *Towards Understanding the Interplay of Generative Artificial Intelligence and the Internet*, *in* 14523 EPISTEMIC UNCERTAINTY IN ARTIFICIAL INTELLIGENCE 59–73 (Fabio Cuzzolin & Maryam Sultana eds., 2024); Lauren Leffer, *Your Personal Information is Probably Being Used to Train Generative AI Models*, SCI. AM. (Oct. 19, 2023), https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/ [https://perma.cc/P3RX-BQF9].

387 *See Privacy Considerations for Generative AI*, UNIV. OF ILL. URBANA-CHAMPAIGN, https://cybersecurity.illinois.edu/policies-governance/privacy-considerations-for-generative-ai/ [https://perma.cc/V7WZ-J245].

depending on how and where they are stored, and who or what may want access, these standards, frameworks, best practices, industry standards or practices,[388] and industry regulations may be important or relevant. In this regard, "expert testimony respecting measures used in the industry has been admitted on the reasonable measures question."[389]

For example, the NIST,[390] the International Organization for Standardization (ISO),[391] and the Cloud Security Alliance (CSA),[392] among others, offer such standards and frameworks. Some specific examples include The NIST Cybersecurity Framework (CSF) 2.0,[393] ISO/IEC 27001:2022,[394] and the CSA Cloud Controls Matrix (CCM).[395] A number of such mechanisms can be used by organizations to meet the standards or recommended practices of such organizations. However, they could also argue that implementing, complying with, or otherwise adhering to such standards meets reasonable measures.

---

388 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.01; Fmc Techs. v. Murphy, 679 S.W.3d 788, 811 (Tex. App. 2023); Neural Magic, Inc. v. Meta Platforms, Inc., 659 F. Supp. 3d 138, 151 (D. Mass. 2023).

389 *Id.*

390 NAT'L INST. OF STANDARDS AND TECH., https://www.nist.gov/ [https://perma.cc/H7V5-RDQF].

391 INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/home.html [https://perma.cc/83JH-4Z6J].

392 CLOUD SEC. ALLIANCE, https://cloudsecurityalliance.org/ [https://perma.cc/3EBG-MLPB] (In full disclosure, author proposed and created the Legal Control in the Cloud Security Alliance IoT Security Controls Framework Version 2).

393 *The NIST Cybersecurity Framework (CSF) 2.0*, NAT'L INST. OF STANDARDS AND TECH. (Feb. 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf [https://perma.cc/6VYY-K3DF].

394 INT'L ORG. FOR STANDARDIZATION, *supra* note 391.

395 *Cloud Controls Matrix (CCM)*, CLOUD SEC. ALL., https://cloudsecurityalliance.org/research/cloud-controls-matrix [https://perma.cc/4B63-NU5Q].

In fact, some courts may look to, or parties may argue that they implement at least what others—such as competitors or industry participants—implement to protect similar trade secrets. In some cases, organizations in certain industries have specific legal obligations, such as requiring the protection of personally identifiable information (PII), which may be traced back to a specific person or individual.[396] For example, under the *Health Insurance Portability and Accountability Act* (HIPAA), the HIPAA Security Rule "requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[397] It will be interesting to see whether, in the context of digital trade secrets, industry specific PII requirements may play an important role in informing reasonable measures in the digital trade secret context, even if not stemming from the same requirement. In *Houser v. Feldman*, it was found to be sufficiently pled, among other measures taken, that the plaintiff alleged adherence to industry-standard protocols recommended by the National Institutes of Health.[398]

While the court focused on the contractual claims to largely base its granted injunction, in *Capital One Fin. Corp. v. Sykes*, an expert witness testified that "Capital One, in line with industry standards, takes reasonable steps to maintain the secrecy" with respect to customer lists and other information.[399] However, in *Proofpoint, Inc. v. Vade Secure, Inc.*, an important question was raised as to whether "best

---

[396] *Personally Identifiable Information*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/personally_identifiable_information [https://perma.cc/5GQE-A6ZE].
[397] *The Security Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/index.html [https://perma.cc/QKN2-NH2Y].
[398] Houser v. Feldman, 569 F. Supp. 3d 216, 230 (E.D. Pa. 2021).
[399] Capital One Fin. Corp. v. Sykes, No. 3:20cv763, 2021 U.S. Dist. LEXIS 128617, at *26 (E.D. Va. July 9, 2021).

practices" was the correct standard to use to assess reasonable measures.[400] One of the defendant's expert witnesses reported that the plaintiffs did not employ what was called "best practices," and the plaintiffs argued that this was a much higher standard than "reasonable measures," seeking to exclude the expert's testimony.[401] However, in denying this request, the court found that the expert witness opined that best practices are "quite certainly a step above reasonable measures."[402] While the Court did not itself delve deeply into this consideration, it is important to note that the terminology of best practices, if employed, might be argued to exceed the requirement of reasonable measures.[403]

However, in the cybersecurity industry, the phrase "best practices," at times, might actually be used to describe "basic measures".[404] Although the latter may sometimes be akin to "reasonable measures," it is not always the case, depending on the type of trade secret, its value, and other factors. For example, CISA describes on a page dedicated to cybersecurity best practices that, while "[i]mplementing safe cybersecurity best practices is important for individuals as well as organizations of all sizes," they outline that "[u]sing strong passwords, updating your software, thinking before you click on suspicious links, and turning on multi-factor authentication are the basics" of what is termed "cyber hygiene," which will "drastically improve your online safety."[405] These, as recognized, seem to be covered under

---

[400] Proofpoint, Inc. v. Vade Secure, Inc., No. 19-cv-04238-MMC, 2021 U.S. Dist. LEXIS 118313, at *4 (N.D. Cal. June 24, 2021).
[401] *Id.*
[402] *Id.* at *5.
[403] *Id.*
[404] *Cybersecurity Best Practices*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cybersecurity-best-practices [https://perma.cc/E5SC-9PFU].
[405] *Id.*

best practices but are actually the basics.[406] Therefore, it is important to watch the use of terminology carefully in legal settings, such as in trade secret litigation, as its distinct legal meaning may differ from the technical one. CISA further opines that "developing and implementing tailored cybersecurity plans and processes is key to protecting and maintaining business operations."[407] Therefore, what may be reasonable for one organization or type of trade secret may not be reasonable for another.

D. Limitations and Flexibility

As with any technology-based assessments, the specific cybersecurity measures that are expected to meet the "reasonable measures" requirement will evolve as technology evolves. Likewise, if there is a serious departure from how the law or the courts might treat the "reasonable measures" requirement, or if key methods in assessing it evolves, there will be a need to update the framework.

However, the model is flexible to adapt to changing technological and legal environments. Key cybersecurity measures shown may be adapted based on nuances and changes within the measure. The discussion on any one specific measure does not incorporate all possible inclusions. For example, the discussions of firewalls or VPNs do not cover all possible firewalls or VPN types and are flexible enough to consider any that might fall under these, including those not yet developed.

VI. CONCLUSION

As technological advances provide new ways of using, storing, and managing digital trade secrets, and as new and emerging threats challenge the notions of cybersecurity

[406] *Id.*
[407] *Id.*

in an increasingly digital world, the subject matter of this article is necessarily evolving.

Digital trade secrets in marketing may include a variety of information, and technology plays an increasing role in their storage, use, and management. Inevitably, trade secrets will be stored in digital means, and their loss could result in a substantial impact on a brand or organization. There are many potential bad actors seeking to profit from digital trade secrets, along with the possibility of errors or careless mistakes that could result in their loss. A variety of factors also impact trade secrets, and there is no single solution that may be employed to address trade secrets broadly.

It is the duty of those who wish to maintain trade secrets falling under the DTSA or state law to employ reasonable measures or their equivalent. This is not well defined, nor is adequate guidance provided to interpret it.[408] There also appears to be a harmonious yet confused relationship between trade secret law and cybersecurity. While it is clear that cybersecurity measures are required in a digital setting, it is argued that various specific technical factors play, or should further play, a key role in establishing whether the required level of measures are met.

The Reasonable [Cybersecurity] Measures Framework provides a basis from which courts can better assess reasonable measures from the perspective of cybersecurity measures. It is argued that this framework provides a systematic method for courts to analyze reasonable cybersecurity measures and fills the gap of applying a broad brush. It also recognizes the role of experts in the analysis. Further, the framework may be used by judges to instruct a jury. Practitioners and organizations may find the framework useful to consider when addressing

[408] *See* Turret Labs USA, Inc. v. CargoSprint, LLC, No. 21-952, 2022 U.S. App. LEXIS 6070, at *4–5 (2d Cir. Mar. 9, 2022).

cybersecurity for trade secrets or in the process of litigation. Scholars may find the framework useful to their research, and faculty may find this article supportive of teaching this topic in trade secrets.

The framework sets the stage by recommending an assessment of key initial considerations, based on which specific cybersecurity measures may be considered by courts. These specific cybersecurity measures include various technical considerations to differentiate between a broad reference to a cybersecurity measure and to help understand some of the technical aspects that should be considered. Specifically, a number of cybersecurity measures were discussed, including how courts have engaged with many of these—either accepting, rejecting, or conditioning their implementation on other measures. While some measures have regularly been recognized by the courts, such as password protection,[409] VPNs,[410] and agreements,[411] among others, it is argued that, where not already considered, courts should further examine technical aspects of all cybersecurity measures to determine whether they are reasonable. In essence, blanket assumptions about password protection, cloud security, or other measures is argued to not be sufficient to establish reasonable measures, even if it may potentially be sufficient at the pleadings stage. Following these specific measures, where relevant, cybersecurity standards, frameworks, and other factors may be considered.

---

[409] Houser v. Feldman, 569 F. Supp. 3d 216, 221 (E.D. Pa. 2021); Iacovacci v. Brevet Holdings, Ltd. Liab. Co., 437 F. Supp. 3d 367, 381 (S.D.N.Y. 2020).

[410] Brown & Root Indus. Servs., LLC v. Brown, No. 21-291-JWD-SDJ, 2022 U.S. Dist. LEXIS 174537, at *23 (M.D. La. Sept. 9, 2022); Hedgeye Risk Mgmt., LLC v. Dale, No. 21-cv-3687 (ALC)(RWL), 2023 U.S. Dist. LEXIS 177181, at *20 (S.D.N.Y. Sept. 29, 2023).

[411] Charles Ramsey Co. v. Fabtech-NY LLC, No. 1:18-CV-0546 (LEK/CFH), 2020 U.S. Dist. LEXIS 9348, at *42 (N.D.N.Y. Jan. 21, 2020).

It is hoped that this article will be informative in marrying legal concepts with technical cybersecurity concepts for those engaging with matters pertaining to any digital trade secrets through lessons from marketing.