The Sedona Conference Journal

Volume 24 2023

The Sedona Conference Commentary on the Governance and Management of Trade Secrets

The Sedona Conference

Recommended Citation:

The Sedona Conference, *Commentary on the Governance and Management of Trade Secrets*, 24 SEDONA CONF. J. 429 (2023).

For this and additional publications see: https://thesedonaconference.org/publications.

THE SEDONA CONFERENCE COMMENTARY ON THE GOVERNANCE AND MANAGEMENT OF TRADE SECRETS

A Project of The Sedona Conference Working Group 12 on Trade Secrets

Author:

The Sedona Conference

Editors-in-Chief:

James Pooley Victoria Cundiff

Managing Editors:

Jim W. Ko Casey Mangan

Senior Editors:

Nicole D. Galli
Elizabeth McBride
Jennifer Lynn Miller

Contributing Editors:

Cassius A. Elston
David Prange
Nicholas Steele

Staff Editor:

David Lumia

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference's Working Group 12. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any organizations to which they may

belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *Commentary on the Governance and Management of Trade Secrets*, 24 SEDONA CONF. J. 429 (2023).

PREFACE

Welcome to the July 2023, Final, Post-Public Comment Version of *The Sedona Conference Commentary on the Governance and Management of Trade Secrets*, a project of The Sedona Conference Working Group 12 on Trade Secret Law (WG12). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG12, formed in February 2018, is "to develop consensus and nonpartisan principles for managing trade secret litigation and well-vetted guidelines for consideration in protecting trade secrets, recognizing that every organization has and uses trade secrets, that trade secret disputes frequently intersect with other important public policies such as employee mobility and international trade, and that trade secret disputes are litigated in both state and federal courts." The Working Group consists of members representing all stakeholders in trade secret law and litigation.

The WG12 *Commentary* drafting team was launched in November 2018. Earlier drafts of this publication were a focus of dialogue at The Sedona Conference on Trade Secrets in Denver, Colorado, in May 2022, The Sedona Conference WG12 Annual Meeting 2021, in Phoenix, Arizona, in December, 2021, the WG12 Annual Meeting, Online, in November 2020, the WG12 Annual Meeting in Charlotte, North Carolina, in November 2019, and the WG12 Inaugural Meeting in Los Angeles, California, in November 2018. The editors have reviewed the comments received through the Working Group Series review and comment process.

This *Commentary* represents the collective efforts of many individual contributors. On behalf of The Sedona Conference, I thank in particular James Pooley, the Chair Emeritus of WG12, and Victoria Cundiff, the Chair of WG12, who serve as the Editors-in-Chief of this publication, and Nicole D. Galli, Elizabeth McBride, and Jennifer Lynn Miller, who serve as the Senior Editors of this publication. I also thank everyone else involved for their time and attention during this extensive drafting and editing process, including our Contributing Editors Cassius A. Elston and David Prange, and also Nicholas Steele.

The drafting process for this *Commentary* has also been supported by the Working Group 12 Steering Committee and Judicial Advisors. The statements in this *Commentary* are solely those of the nonjudicial members of the Working Group; they do not represent any judicial endorsement of any recommended practices.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG12 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, data security and privacy liability, patent remedies and damages, and patent litigation best practices. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

Craig W. Weinlein
Executive Director
The Sedona Conference
July 2023

TABLE OF CONTENTS

FOREWORD

This *Commentary* was written from both legal and business perspectives as a useful reference for the design and implementation of trade secret governance and protection programs in corporate environments. It can also provide insight to litigators and judges about the practical ways companies approach the "reasonable efforts" requirement in trade secret law. The central message is that programs to manage trade secrets, like other business processes, should align with business objectives *in the context of the needs of the specific business*. Ideally, trade secret management should be contextual and strategic, and not just a collection of "boilerplate" forms and protocols that may bear little relationship to the actual trade secrets and risk environment of a particular company.

While trade secret management demands strategic business thinking, it also has a legal dimension. The existence of a trade secret depends in part on whether the company has exercised "reasonable efforts" (or "reasonable measures") directed at maintaining its secrecy. This standard corresponds to the relevant circumstances of each enterprise, so that there can be no "one size fits all." In effect, it suggests that the judge or jury apply the same kind of analysis; namely, an assessment of the value of, and risks to, specific trade secrets in the context of the company's particular business and resources. We hope that this paper will help management formulate a proactive, tailored, and practical approach to managing trade secret assets that will address both business and legal requirements.

This *Commentary* differs from some other Sedona Commentaries not only in its intended audience but also in its focus on "issues to consider" rather than on developing specific guidelines that may be seen as insufficiently flexible. By thinking through the questions raised by this *Commentary* and utilizing the framework for the design and implementation of trade

secret management programs provided, companies will more effectively exercise control over their trade secrets and understand the value of sustained investment to that end.

James Pooley
Victoria Cundiff
Editors-in-Chief and Working Group 12
Steering Committee Chair Emeritus and Chair

Nicole D. Galli
Elizabeth McBride
Jennifer Lynn Miller
Senior Editors

GOVERNANCE AND MANAGEMENT OF TRADE SECRETS PRINCIPLES AT A GLANCE

PRINCIPLE No. 1 – Trade secrets should be protected by efforts that are reasonable under the circumstances to maintain their secrecy and value. Absolute secrecy is neither possible nor required. There is no one-size-fits-all approach.

PRINCIPLE No. 2 – A trade secret protection program should be actionable and achievable, rather than conceptual or aspirational. Once implemented, it should be periodically evaluated and adjusted as the company's trade secrets, business, and risk environment evolve.

PRINCIPLE No. 3 – A trade secret protection program should align with business goals and measurable objectives such as (1) securing and maintaining competitive advantage for the business; (2) leveraging trade secrets to commercialize new products and services; (3) supporting, generating, and incentivizing continued innovation; (4) extracting additional value from trade secrets through licensing, acquisitions, or secured financing; and (5) enforcing trade secret rights as necessary.

PRINCIPLE No. 4 – Trade secret governance generally requires an integrated enterprise approach that should accommodate and satisfy multiple and potentially conflicting corporate interests, including effective controls, information governance and data security, talent acquisition and retention, operational efficiency, disciplined budgets, reasonable return on investment, third-party information sharing demands, and legal enforceability.

I. INTRODUCTION

Trade secrets are intellectual property assets whose value stems from secrecy and the competitive advantage provided to their owner. Because trade secrets can also be cultivated, maximized, and profitably exploited along with other corporate assets, they can contribute to increasing the overall value of the business. Financial markets increasingly look to leverage trade secrets as assets in a range of transactions, including, in many cases, in mergers and acquisitions, licensing, securing loans, and risk transfer solutions.

But not all trade secrets are alike, nor are the businesses that seek to exploit them. Business success and progress often derive from not just one but many categories of confidential information. The Coca-Cola Company does not rely solely on the formula for its famous beverage. Like other businesses, it also has secrets related to product road maps; product modifications for multiple markets; planned advertising campaigns; sources of key ingredients; and research and development programs. Some of this information needs to be shared in a controlled fashion with people within and outside the organization, while other trade secrets may best be protected by keeping them locked away for occasional reference by a select few.

The value of particular trade secrets, the risks they face, and the effectiveness of controls may all change over time, particularly as the trade secret owner and its business operations and goals evolve. Some information will lose protection when a product is released or a patent issues, while other trade secrets may remain valuable indefinitely. Future technologies or market conditions may render a secret obsolete; or the success of a product or division may grow, and along with it the value of the related secrets. Resource constraints or operations flows affecting a company's ability to adopt certain security measures may vary over the life cycle of the trade secret. So too, the risks to

trade secrets are often dynamic, affected by changes in the workforce or in supply chains. And they may be amplified by externalities such as cybertheft or the shift to more remote work.

For all these reasons, protecting trade secrets is almost never a "once and done" project—it is a process to be evaluated over time as the nature and value of trade secrets to a company shift and as the company itself evolves. Further, protecting trade secrets cannot happen in isolation: trade secrets may be part of a larger portfolio of intellectual property assets that needs to be managed in accordance with the rules for each applicable legal regime. While every invention conceivably can be protected for at least some period of time as a trade secret, the long-term protectability of particular information as a trade secret may evolve as patents and copyrights are sought and issued.

Trade secret programs should be designed, in the first instance, under the scrutiny of business leaders and other relevant stakeholders. This allows decisions on investment in security to align with perceived value of the information and the operations and overall goals of the company and the interests of its various business units or functions.[1] In this way, trade secret protection programs will be integrated with strategic

1. Because we are speaking to business leaders who evaluate the need for and effectiveness of trade secret programs primarily in business terms, this *Commentary* employs some business terminology. For example, "return on investment (ROI)" refers to recapturing in the future what is invested today, together with an additional amount representing the risk to capital. A trade secret owner may realize a return on its investment not only by using information to increase internal efficiency and by better leveraging advantages commercially, but also or alternatively through licensing the information to third parties or avoiding costly litigation. Another example is "key performance indicators" ("KPI"), a set of metrics used to track performance of a person, business unit, product, or goal. The KPI metrics for a particular program are set up in advance to track performance, often through a "dashboard" or other reporting tool.

management. Of course, such programs must also be informed by legal considerations.

The law requires that trade secrets be protected with "reasonable measures" to maintain secrecy.[2] What is "reasonable" implies an inherently fact-specific analysis, so the case law can provide only general guidelines for companies to consider.[3] In general, when establishing policies, controls, and other mitigation measures, the owner should consider the value of the information assets, the risks of loss or contamination, the effectiveness and cost of potential policies, controls, and other measures, as well as the practical realities of the business's operations and strategic goals.

Because the legal framework is contextual, there can be no definitive set of "best practices" in developing a trade secret protection program. Rather, each company should choose an approach that fits its unique business circumstances as well as its most valuable information. While perfection is not required, thoughtful care and attention to the needs of the specific organizational context are.[4] This *Commentary* seeks to provide

---

2. 18 U.S.C. § 1839(3)(A); *see also* Uniform Trade Secrets Act § 1(4)(ii) (requiring "efforts that are reasonable under the circumstances").

3. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. c (Am. Law Inst. 1995).

4. Several research studies have found that most companies rely on fairly rudimentary measures to protect their trade secrets, e.g., confidentiality and noncompete agreements, general cybersecurity protection, employee policies, and enforcement efforts. *See, e.g.*, BAKER MCKENZIE, THE BOARD ULTIMATUM: PROTECT AND PRESERVE, THE RISING IMPORTANCE OF SAFEGUARDING TRADE SECRETS (2017), https://www.bakermckenzie.com/-/media/files/insight/publications/2017/trade-secrets; David S. Almeling, et al., *A Survey of In-House Attorney Views on Trade Secrets*, LAW360 (Jan. 12, 2018), https://www.law360.com/articles/999664/a-survey-of-in-house-attorney-views-on-trade-secrets. Some courts may reject such measures as "normal business practices" insufficient to meet the "reasonable measures"

companies with an outline of issues to be evaluated, an array of sample measures that can be considered for implementation, and an overall framework for assessing the relevant circumstances and designing and implementing a program sufficient to meet the company's ongoing needs.[5]

Principle No. 1 – Trade secrets should be protected by efforts that are reasonable under the circumstances to maintain their secrecy and value. Absolute secrecy is neither possible nor required. There is no one-size-fits-all approach.

Whether viewed through the legal lens of "reasonable" measures, or as a process of classical corporate asset management comparing risks, value, and rewards, the imperatives are the same. To protect the integrity of what it owns and preserve its ability to enhance enterprise value, the company should define in some practical way its most important secrets, so that it

---

standard. *See, e.g.*, Opus Fund Servs. (USA) LLC v. Theorem Fund Servs., LLC, No. 17 C 923, 2018 WL 1156246, at *3 (N.D. Ill. Mar. 5, 2018) (dismissing complaint).

5. Other related Sedona Conference commentaries provide useful guidance as well, including: The Sedona Conference, *Commentary on Privacy and Information Security*, 17 SEDONA CONF. J. 1 (2016), https://thesedonaconference.org/publication/Commentary_on_Privacy_and_Information_Security; The Sedona Conference, *Commentary on Information Governance, Second Edition*, 20 SEDONA CONF. J. 95 (2019), https://thesedonaconference.org/publication/Commentary_on_Information_Governance; The Sedona Conference, *Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents and Communications Generated in the Cybersecurity Context*, 21 SEDONA CONF. J. 1 (2020), https://thesedonaconference.org/publication/Commentary_on_Application_of_Attorney-Client_Privilege_and_Work-Product_Protection_to_Documents_and_Communications_Generated_in_the_Cybersecurity_Context; The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 SEDONA CONF. J. 495 (2018), https://thesedonaconference.org/publication/Commentary_on_BYOD.

can assess their value relative to the cost (in money or administrative inconvenience) of maintaining control through various security measures and to educate its workforce on what needs protection. While various checklists or examples of security measures (such as those in Appendix A) may be helpful references, only the company's management can be aware of the cost-benefit variables, corporate culture, existing operations and systems, and business goals that will drive decisions regarding protection of its own information. This *Commentary* is intended to provide a review of the legal and business landscape related to trade secret protection, including the array of factors that should be considered by all sizes and kinds of companies when developing the company's approach to trade secret protection, whether the company be a "mom and pop" business or a large global enterprise.

Principle No. 2 – A trade secret protection program should be actionable and achievable, rather than conceptual or aspirational. Once implemented, it should be periodically evaluated and adjusted as the company's trade secrets, business, and risk environment evolve.

No program or policy is effective if it is only published in a document. Aspirational standards that are never implemented or consistently followed are at best counterproductive. Among other things, defense counsel in litigation may seek to exploit the trade secret owner's failure to adhere to stated policies and procedures as a reason to block enforcement. An important element of building a sustainable trade secret governance approach consists of effective implementation and compliance, measured by appropriate controls across the company and its workforce. A court may ultimately find that the legal standard was met if key portions were implemented and consistently followed, even without complete fidelity to the program charter or

policy. But lapses can present otherwise avoidable challenges during litigation.

II. INHERENT CHALLENGES TO DEVELOPING A TRADE SECRET PROTECTION PROGRAM

A. The Legal Framework for Protecting Trade Secrets Provides Limited Concrete Guidance in the Face of Complex Organizational Factors

The range of information eligible to be a trade secret is vastly broader than patent- and copyright-eligible subject matter and can include virtually any information that provides a competitive advantage. State and federal laws and reported decisions have found a wide variety of information eligible to be a trade secret. Frequent candidates for protection as a trade secret include business plans, marketing roadmaps, organizational designs, algorithms, proprietary data sources and databases, technical drawings, source code, recipes, formulas, new product specifications, manufacturing processes, and concrete business strategies.

The fact that information may be eligible to be a trade secret, however, does not mean that in a particular case it will ultimately be found to be a trade secret. The Uniform Trade Secret Act (UTSA), state implementations of the UTSA, and the federal Defend Trade Secrets Act (DTSA) all include as part of the definition of a trade secret the requirement that the information must be the subject of "reasonable measures" to protect it.[6] Decisions in some jurisdictions under both the UTSA and the DTSA are also still influenced by the Restatement (First) of Torts, referencing the "extent of measures taken to protect the

6. *See* 18 U.S.C. § 1839(3)(A) (2016); *e.g.*, CAL. CIV. CODE § 3426.1(4) (2006); 765 ILL. COMP. STAT. 1065/2(d)(2) (1988); MINN. STAT. § 325C.01 Subd. 5(ii) (1986); Uniform Trade Secrets Act § 1(4)(ii) (1985).

information" as one of a set of factors to be considered in determining whether there is a trade secret.[7]

The legal framework for protecting trade secrets in the United States can vary from state to state. Federal law echoes the theme that trade secrets must be subject to reasonable measures to protect them and must not be readily ascertainable by others who can obtain value from them, but it generally does not impose specific requirements as to what the protection measures must be. The laws of other countries will be pertinent for companies that operate internationally; some of these laws spell out precise requirements that must be followed to protect trade secrets within that jurisdiction. Other commentaries have provided extensive analysis of key statutory regimes, and we rely on those to inform our analysis here.[8]

Reported judicial decisions throughout the United States, while finding certain behavior to suffice or fall short of "reasonable," focus primarily on unique facts of the case.[9] Therefore,

---

7. *See* Ashland Mgmt. v. Janien, 624 N.E.2d 1007, 1013 (N.Y. 1993) (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW INST. 1939)); *see also* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. L. INST. 1939). *But see* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (AM. L. INST. 1995) (not including within definition of "trade secret" a requirement that information be protected by measures that are reasonable under the circumstances).

8. For survey of trade secret laws in key U.S. states, *see generally* The Sedona Conference, *Commentary on Protecting Trade Secrets Throughout the Employment Life Cycle*, 23 SEDONA CONF. J. 807 (2022), https://thesedonaconference.org/publication/Commentary_on_Protecting_Trade_Secrets_Throughout_Employment_Life_Cycle [hereinafter *Sedona Employment Life Cycle Commentary*]. For survey of trade secret laws in key non-U.S. countries, *see generally*, The Sedona Conference, *Framework for Analysis on Trade Secret Issues Across International Borders: Extraterritorial Reach,* 23 SEDONA CONF. J. 909 (2022), https://thesedonaconference.org/publication/Trade_Secret_Issues_Across_International_Borders_Extraterritorial_Reach.

9. *See, e.g.*, Tax Track Sys. Corp. v. New Inv. World, Inc., 478 F.3d 783, 787 (7th Cir. 2007) ("The question here is how much effort to keep

while case law can be informative, it offers little in the way of concrete guidance from which a company can design and implement its own strategy to protect trade secret assets.[10]

Along with these intentionally elastic legal assessments made in the context of specific cases that often do not give detailed insight into the business organization involved, companies must contend with different business and development environments, along with, in many cases, competing internal corporate programs and priorities and preexisting information

---

information confidential is enough to be considered reasonable? Courts evaluate this question on a case-by-case basis, considering the efforts taken and the costs, benefits, and practicalities of the circumstances . . . . Typically, what measures are reasonable in a given case is an issue for a jury . . . . In some circumstances, however, it may be readily apparent that reasonable measures simply were not taken.") (internal citations omitted); Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991) ("[O]nly in an extreme case can what is a 'reasonable' precaution be determined on a motion for summary judgment, because the answer depends on a balancing of costs and benefits that will vary from case to case and so require estimation and measurement by persons knowledgeable in the particular field of endeavor involved."); Mattel, Inc. v. MGA Ent., Inc., 782 F. Supp. 2d 911, 959 (C.D. Cal. 2010) ("The determination of whether information is the subject of efforts that are reasonable under the circumstances to maintain its secrecy is fact specific."); Data Gen. Corp. v. Grumman Sys. Support Corp., 825 F. Supp. 340, 359 (D. Mass. 1993) ("Whether reasonable steps have been taken depends on the circumstances of each case, including the nature of the information sought to be protected and the conduct of the parties.").

10. *But see* NEV. REV. STAT. § 600A.032 (2001), the Nevada Trade Secret Statute, establishing that "[t]he owner of a trade secret is presumed to make a reasonable effort to maintain its secrecy if the word 'Confidential' or 'Private' or another indication of secrecy is placed in a reasonably noticeable manner on any medium or container that describes or includes any portion of the trade secret. This presumption may be rebutted only by clear and convincing evidence that the owner did not take reasonable efforts to maintain the secrecy of the trade secret." Some foreign trade secret laws also impose more formalistic requirements than the contextual "reasonable efforts" standard.

technology systems. Potentially conflicting company strategies and objectives must be considered, as well as the practical realities of running a business. Company priorities and resources may shift over time. These variables can make it difficult to build support and secure budgets. These challenges can be frustrating to business leaders focused on execution (and those tasked with protecting intellectual property) and can lead to inconsistent and ineffective implementation and compliance.

Many different inputs can affect a decision about what measures are reasonable within a particular organization. Companies come in all shapes and sizes and industries, and they manage different risks and challenges in designing, implementing, and sustaining such measures, while also absorbing the related cost and operational burdens. While most companies need to make some disclosures of their trade secrets to capture value from them, companies differ in the extent to which they need, or strategically choose, to disclose information both internally and externally. Companies may be required or elect to disclose some trade secrets to suppliers, to government agencies, or across borders, presenting additional risks and challenges. Research-focused organizations may choose to extend access to a broad group of personnel and also to outside contractors or collaboration partners, both private and public. Companies in some fields may face market or business pressures to seek patent protection for some innovations, which may impact the issue of what related information can later be claimed as a trade secret.[11] On top of these sometimes conflicting demands, the

11. *See, e.g.*, Hickory Specialties, Inc. v. Forrest Flavors Int'l, Inc., 12 F. Supp. 2d 760 (M.D. Tenn. 1998), *aff'd* 215 F.2d 1326 (6th Cir. 2000) (holding that information disclosed in a patent is not protectable as a trade secret even if the patent was not the source of defendant's access to the information at issue). However, the issue of whether a patent negates a trade secret is nuanced as courts have also recognized that a patent has not resulted in lost

business may have to contend with different policies and systems as well as the objectives and practices of key functions such as information technology (IT), human resources (HR), security, legal (potentially including patent as well as other legal teams), communications, and marketing.

The nature of the secret information can also significantly impact whether reasonable measures have been employed to protect it. Trade secrets can be expressed, stored, and secured in many different ways and embodiments. Some information can be productively shared through providing highly restricted access to only a handful of people, while other information may need to be shared more broadly to multiple constituencies to effectively operate key business functions. Some trade secrets, such as prototype equipment on a manufacturing floor, require physical security measures. And a large amount of trade secret information is stored and communicated digitally, potentially necessitating use of sophisticated technological as well as

---

trade secret protection. *See also* Allied Erecting and Dismantling Co., Inc., v. Genesis Equip. & Mfg., Inc., 649 F. Supp. 2d 702 (N.D. Ohio 2009)("while, as a general proposition, there is no trade secret protection for secrets that are disclosed in a patent application, numerous courts have allowed trade secret protection for processes or specifications related to the patented device that are not disclosed in the patent."); Tex. Advanced Optolectronic Sols., Inc. v. Renesas Elecs. Am., Inc., 895 F.3d 1304 (Fed. Cir. 2018) (patent must disclose combination of elements that comprises trade secret to render trade secret protection extinguished); Wellogix, Inc. v. Accenture, L.L.P., 716 F.3d 867 (5th Cir. 2013) ("patent destroys the secrecy necessary to maintain a trade secret only when the patent and trade secret both cover the same subject matter."); AgroFresh Inc. v. Essentiv LLC, C.A. No. 16-662 (MN), 2020 WL 7024867, at *5 (D. Del. Nov. 30, 2020) (trade secret protection not lost through publication because it did not reveal specific mechanisms protected by trade secret); Celeritas Techs. Ltd. v. Rockwell Int'l Corp., 150 F.3d 1354 (Fed. Cir. 1998) (upholding verdict that information in the patent was not readily ascertainable because the "implementation and techniques" protected by trade secret "went beyond the information disclosed in the patent").

contractual controls, sometimes including controls such as multifactor authentication, biometric identification, or otherwise highly restrictive access management.

Companies often look to benchmarking data, where available, in order to design new programs and policies, hoping to become better informed and borrow from "best practices" and industry leaders. Such an approach may indeed be helpful to inform the process but should not be relied on as the sole basis for design; the variation in circumstances among businesses means that "borrowing" of generalized strategies can result in expensive overkill or leave major gaps in a protection plan.

B. Generic Confidentiality Measures Can Be Effective but Carry Their Own Risks

Various checklists, frequently promoted by security vendors or in alerts proposing security audits, suggest that adequate protection can be provided by certain general practices, such as employee and third-party confidentiality agreements, facilities security, and robust IT systems. These generic practices or general confidentiality approaches can be helpful as a starting point and in some cases can be adequate protection. But relying only on generalized checklists and generic approaches, without critical analysis as to their adequacy or applicability to the needs of the particular information and company, can instill a false sense of security for the simple reason that most businesses face a unique set of risks regarding a unique set of valuable information assets. Generic programs tend to homogenize the risk across business in general or a given industry. Generalized approaches can only address the risks mitigated by these baseline measures, and not any risks that are peculiar to a company's own information, operations, and business. For example, consider "customer information," which can be extremely valuable in the abstract. Very little in the way of specific security measures may be necessary for a small business where a

customer list is known to and accessible by only the two owners, while much more may be required to protect a broader scope of customer information at a large company with a sales force, accounting staff, and customer service representatives who work closely with assigned accounts, and where sophisticated analytic tools are used to model, predict, and influence customer behavior or to assess competitive offerings. Further, "standard" measures may become "shop worn" and may not reflect evolving case law or new contractual or technological tools for companies to consider.

C. *Attorney-Client Privilege and Business Records: A Double-Edged Sword*

Designing and administering trade secret programs present special challenges around protecting attorney-client privilege during company operations and processes. Ideally, counsel (whether in-house or external) should assist in the identification of trade secrets and formulation of a trade secret protection effort. There are many nuanced legal issues involved with identifying what is a trade secret, how the program will be evaluated as "reasonable" in an enforcement action, optimal contract protections, and the like. It may also be helpful to have attorney-client privilege attach to the communications among those doing this work without worry that it will later be subject to discovery and attack by opposing counsel in an enforcement action. The same is true for compliance efforts, periodic reviews of the program, and investigations related to potential losses and enforcement. This protection from disclosure to promote candor is why the attorney-client privilege exists—so that these valuable legal communications are not stifled.

However, in a later enforcement action, a company may want to present internal communications that identify the relevant trade secrets or document its protection efforts. If such efforts are solely reflected in communications with the legal

department, production of the communications in litigation may risk a broad subject-matter privilege waiver. Therefore, it is equally important when designing a protection program to consider what information and documentation the company would like to treat as a "business record" that can be used without waiving any attorney-client privilege. For example, once trade secrets have been identified with legal input, some companies choose to create a business record to identify the trade secrets as part of a training and compliance program aimed at protecting them. This nonprivileged record can be used to make sure the appropriate staff know what the trade secrets are and what security measures are required to protect them. Where appropriate, such records can also become part of a document retention policy or exit interview protocol. These business records can be put forward in any enforcement action without jeopardizing privileged communications.

If counsel providing advice to the team is in-house, the privilege issues can be more complicated. This is particularly true in smaller companies where in-house counsel can have several roles, some of which are more business related than legal. In this situation, some communications with these persons are privileged (where they are providing legal advice) and some are not (where they are performing, for example, an HR or purely business strategy function). Under these circumstances, it is particularly important to understand and act purposefully in making judgments before any litigation about what information is and is not intended to be privileged and to mark documents and consider information flows accordingly.

III. DEVELOPMENT OF THE TRADE SECRET PROTECTION PROGRAM

Implementation of a trade secret protection program generally consists of three steps. The first step is designing the program, including identifying the information to be protected and evaluating and choosing appropriate protective measures. The second consists of implementing the program in a way that breathes life into the chosen policies, processes, and controls. Third is building and sustaining compliance, which includes periodic assessment and updates of the program to ensure it continues to provide adequate protection in the face of changes to the external environment and to the company's trade secrets, risk environment, operations, and strategic goals.

Principle No. 3 – A trade secret protection program should align with business goals and measurable objectives such as (1) securing and maintaining competitive advantage for the business; (2) leveraging trade secrets to commercialize new products and services; (3) supporting, generating, and incentivizing continued innovation; (4) extracting additional value from trade secrets through licensing, acquisitions, or secured financing; and (5) enforcing trade secret rights as necessary.

While designing and implementing a protection program can require extensive executive engagement, sustained investment, and enterprise discipline, the reality is that there are usually existing processes and practices that can be leveraged for this purpose. In some cases, the bulk of the effort lies in simply centralizing (and sometimes harmonizing) these other processes for the governance of trade secrets in a manner that will meet a "reasonable efforts" standard.

The success of a program often depends on executive leadership and business general managers "buying in" to the value

of the secrets and the measures needed to protect them. This support may be necessary to justify the cost, as well as to establish the "tone at the top" that is so important in driving compliance. For these reasons, it is important to identify all stakeholders at the beginning of the project, and to think about the company's goals and the range of benefits and return on the investment (ROI) that the program can deliver.

<u>Principle No. 4</u> – Trade secret governance generally requires an integrated enterprise approach that should accommodate and satisfy multiple and potentially conflicting corporate interests, including effective controls, information governance and data security, talent acquisition and retention, operational efficiency, disciplined budgets, reasonable return on investment, third-party information sharing demands, and legal enforceability.

A. Preliminary Steps

1. Articulate the value of the program and its return on investment

Within the last quarter century, intangible property has emerged as the single most significant asset of S&P 500 companies. A 2020 study by Ocean Tomo concluded that the share of intangible asset market value (primarily intellectual property) of the S&P 500 increased from 68 to 84 percent between 1993 and 2015, and COVID-19 accelerated that trend, with intangible assets now commanding over 90 percent of the S&P500 market value.[12] A trade secret protection program, when understood in

12. A summary of the current Ocean Tomo study is available at *Ocean Tomo Releases Intangible Asset Market Value Study Interim Results for 2020*, OCEAN TOMO (Sept. 22, 2020), https://www.oceantomo.com/media-center-

the context of protecting a company's core value, is increasingly important to the company. Framing the effort in a way that emphasizes the return on investment (ROI) is important to gain buy-in from stakeholders and the sustained investment required. The "return" can be in the form of asset values identified, created, increased, or extracted. It can also be expressed in the form of the support the program provides the company in achieving its goals and improving financial performance, as well as in the company avoiding costs associated with loss of its trade secrets or liability for mishandling the secrets of others.

Substantiating an ROI can be achieved in numerous ways. The most rudimentary example is for the owner to calculate the value of the secrets to be protected and compare the cost of the protection against the value of preserving and building that value. By statutory definition, trade secrets must have "actual or potential economic value." Companies can extract commercial value for their trade secrets by using them internally to achieve a market advantage over competitors who do not know them. Companies have been able to achieve a market advantage from their trade secrets through innovating new products, through realizing and maintaining higher margins for their products, or through being "first to market" and continuing to preserve a "lead time" advantage even after others enter the field. Many companies have been able to obtain commercial value from their trade secrets through a variety of commercial transactions as well. Some companies, for example, in the semiconductor, petrochemical, and biopharmaceutical industries, have additionally extended their economic reach and achieved substantial value through licensing activity, either by licensing transactions with customers who are willing to pay to gain access to trade secrets they can exploit for themselves, or by

---

item/ocean-tomo-releases-intangible-asset-market-value-study-interim-results-for-2020/.

licensing trade secrets to third parties who may have greater access to particular markets than the trade secret owner does. More recently, a growing number of companies have also been able to derive value for their trade secrets in capital-raising and merger-and-acquisition transactions, by increasing their overall valuation in determining the equity offering or purchase price. A successful protection program will help substantiate, maintain, and even boost this value of core trade secret assets, such as by enabling the use of trade secrets as collateral for financing or for transferring risk with insurance solutions.

Another effective way to show a return on investment may be to determine what costs will be avoided by risk mitigation and properly protecting the trade secret assets. For instance, for a company concerned about misappropriation risk, the prevention of a single incident can avoid significant cost, since even a relatively small dispute can often run into millions of dollars in litigation costs alone,[13] as well as disruption to business processes and distraction to company personnel. And there also can be avoidance of other less direct costs, for example from lost sales, new product delays, lost market share, and reputational damage. A thorough financial estimation of the cost avoidance and risk mitigation that an effective program delivers will serve as a useful foundation for determining ROI.

Another helpful approach is to consider the enterprise value creation of a comprehensive program. This can be calculated based on multiple factors, such as the estimated direct value and improved financial performance that core competitive advantages deliver to the business (e.g., higher margin sales).

13. AIPLA, REPORT OF THE ECONOMIC SURVEY I-225 (2021) (mean cost to litigate a trade secret misappropriation case involving risk of greater than $25 million, inclusive of discovery, pretrial, trial, posttrial, and appeal, at $4.582 million, and first and fourth quartile of respondents reporting litigation costs of $1.5 million and $8 million, respectively).

Indeed, an effective trade secret protection program not only focuses on providing robust protection and supporting a strong enforcement position but can also serve as a catalyst for inspiring and reinforcing a culture of innovation—and the creation of new trade secrets. In this respect, an ROI can be derived based on the value attributable to these new innovations and how they explicitly map to value chains and select product lines. The ROI calculation can also consider the value of prevention of loss of institutional knowledge, because the program can ensure the consistent documentation of that knowledge.

In considering the investment side of the equation, it is important to consider the company's ability to leverage any existing systems or processes to protect the secrets, thereby avoiding the expense and operational distraction of developing these systems from scratch.[14]

2. Identify all potential stakeholders

For many companies, the information, input, and buy-in will come from different functional areas of the company, such as legal, human resources, information technology, data owners, executive leadership, finance, risk management, supply chain and vendor management, communications, regulatory, research and development, business development, and various operating divisions or business units. Even within these groups, there may be differing perspectives or priorities to take into consideration (e.g., intellectual property, commercial, and corporate governance counsel may have very different points of view on some program measures).[15] Many companies form a cross-

14. *See infra* Section III.B.4 (Integrated enterprise approach: Leverage existing capabilities and processes and navigating conflicting or competing objectives).

15. Companies in some fields may face market or business pressures to seek patent protection for some innovations, which would benefit from close

functional team, including representatives from each of these functions (or a smaller team may tap into these areas as needed), to *design* a program. For the *implementation and operation* of a program, sometimes a different cross-functional team is put together based on the desired expertise, influence, and capabilities.

It is important to identify all the groups and individuals that are potential stakeholders in the planning phase. Each may have a distinct interest in identifying the trade secrets, determining value and risks, establishing the ROI, and choosing compliance policies. Regardless of who is directly involved, engagement and buy-in from senior management will be critical. Following the design phase, this same or a new set of stakeholders may also have a role to play in implementation, compliance, monitoring, and enforcement.

The decision of who should be involved in planning and, later, implementing a protection program will vary across companies and industries.[16] The team members bring not only

---

coordination between the legal requirements of patent and trade secrets law as well as strategic consideration of what information will be claimed under a patent application and what will be retained as a trade secret. For example, some companies will face the business need to make disclosures of information they hope to patent to potential sources of funding under nondisclosure agreements but will need to evaluate the potential impact of the timing of even protected disclosures on their ability to later secure patent protection for the information that has been disclosed. *See* Helsinn Healthcare S.A. v. Teva Pharms. USA, Inc., 139 S. Ct. 628 (2019) (holding that the sale of an invention to a third party who is obligated to keep the invention confidential may place the invention "on sale" for purposes of the Leahy-Smith America Invents Act, which bars a person from receiving a patent on an invention that was "in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention").

16. These functions can be in separate departments or personnel or, especially in smaller companies, may be performed by management generally. In certain companies, the titles of relevant individuals could include Chief

different perspectives, but different expertise. For example, an HR manager will consider the interplay of the program with any existing or planned employee restrictive agreements, or whether employee surveillance as a protective measure may be improper or unwise. Counsel will consider the interplay between trade secret, copyright, and patent protection. Licensing personnel will consider the potential value of information in existing and planned licensing transactions. Transactional personnel will consider the impact of protective measures on assets that are being acquired and on managing information that may be shared or spun off as part of a transaction. Finance personnel will be focusing directly on the cost and impact of protective measures on enhancing asset value. Information technology and security personnel will bring expertise in existing programs and the availability of additional resources.

Organizing teams to manage trade secret information should not focus simply on team members whose primary focus is internal. Some functional areas—such as marketing, sales, public relations and communications, supply chain and purchasing, patent procurement, and regulatory compliance—inherently involve disclosing information to the public or sharing information with third parties. Some research and development (R&D) organizations have close relationships with universities and may be parties to grant arrangements that require disclosure of some information to the university or the government. Without buy-in from these functional groups and leaders and working out measures that allow these functional areas to do their work, implementation and compliance with a program to

---

Executive Officer, Chief Financial Officer, Chief Information Officer, Chief Information Security Officer, General Counsel, Intellectual Property Counsel or Manager, Chief Compliance Officer, Chief Risk Officer, Chief People Officer, Chief Technology Officer, and Competitive Intelligence Officer.

control and manage the flow of assets identified as trade secrets can be difficult.

Bringing complex teams together to design and implement a program will require that assessments and decision making are not siloed, but instead are centralized or reached by consensus of the whole. While identifying stakeholders is the critical first step, outlining a centralized governance model, how decisions will be made, and how these stakeholders will each effectuate their roles and responsibilities within the team is another important step.

3. Identify the company's trade secrets

Whether to enumerate or create an "inventory" or "list" of trade secrets and, if so, to what degree of specificity may be one of the more controversial design decisions. Some companies proactively catalog and manage detailed portfolios of trade secrets; this approach can result in broader business benefits, insights, and risk mitigation. For example, Taiwan Semiconductor Manufacturing Company Ltd. (commonly referred to as TSMC) has been internally registering trade secrets since 2013, growing to a catalog of over 140,000 trade secrets by 2021.[17] For some businesses, however, building and maintaining such a corporate-wide trade secret registry may be seen as daunting and overly resource-intensive. Some companies can create an inventory or list without disproportionate administrative burden.

17. Jacob Schindler, *TSMC Has Catalogued More Than 140,000 Trade Secrets Since 2013, Company Says*, IAM (Oct. 1, 2021), www.iam-media.com/trade-secrets/tsmc-has-catalogued-more-140000-trade-secrets-2013-company-says. Such a registry is embedded in the company's invention and disclosure process, designed to capture and record a more expansive portfolio of intellectual property beyond patents. Developers at TSMC are encouraged to focus on the commercial value of information they are creating and on why it gives a competitive advantage over those who do not know the information.

Many companies may see the need for, and benefit from, some system of tracking that does not necessitate or create excessive administrative burden.

That said, some argue that establishing an inventory of trade secrets in advance of a specific dispute can create business risk because some secrets might be inadvertently omitted from the inventory, potentially impairing a future trade secret enforcement action. Others argue that it is simply an impossible task, particularly for large, multinational companies, to create and maintain a current and complete inventory of trade secrets. These objections should be scrutinized and weighed against the benefits of some form of identification or cataloging that minimizes litigation risk, informs the design team and workforce of what is being protected, and prepares the company to respond quickly in the event that enforcement is required.

Regardless of the mechanics of identifying trade secrets, and whether a formal inventory is prepared, many businesses already have an understanding of many of the key assets they own, at least to enable communication with employees and trusted outsiders about what information is to be treated as a trade secret.[18] When, however, trade secrets are vaguely defined and shared to receiving parties, they are at practical risk of loss, and in any enforcement litigation, the receiving party may be able to argue convincingly that it did not have reason to know that the information should be protected.[19]

Identifying or tracking trade secrets for purposes of designing or managing a protection program usually requires less specificity than identifying trade secrets for an enforcement

18. *E.g.*, Big Vision Priv. Ltd. v. E.I. DuPont de Nemours & Co., 1 F. Supp. 3d 224 (S.D.N.Y. 2014), *aff'd*, 610 F. App'x 69 (2d Cir. 2015).

19. *E.g.*, Scentsational Techs., LLC v. Pepsico, Inc., 13-cv-8645 (KBF), 2018 WL 2465370 (S.D.N.Y. May 23, 2018), *aff'd*, 773 F. App'x 607 (Fed. Cir. 2019).

action. The purpose of the former is to inform the business process designing the overall program, including high-level categories of risk and means to mitigate it. Enforcement litigation, in contrast, requires identification with particularity sufficient to enable the defendant to prepare a defense to specific claims of misappropriation and the court to manage the action, a process subject to defined legal principles and civil procedure.[20] The two approaches are not unrelated, but identifying trade secrets in the course of business operations is generally directed to a larger universe of information and may be less formal than for presentations in the course of litigation.[21]

When managing protection programs, some companies identify categories of trade secrets without enumerating each specific secret. If the category has meaning for the company and its employees sufficient to create a shared understanding of what the trade secrets are, then this may be sufficient, even if more exacting descriptions may be needed for litigation. For example, if the trade secret is related to the operation conditions used to perform a method of manufacture in a particular piece of equipment (e.g., specific temperature, agitation torque, shear level, and residence time) then identifying the trade secret as "the process conditions of mixing in Tank P123" may be enough for purposes of internal management. However, it may not meet the particularity standard of an enforcement litigation since it

20. *Big Vision Private*, 1 F. Supp. 3d at 260–61 (S.D.N.Y. 2014) (disclosures during a corporate disclosure of trade secrets to a third party need not use the word "trade secret" but should do "something" to put the recipient on notice of his obligations related to the trade secret information being disclosed whereas in the litigation itself, the plaintiff was required to identify with particularity exactly what information was at issue in the litigation).

21. *See* The Sedona Conference, *Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases*, 22 SEDONA CONF. J. 223 (2021), https://thesedonaconference.org/publication/Commentary_on_Proper_Identification_of_Trade_Secrets_in_Misappropriation_Cases.

does not reveal what the process conditions are. "Customer lists" is another trade secret identification category that may be adequate for an internal program, as employees will often understand what that is even though specifics—the "list" at issue is this particular portion of a specific customer database—may need to be parsed out in litigation.

In any event, potential risks attach to any level of identification or decision not to identify. If there is litigation, the way that trade secrets have been internally identified (or not) may become relevant. Taking the manufacturing trade secret example from the preceding paragraph, if the enforcement action identifies the trade secret as the specific temperature, agitation torque, shear level and residence time of mixing but ties these variables to a completely different piece of equipment (e.g., a tubular reactor rather than Tank P123), defense counsel will be asking some very difficult questions and likely arguing that the information at issue in the lawsuit was never treated as a trade secret by the plaintiff before litigation.

Identifying trade secrets in the course of business should take into account differences in the type of information being considered. Some trade secrets, by their very nature, can be precisely captured and documented (e.g., the formula for Coca-Cola). Others may be identifiable more generally at a high level but challenging to break down, define, and summarize concisely (e.g., source code or a large data set collected and held by a company). And still others are legitimate secrets developed over time but are harder to define or distinguish from unprotectable personal skill (e.g., a business method to achieve a specific result, such as leadership development or converting marketing targets into paying customers). Some, such as software applications, are inherently fluid, dynamic, and continuously evolving or overtaken by market developments or technical improvements. Notwithstanding these differences in types of trade secrets, the company's focus should be on communicating

to recipients that particular information is to be protected as a trade secret. Procedures can also be established to address questions, both during the relationship and, particularly, when a relationship with the receiving party or employee ends.

Some emerging approaches to trade secret protection leverage new technologies to apply to the process of identification. Software can inspect contents of documents and machine-learning tools can review internal correspondence to help flag particular information as potentially qualifying as a secret. In addition, trade secret registries and other software included in a company's research and development environment can enable engineers to identify and effectively document trade secrets during and after innovation. Registering trade secrets on blockchain could create an immutable, verifiable record of creation that may ultimately strengthen legal enforcement positions.

Regardless of one's view of the relative merits of these approaches in the abstract, companies should consider whether individuals within the organization are already making *their own* rather than *institutional* decisions about what information should be kept secret and access controlled, what must stay internal within the company, what can be shared securely with partners, and what can be put into the public domain. Those who are engaged in designing a protection program should consider these realities. They should consider collecting documentation of existing approaches to protecting information and interview senior management, R&D personnel, and other professionals about what they think is most valuable.

4. Conduct an internal assessment

a. Valuation and business impact assessment

Recognizing the value of the trade secrets informs an understanding of the potential impact to the business of a loss or compromise of sensitive information. That understanding, in turn,

will permit a reasoned judgment about the level of cost—in terms of resources and accepted inconvenience—that is appropriate to secure that information. Valuation for this purpose is not a precise numerical exercise; it is necessary, however, among other reasons, to enable the company to assess priorities. At times there also may be good reasons to determine more precise values, including to justify collateral for debt and investment, establish insurability, and to inform negotiation of merger and acquisition or license transactions. When considering valuation for this purpose, questions to be explored may include:

- *Confidentiality*. What would be the business consequences if competitors or other interested parties saw or copied the secrets?
- *Integrity*. What if secrets are deliberately or accidentally altered or contaminated with information belonging to another?
- *Availability*. What if the secrets were irreversibly lost, deleted, or destroyed?[22]
- *Cost to Develop*. What did the owner spend to develop the trade secrets?
- *Market Value*. What would a willing buyer pay for the secrets?
- *Discounted Cash Flow*. What is the net present value of income that can be derived from the secrets?

b. Risk assessment and management

Once management has aligned on what the company's trade secrets are, then threats, vulnerabilities, and risks can be identified as well. It is important to remember that loss may occur through internal or external actors, and the behavior may be

22. *See generally Sedona Employment Life Cycle Commentary*, *supra* note 8.

inadvertent or intentional. The business should consider these vectors of loss in the context of its unique information assets. This connecting of risks to related categories of valuable assets is important in supporting business decisions on protection measures and controls.

Risks can be both outbound and inbound. Outbound risks include theft by a third party, leakage from the inside (employees taking secrets out the door or sharing them carelessly while employed), loss of the institutional knowledge of a secret (e.g., when employees leave and the secret is not fully recorded or documented), and loss from unauthorized use or disclosure. Inbound risks can include contamination by confidential information from a third party entering the company, including from new hires[23] or from customers, vendors, or other business partners. Potential but ultimately unsuccessful acquisitions often present a high risk of inbound infection, as those evaluating a transaction gain greater exposure to work others are doing. Even completed transactions, where a company is acquired and there is an imperfect record of confidentiality agreements or third-party custodial data, can lead to unwanted contamination.

With the rise of the gig economy, companies face increased inbound and outbound risks when using workers who are not employees, such as consultants, temporary or contingent workers, or workers in shared or coemployment situations (also referred to as "secondments"). Consultants working simultaneously for competitors can present a particularly high risk. Many may believe that they are free to take work they have done for one company as part of their "portfolio" of tools to use for others. Misunderstandings abound regarding what may constitute properly portable "residual" knowledge. Unmanaged risks arise against the background of often inadequate training,

23. *See id*.

policy, contractual clarity, and processes designed to safeguard against them.

If a company's business is international, diligence and understanding of the risks in these other countries (particularly those known for or suspected of not respecting intellectual property) is particularly important to developing protective measures. Companies may interact with a workforce employed by a third-party entity they do not directly supervise or manage. The company should consider the qualifications of foreign suppliers and licensees, comply with required protocols that may be imposed in other countries, and include procedures for securing necessary contractual protections and enforcing compliance, both during and after termination of the relationship. Companies should also familiarize themselves with any formal requirements in the countries of concern for keeping records of trade secrets.

The sheer number and types of risks that could possibly arise with respect to any one of a company's trade secrets or third-party trade secrets in a company's possession, regardless of how significant or valuable they are, may effectively make it impossible to guarantee full compliance and prevention of all potential breaches. Risk assessment and threat profiling can be used, however, to help assess "touch points" with trade secrets and prioritize potential risks of theft, loss, or misuse of such trade secrets and how resources should be allocated to address those risks. Strategic risk assessment and risk management can help a company identify the most vulnerable technology, information, and actors on which to focus policies, processes, or even ongoing monitoring—for example, on particular types of technical or business information, particular suppliers, highly sensitive incubating projects, or particular technological entry and exit points.

Many companies use ongoing enterprise risk management (ERM) tools to identify, assess, and manage a variety of risks that their businesses face.[24] Risk assessment in the area of trade secret protection can be carried out as a separate initiative, but also can be a logical issue to include in a company's ERM program in order to achieve executive oversight and centralized trade secret governance overall, in light of other risks and mitigation strategies. For example, a company may wish to limit who has access to a sensitive portion of the manufacturing floor where equipment is operated and trade secret processes may be visible. Limiting means of ingress and egress to this portion of the manufacturing floor may add physical security of the secret but may also create an operational bottleneck with other production lines or equipment in close proximity. Finding the appropriate balance between these interests becomes a business judgment.

c. Assess company structure, systems, workflows, and culture

An overall assessment of the company's systems to determine what can affect trade secrets (positively or negatively) is important to determine what program components will be both practical and effective. For example, companies should consider their own corporate and management structure, the culture and awareness around confidentiality, any existing functional areas that could be part of a designed program, and how the company, and its competitors, interact with the outside world.

24. Enterprise risk management is a plan-based business strategy that aims to identify, assess, and prepare for risks, dangers, and other potentials that may interfere with a company's operations and objectives, assessing the potential impact of each and methods to mitigate them. This informs a decision about which risks to manage actively, and which risks are not worth the cost of mitigation.

Based on this assessment, a program might be designed and implemented with an enterprise-wide approach, or it could be focused on specific business units or functions within the company. Large companies may consider whether a diversified approach to implementing reasonable measures within the corporate structure is appropriate (at the corporate, business unit, or technology segment levels), with periodic coordination on the reasons for and lessons learned from different approaches. Small or young companies tend to implement trade secret protection on a company-wide basis, reflecting a lesser need for hierarchy. Large companies with varying needs for access to more complicated sets of sensitive information will generally need more detailed policies and protocols, coupled with more intensive efforts at training and compliance.

Assessing existing company systems and workflows is important for at least two reasons. First, some of them can be leveraged in the design and implementation of the protection program. For example, if a company already has hardware and software firewalls and other cybersecurity protections, document retention, social media, and other relevant policies, and locks on the doors, there is probably no need to replace those measures or start over. Instead, these existing systems, policies, and practices can be adapted and leveraged to fit within the comprehensive trade secret management program. Other company functions or workflows may present risks to be evaluated and mitigated. For example, patent application strategies, public relations, marketing, sales, and regulatory reporting compliance, while being critical to overall success of the business, are all areas potentially ripe for inadvertent disclosures.

Like all corporate assets, the scale, types, amount, and location of trade secrets within the company should be considered. For example, for secrets embedded in digital files, what is the general ratio of "secret" data in relation to all digital data of the company? For physical secrets, what is the size and volume of

the equipment? Where are the secrets stored or used (e.g., within the "four walls" of the company or shared with third parties, on what computer systems or in what storage locations, in what countries)? This information can inform decisions on who has access and how access can be controlled and monitored.

Company culture plays a significant role in both supporting a protection program and creating compliance risks. Emphasizing speed can foster engineering and technology advancements, for example, but can deprioritize security and compliance. Similarly, open and collaborative work environments can benefit creativity and innovation and enhance development of a variety of kinds of goodwill but can be more susceptible to trade secret leakage.

Front-line employees are sometimes in the best position to recognize risky situations such as outsiders who are not following visitor protocols, emails inadvertently sent to the wrong recipient, confidential information that is not appropriately marked or stored, or offers to view the trade secrets of other companies. A "see something, say something" culture empowers employees, managers, and leaders to become ambassadors of the protection program. On the other hand, a company whose R&D team, intellectual property team, and salesforce tend to act independently in "silos" may suffer from a lack of awareness, allowing trade secrets to be lost through inadvertent leakage. Another potential risk area is when company personnel with trade secret knowledge have come from academia or are working with academia on trade secret projects or technologies. Academia is generally a group whose orientation is to publish and share information, rather than keep secret and protect it.

B. Designing the Program

Having identified the trade secrets and their business impacts, risks, value, locations, and formats as determined in the

assessment phase, potential risk mitigation measures can be considered, and an overall program designed (or in the case of established programs, refined). This phase will address not only specific protective measures, but also the implementation plan, anticipated compliance efforts, responsible persons, and associated roles and processes. Most importantly, the design (and as discussed below, periodic review and modification) of a program should seek a balance among effective protection, potential business impact, parallel or conflicting business processes and functions, information sharing demands, and legal enforceability.

1. Selecting "reasonable measures" for protecting trade secrets

Regardless of the level of particularity with which a company identifies its trade secrets, the reasonableness of its efforts should always be considered in the context of the totality of the circumstances. For litigation purposes, the core inquiry for determining whether reasonable measures have been employed is often how the information was treated by the company before the dispute arose.

It is difficult to draw useful conclusions from case law because most opinions arise on motions addressing the sufficiency of allegations or evidence, and even where the facts are directly addressed on the merits, the treatment is often cursory. However, some examples of the factors courts may consider are:

- *The size and maturity of the enterprise.* Large, multinational companies are often held to a higher standard of secrecy controls than a small, single-location business.[25]

25. Puroon, Inc. v. Midwest Photographic Res. Ctr., Inc., No. 16 C 7811, 2018 WL 5776334, at *7 (N.D. Ill. Nov. 2, 2018) ("Reasonable steps for a two-

- *The location of the enterprise.* A company located in an industrial, competitive environment with frequent cross-movement of employees may require a different level of security than a company located in a remote, rural area and having a stable workforce.
- *The value of the trade secret.* In general, the greater the importance of the particular secret to a profitable and differentiated product or service, the greater the extent of protective measures the owners will naturally take to reasonably protect the trade secret.
- *The extent and cost of the measures taken.* A judge or jury may be more likely to find reasonable efforts when a trade secret owner implements more robust measures and does so consistently, ensuring that those with access understand what is confidential and how they are expected to protect it.
- *The rationale for the selection of the measures taken and not taken.* Trade secret owners do not have to anticipate all possible risks to the integrity of their information,[26] but control failures will be more readily understandable and excused when the owner can demonstrate that its decisions on security measures were thoughtfully tied to the reasonably anticipated risks.

For a discussion of different size, maturity, and types of companies and trade secrets and how these factors might impact a

---

or three-person shop may be different from reasonable steps for a larger company.") (citation omitted).

26. *See, e.g.,* E.I. DuPont de Nemours & Co. v. Christopher. 431 F.2d 1012 (5th Cir. 1970) (a classic observation that "we need not require the discoverer of a trade secret to guard against the unanticipated, the undetectable or the unpreventable methods of espionage now available"); *see also* Compulife Software Inc. v. Newman, 959 F.3d 1288, 1311–15 (11th Cir. 2020).

"reasonable measures" determination for protecting trade secrets, see Appendix B.

2. Choosing appropriate measures based on the assessment

Based on the assessment of the trade secrets and the business, measures can be chosen to protect particular categories of secrets, taking into consideration their impact value, risks, existing controls, and company functions.

a. Nature of the trade secret

The nature and value of a company's trade secrets informs the selection of effective measures. For example, trade secrets can consist of business information, such as product roadmaps, customer and supplier strategies, marketing, sales, and financial performance targets, which may be adequately protected by general policies and controls. In contrast, technical trade secrets (e.g., often related to the design, functionality, and engineering of a product, how a product is manufactured (process), specialized machinery or specification to achieve a performance outcome) may have longer-term value and require more specific protection policies and measures.

Secrets can be stored digitally or physically. A design drawing can be protected with digital rights management and access governance. In contrast, secrets embodied in a machine, customized equipment, genetic material, process methods, or techniques on a manufacturing floor present different kinds of challenges to ensure adequate protection.

Trade secrets can also consist of methods or processes, compositions or specifications, and apparatuses, with corresponding differences in measures to protect them. For example, method secrets can be recorded in operating procedures, which can be protected in locked drawers and with information

security controls. However, some methods may exist primarily in the memories of those employees who use them and train others to do so (often called "institutional" or "tacit" knowledge). The fact that only a few know the secret may provide great protection from theft but also increases its vulnerability to loss or contamination.

"Negative" trade secrets present unique challenges. Where a company must experiment with multiple paths or iterations before finding the one that works or that works optimally, not only its solution but often also information related to the failed experiments can be considered a trade secret. There is often significant investment in developing what does work (know-how) and what does not (negative know-how). If a competitor knew what paths or iterations did not work, it would save time and money and thereby increase profitability by skipping all the experimentation and resulting failures. These specific negative trade secrets are sometimes improperly confused or conflated with an employee's general skill and knowledge. Negative information, however, is often documented in detail in lab notebooks, as well as in photographs of whiteboards and other data sources that are less frequently subject to corporate retention policies. Considering how and where such information resides and the extent to which it is protectable, and informing those who are aware of research failures that this negative information is itself protectable as a trade secret, may require specific attention in training and the development of special policies and procedures.

b. Different measures and varying effectiveness

Selecting protective measures is one of the most important elements of any protection program. Strong protective measures can not only prevent loss; in doing so they can build and be part of the evidence of value for collateral, mergers and acquisitions, licensing, and other corporate transactions.

Completing a thoughtful assessment and program-designing process can also help identify possible leaks or breaches in a company's security. By identifying and then mitigating these possible leaks and breaches, the entire company (not just the trade secrets) is better protected, which could be important elements of the return-on-investment package when seeking executive buy-in. While this *Commentary* cannot possibly list or describe every possible protective measure, some of them are summarized below, and additional examples and more detailed descriptions are provided in Appendix A.

Policy, process, and awareness are critical to establishing a baseline of expectations and workflows for handling trade secrets across a workforce. Physical security measures (e.g., gates, entrance door locks, safes, restricted areas) are a company's initial line of defense for trade secret protection, in part because they limit access and in part because they signal to employees and others the importance of security. If the trade secret is physical equipment or methods in operation, then campus and building security where the equipment or operations are located may be quite important. If the secret is something easily kept to a small number of those "in the know" (such as a customer target list or a formula that can be programmed into machine operations), then a strict "need to know" restriction is a quite useful, effective, and inexpensive protective measure. In other cases, separating the secret into smaller parts to ensure only a small group of people understand and can access the entire secret may appropriately balance the need to make information available internally against the risk of leakage. However, if every employee on the manufacturing floor, the quality and safety teams, and even third-party vendors need to know the particular secret in order for each manufacturing facility to function, then controls oriented solely around access privileges will need to be augmented by other protective measures such as

strong confidentiality agreements and robust training and compliance protocols.

Contractual safeguards may range from confidentiality marking requirements,[27] document retention policies, social media and electronic device policies, and contracts and policies for nondisclosure agreements and other contracts that govern trade secret information and place the receiving party on notice that particular categories of information are to be protected.

Awareness campaigns can include company-wide messaging, mandatory online training modules, and even live training or podcasts on particular trade secret topics, such as customer information sharing and protecting intellectual property in the supply chain.

3. Process for monitoring, improving the program, and incident response

A thorough and comprehensive program will generally include elements addressing monitoring and assessing the effectiveness of and compliance with the program, making improvements to the program as needed, systems for ensuring that the company promptly becomes aware of incidents of

27. "Confidentiality marking" (sometimes alternatively referred to as "labeling" or "legending") refers to the practice of placing a set of words on a document to signal to the reader how the document and the information contained therein should be handled. Some companies may adopt a scheme to indicate the level of sensitivity or the permitted use for the document, using such terms as "external," "confidential," "highly confidential," "internal use only," and "do not copy." Some companies may implement a particular confidentiality marking scheme for specific types of relationships (e.g., a technical collaboration as opposed to a supplier relationship) and may contractually negotiate for a particular confidentiality marking scheme to be applied. One practice is to include a specific reference to the governing agreement between the parties as part of the confidentiality markings to be applied to each document.

noncompliance, breaches, or loss, and a well-developed incident response plan.[28] These elements may also be factors that courts consider in determining the ongoing reasonableness of protective measures.

4. Integrated enterprise approach: Leveraging existing capabilities and processes and navigating conflicting or competing objectives

Many companies have existing functions and workflows that can be leveraged in developing a program, for example, employee onboarding and ongoing training programs. Usually, companies can add the topic of trade secrets in a way that helps employees understand what the company considers to be valuable and what employees are expected to do to protect it. Another example is document storage in IT systems. A review of the security of information technology systems may reveal an already existing strong system (e.g., passwords, encryption, firewalls, virus and malware protection, and auto backup). In this case, the strength of the system is a measure protecting the secrets, even though it may not have been initially designed solely for that purpose. In all cases, the IT system needs to be maintained and periodically reviewed for adequacy of trade secret protection and updated as needed.

However, additional program measures may still be required based on special circumstances. Carrying through the IT example, should access to files or folders where secrets are stored be limited, and who should administer and control such access? Should the secrets be segregated? If there are

28. *See, e.g.*, Hagler Sys., Inc. v. Hagler Grp. Glob., LLC, No. CV 120-026, 2020 WL 2042484, at *2, *11–12 (S.D. Ga. Apr. 28, 2020) (discussing with approval electronic security measures including tracking network activity as well as storing information on private database and requiring multiple credential levels).

weaknesses in the system, then new measures will require more extensive IT planning, modification, and implementation. If there are strengths, they can be harnessed. Identifying existing functions and workflows to be leveraged in a program can lead to effective protection with minimal business interruption and cost. The company's existing document storage system often allows for granting and withholding permission to individuals on a folder-by-folder basis, for example. Controlling access to sensitive information in the document storage system can be straightforward, with some forethought.

In contrast, some existing functions and workflows can present conflicting goals and disclosure risks. For example, companies communicate with the outside world through press releases, trade conferences, regulatory reporting, and sales and marketing efforts. The purpose and goal of these efforts is to obtain a variety of benefits by getting information about the company and its products out to the public.[29] These efforts can, however, depending on the information and the nature of the disclosure, be in conflict with the secrecy goals of a trade secret program. In developing a program, these organizational conflicts need to be identified so that a proactive plan is put in place to prioritize and intentionally decide among multiple goals (instead of reactive damage control). Engaging necessary stakeholders from the beginning and providing trade secret training to the leadership of these functions can help ensure that competing objectives are appropriately weighed.

Coordination continues to be important where trade secrets at issue relate to products that will be publicly marketed or licensed. The team would benefit from early coordination on the timing and legal impact of any public release: the existence and

29. Popular examples of this kind of technology signaling are patent applications and white papers.

configuration of a product can no longer be kept "under wraps" as a trade secret after the product is publicly marketed, for example; however, new protocols, contractual and technical, may need to be adopted to maintain secrecy over the inner workings of the released product.[30]

5. Information technology and cybersecurity

Technologies for both protecting and stealing trade secrets are constantly evolving in sophistication and availability. In most cases, however, companies already have encryption, firewalls, and other protections in place and only need to identify and mitigate gaps in the system rather than design or implement an entirely new IT security system to address external risks.[31]

Trade secrets need to be accessed by at least some employees in day-to-day activities—indeed, that is how a company derives competitive advantage. On the other hand, the digitization and democratization of these same trade secrets, which typically makes their use more efficient, makes them more susceptible to loss, by enabling their exfiltration through an errant email or on a single thumb drive or contractor's smartphone. In any program, it is essential for decision makers who are well versed in the value of particular information to strike the right balance *for the particular company* between the productivity boost afforded

30. *See, e.g.*, Broker Genius, Inc. v. Zalta, 280 F. Supp. 3d 495 (S.D.N.Y. 2017) (denying motion for preliminary injunction on a trade secret claim where the alleged trade secrets had been disclosed to software licensees under a software license prohibiting copyright infringement but imposing no confidentiality obligations or restrictions on reverse engineering; the case illustrates the potential importance of coordinating the protection of information under a variety of intellectual property regimes).

31. *See Commentary on Information Governance, Second Edition*, *supra* note 5, at 114.

by these powerful digital applications and tools and the risk of inadvertent disclosure or outright misappropriation of *particular* trade secrets. This need has only increased in importance in the wake of digital transformation and remote work environments across companies.

While securing "structured data" in databases and systems using access governance and encryption can be more easily implemented, "unstructured data" (e.g., emails, PDF, PowerPoint, Word, and Excel documents), as well as collaborative communication services such as Zoom, Slack, Monday.com, or Microsoft Teams, which are ever more pervasive in today's communication culture, can often be more difficult to secure. Classification of emails and electronic documents and adding rights-management protection for both internal and external sharing can add additional layers of security to more transient information. Becoming familiar with the security options and tools afforded by new technologies is helpful; failing to take advantage of such protections, when available and in wide use, has been found in some cases to be a failure to take reasonable measures to protect trade secrets.[32]

6. Managing and sharing information with third parties with a need to know

Certain businesses thrive or grow with the assistance and collaboration of third parties. These third parties might be key vendors or suppliers, part of R&D and the innovation process, cloud service providers, distributors, licensees or franchisees of the technology being protected, customers, or regulators and

32. *See, e.g.*, Smash Franchise Partners, LLC v. Kanda Holdings, Inc., No. 2020-0302-JTL, 2020 WL 4692287 (Del. Ch. Aug. 13, 2020), *vacated in part* (Del. Ch. Oct. 8, 2020) (finding that failure to use tools to restrict access to Zoom conference calls and to keep track of attendance evidenced failure to take reasonable measures to protect secrecy of information disclosed on the calls).

certification auditors. Protective measures adopted and designed for a company's own workforce usually are not applicable and may not be fully appropriate for these partners and third parties.

Program design should include measures that have been adapted to these third parties and the unique risks that information sharing entails in these relationships, taking into consideration any professional confidentiality obligations, legally required disclosure obligations, and other relevant factors. For example, the risk of theft by an auditor, legal counsel, or an investment banker is usually substantially different from the risk posed by an acquisition target, supplier, or customer with technology or products in the same industry.

When arms-length third parties who are not otherwise bound by professional obligations seek access to trade secrets, confidentiality agreements, pre-engagement due diligence regarding such third parties and their information security practices, and restricting exposure to only those secrets necessary for the relationship are widely used measures to control use and disclosure of shared trade secrets. Pre-engagement due diligence of a "receiving" third party's corporate culture and safeguards regarding its own confidential information can be highly informative. This kind of due diligence can include reviewing the third party's confidentiality policies, conducting public record searches (including searches of litigation filings for claims of violations), and gaining other insights into the counterparty's industry reputation and likely need for or incentive to misuse particular information. If due diligence leads an owner to believe the corporate culture and safeguards used by a third-party seeking access to the trade secret owner's information are lax even in regard to its own information, it is not realistic to believe such company will do well protecting trade secret information of a third party. The key is to learn this pre-engagement so that controls and protection can be implemented (such as security

controls, disclosure limits, protection requirements, and the like in contracts and in disclosing company's internal protocols with this third party). Conversely, when the receiving party's internal policies seem to be both sound and actually enforced, agreeing that information the trade secret owner discloses will be handled in accordance with the receiving party's existing policies may be appropriate and practical, as it will be an approach the receiving party is already following.

The terms of some protective measures when sharing information with third parties will likely be driven by the secret itself. For example, if a licensee is provided a "black box" for a key portion of the manufacturing process,[33] the contract may prohibit the licensee from opening it and require that the licensor, not the licensee, make any necessary repairs. Another practical control is to embed protection inside software code that contains trade secrets to prevent the code from being copied or downloaded on an unauthorized machine.[34]

In many cases it may not be necessary for the trade secret owner to transfer information to the receiving party's premises or computer system; information can be made accessible through use of a secure electronic site allowing the receiving party to access, but not download, information stored on the trade secret owner's computer system in a virtual data room. Technical resources may even be set to track the identity of user accounts accessing the information, a useful feature in monitoring compliance.

---

33. *See infra* discussion at Appendix A, Part C.

34. This kind of protective measure is an example of a measure that should be protected as much as the trade secret itself, since it will provide a road map to the secret being protected and potentially the key to unlocking its protection.

7. Adding new business processes or systems

Depending on the company's trade secret assessment or review, it may be necessary to develop and implement new "systems" to adequately protect the trade secrets at hand. For example, a company with an "open door" practice may need to establish a sign-in procedure for all visitors and deliveries, with a visitor log, name tags, escort requirement, express prohibitions on mobile phones or cameras in certain areas, or the like. A company that previously shared all contacts and customer prospects or technology advancements company-wide may determine that it is more appropriate to limit disclosure of this kind of information to a smaller group of individuals or add additional protections to the information shared. Many of these kinds of measures provide good protection and are not expensive to implement, but they may cause friction to those excluded from the knowledge sphere, or compliance resistance from those who prefer the less restrictive or prescriptive way of doing business. Leveraging HR in designing these measures, communicating the measures and the rationale to employees, and driving compliance (including senior managers who "lead by example") can help ensure success of the modified program.

8. Consider the stakeholders and likelihood of compliance

As a protection program is coming together, it is important to check back with the groups and individuals identified as potential stakeholders in the assessment phase. How will the measures being considered for adoption impact these stakeholders and their ability to perform their business function?

If suggested protection measures are too complicated, harsh, or cumbersome for regular operations, staff are likely to ignore or work around them in their day-to-day work. For example, implementing cumbersome or restrictive IT structure and requirements may result in numerous "shadow IT" data transfer

systems that become difficult, if not impossible, to track and manage. Employees might create their own data repositories with confidential and trade secret information that is easily accessible to them for their daily work, creating multiple copies of this sensitive information in places where access is broad or protection is light. Or employees might turn to a publicly available app or cloud tool to facilitate a team project because it is easier for their team to collaborate and share information. These types of publicly available tools can be fraught with ownership and confidentiality issues, in addition to cyber risks. Failing to consider the day-to-day practicalities and the needs of employees to perform their jobs when choosing and finalizing measures can doom the ultimate success of the program.

Consider as well the needs of stakeholder groups who have different objectives, such as marketing, R&D, and government compliance, but who may have access to the same trade secrets. Can the measures be adapted to work for all stakeholders and still provide the protection needed? Can the same measures be adjusted for these different groups' compliance? Or should different measures be adopted for them? When conflicts arise, such as when one group within a company seeks patent protection while another group believes trade secret protection is more advantageous, or one group believes that making public disclosures at a trade show is necessary to enhance a market edge while another group is concerned about the timing of the disclosure, how will conflicts be resolved?

Even if it requires more effort or changed workflows, working to understand and manage such issues should result in a better overall program as well as buy-in and compliance from these stakeholders.

9. Identify the responsible persons

Those accountable for implementation and compliance of the program should be clearly identified and made aware of their responsibilities. This is particularly important when multiple company functions, which may include HR, IT, internal audit, and intellectual property, are involved in the program, its measures, and implementation.[35] Some companies have a designated officer filling this role, while others layer this responsibility on other company leaders managing risk and compliance. As with other phases of the project, attorney-client privilege issues should be considered, along with the question of whether design and management of the program is primarily a legal function or a business function.[36]

10. Consider the costs to the company

Companies should identify and, to the extent possible, quantify the anticipated costs to the business caused by the program. Costs include out-of-pocket expenses needed to develop and deploy each of the protective measures; additional headcount that might be needed to implement and monitor controls; the expenses and distraction caused by ongoing compliance; the cost to the company in operational efficiency, throughput, or innovation; and the costs of potential enforcement against noncompliant employees, suppliers, or other third parties. Restrictions on internal information flow may inhibit the business's operations or growth, which should be factored in as well.

If the costs and risks are determined not to be reasonable, consider whether changes to specific measures or the program

35. *See supra* Section III.A.1–2.

36. *See supra* Section II.C (Attorney-Client Privilege and Business Records: A Double-Edged Sword).

overall can facilitate a better balance between adequacy of protection, risk, and cost.

11. Will the program be considered "reasonable measures" and stand the test of time?

When the chosen measures and overall program are nearly complete, it is important to take a step back and consider whether the trade secret owner can frame a reasonable argument and rationale that the program is reasonably adequate, under the owner's particular circumstances, to protect the security and confidentiality of the secrets. If so, the trade secret owner has likely taken "reasonable" measures to protect its information.

Keep in mind that reasonable measures do not mean "all possible measures." Recall that the fact-specific analysis of the "reasonableness" evaluation in litigation requires consideration of the totality of the circumstances and is always considered in hindsight. The core inquiry is whether the measures were appropriate against the backdrop of the risk of loss and the perceived value of the information within the context of the specific company.[37] This is a good time to reevaluate the overall balance among the protection of the secrets, the ability of the company to operate and achieve its business goals, and the relative costs of implementing the program versus any potential loss of the secrets.

37. Xavian Ins. Co. v. Marsh & McLennan Cos., Inc., No. 18cv8273(DLC), 2019 WL 1620754, at *5 (S.D.N.Y. Apr. 16, 2019) ("Each owner must assess the value of the material it seeks to protect, the extent of a threat of theft, and the ease of theft in determining how extensive their protective measures should be." (quoting the Congressional Record for the Economic Espionage Act of 1996, 142 CONG. REC. S12213 (daily ed. Oct. 2, 1996) (Managers' Statement for H.R. 3723, the Economic Espionage Bill))).

Regardless of what measures are ultimately selected and implemented, starting and then making continuous improvements can enhance the safeguards and increase the likelihood that they will be found to be both successful at preventing loss and "reasonable" in the eyes of the law.

IV. IMPLEMENTATION AND MAINTENANCE OF THE TRADE SECRET PROTECTION PROGRAM

A. Implementing the Program

No matter how good a program is on paper, it cannot by itself protect trade secrets, let alone withstand "reasonable measures" scrutiny, if it is not properly implemented and maintained. Indeed, a common defense argument in an enforcement proceeding is to point out anything in a program that was adopted but not implemented consistently.

As discussed above, a successful implementation roadmap requires buy-in from key stakeholders and management, and one way to ensure their endorsement is to fully inform them of the business and operational benefits and articulate a clear return on investment (ROI).

1. Implementation planning and execution

An implementation plan should provide clarity on the "who," "what," "when," and "where" needed to perform the implementation and what constitutes completion. Implementation usually involves rolling out individual policies, training, and awareness campaigns, ensuring necessary business processes are in place, and installing any new technical or physical measures. Some programs may be better implemented in stages, while others should be introduced all at once. If the program is being implemented in stages, attention should be paid to the potential implications for an enforcement proceeding arising out of activities or occurrences during the staged implementation as well as comparisons between the "new" program and earlier measures that may be being litigated.[38]

38. *See infra* Section IV.B.3 (Maintaining Compliance—Monitor and assess compliance).

Once execution begins, progress should be monitored, and impact should be measured.[39]

2. Program launch and communication

Communicating the adoption of the program or the individual policies to all affected persons and companies offers an opportunity to set the tone from the top (and not just from counsel) regarding the value of the program and to gain participation and engagement from every employee and affected third party. This communication may be tailored for various audiences. For example, in a small company that does not generally share information with outside third parties, the launch may consist of a simple email message. However, for a large, multinational corporation with several divisions and locations that work with many third parties in high-risk regions, there may be several different communications to different audiences. No matter who the audience is, a good communication effort can drive effective compliance.

Program "launch" may be a misnomer in that most companies already had some safeguards in place to protect trade secrets. In many cases, a well-considered program such as described in this *Commentary* will be primarily in the nature of enhancement and refinement to prior approaches, offering the added benefit of visibility into the return on investment of the adopted measures. Companies would be remiss in ignoring ways in which they are building on prior approaches to protect and ultimately manage their trade secrets, and they can often benefit from recognizing any existing measures as well as emphasizing the business advantages of new measures and any refinements to existing measures. Otherwise, the program can

39. *See id*.

come to be seen as simply one more set of "legal homework" rather than a value-enhancing tool.

3. Training and awareness

Training and awareness should be the initial focus of any program launch, particularly where the program is aimed at changing behaviors among the workforce. Designing rules and processes in a vacuum, without a dedicated effort to drive and sustain broad adoption, quickly risks unraveling the program. As with the communication plan, consideration should be given to tailoring training for the various impacted groups. For example, if the program includes a new process for logging and escorting visitors to a site, the employees who will be receiving the visitors most likely have no need to know what the trade secrets are but do need to understand the process being implemented and the importance of compliance. However, at this same company, the persons who will be meeting with the visitors and presenting information about the company and its technology do need to know what is and is not a "trade secret," and therefore, what information can be disclosed to these visitors and what "marking" or other identification processes are required, either by the program or by applicable third-party contracts. Training and awareness initiatives should be repeated at appropriate periods to ensure the measures and processes remain effective.

When third parties are part of a program, companies need to decide whether to direct any training to these third parties. This decision may depend on the scope and value of the trade secrets to which the third party has access as well as the nature and duration of the relationship. For example, a licensee of process technology who will be operating a facility using that technology probably has access to a large amount of valuable trade secrets, and targeted training may help reduce the risk of leakage or other misuse.

4. Update and integrate into business and legal processes

Programs should embed policies into existing business processes where possible to drive high levels of adoption and ensure process discipline. For example, it would be desirable to reference the "need to know" policy from the company's trade secret program document when describing the process it uses for deciding which employees will be granted access to which trade secrets, or when explaining how a new work-from-home protocol is supported by the network safety and security measures. Implementation plans should try to anticipate these issues and plan accordingly. Working with the right stakeholders (e.g., IT, HR, or specific managers) to integrate security measures into the overall, regular business workflows will help with ongoing compliance. A compliance and enforcement program can reinforce proper implementation.

5. Update physical and IT infrastructure

Some programs will require physical installations or implementation of additional technological tools and processes, for example, locks on file cabinets or storage rooms, barriers (e.g., gates or locked doors) to entry in sensitive areas, computer hardware (such as firewalls and redundancies), or additional password or authentication protocols. Distraction or loss of productivity while such installations are deployed are best minimized with good preplanning and advance communication or training.

6. Document the program and implementation

Thinking ahead to enforcement, efforts should be made not only to document the program itself, but also its implementation. An effective program may include components that remain in place for a very long time—having a record of when

and how the implementation occurred may be important to demonstrate in enforcement proceedings.[40]

B. Maintaining Compliance

Ongoing compliance and enforcement, as well as periodic review of the program's relevance and effectiveness, can be as important as the program design and initial rollout. Building a culture of familiarity and compliance with a company's program, enforcing protections against breaches when necessary, and regularly monitoring, measuring, and enhancing the program over time can all be vital not only in demonstrating in an enforcement case that a company's trade secret protections were reasonable, but—even more significantly—in reducing the likelihood that trade secrets will be lost, stolen, or disclosed in the first place.[41]

1. Culture of confidentiality and compliance

Developing a "culture of protection" can help to sensitize the entire company (management and staff) to the importance of protecting the company's most valuable information. It can also help people more readily recognize risks in particular situations

---

40. *See supra* Section II.C (Attorney-Client Privilege and Business Records: a Double-Edged Sword).

41. This is not a hypothetical risk. Consider this example drawn from a real-world case: A CEO found a person in his company's conference room after 7 p.m. downloading the company's confidential information. After dealing with the situation and upon investigation, the CEO found out that the person had gained access to the company's offices, walked around taking pictures, and then set up in the conference room where he worked on his computers for hours before being confronted by the CEO. Not one person in the company asked him who he was or what he was doing. Clearly, this company did not have a "culture" of confidentiality or good compliance with its policies—which were reported to require all visitors to sign-in and be escorted and were prohibited from taking pictures without permission.

and to report or take other appropriate and timely action. A confidentiality culture can be built in ways similar to other company cultures, such as physical safety and legal compliance (e.g., relating to securities laws, Sarbanes-Oxley Act compliance, product safety, ethics and anticorruption, and quality requirements). Accomplishing this involves setting the tone at the senior management level, promoting company-wide buy-in, taking thoughtful, affirmative steps to implement policies, and continuing to nurture and message the importance of the issue and the company approach among managers and staff. This is often done in conjunction with HR through training, regular communications, positive reinforcement, and other strategies to build a collective and pervasive appreciation for secrecy and protection.

2. Encourage and facilitate compliance

Periodic communications and reminders, additional or refresher training, and a "secrecy" performance metric in employee reviews can help encourage compliance. So can performing occasional internal "audits," even informally (e.g., conducting a walk-around to determine who is complying with the "clean desk" policy, what desks and file cabinets are locked, whether whiteboards contain confidential information, etc.), and reporting the aggregated results to the entire company (as well as privately counseling those not in compliance).

Facilitating compliance is a slightly different concept. Care should be taken to ensure existing company goals, directives, policies, and practices do not conflict with the new or refined policies and procedures of the program (or vice versa) or create situations where employees become unsure about priorities or their ability to comply with both policies. Coordination of policies may be necessary. For example, a new document retention policy might be issued that could put records of trade secrets at risk for destruction, or office renovations might make it more

difficult to keep confidential information out of sight of visitors. Policies to promote the filing of patent applications or to heavily reward only those applications that are granted (thereby potentially encouraging inventors to add more disclosures in the specifications, e.g., performance or process data, in an effort to bolster the likelihood of issuance of particular claims) may limit the long-term ability to claim particular information as a trade secret. A workforce that begins or stays working remotely can present special difficulties in protecting the company's secret information and may require new approaches to making information securely available offsite. New risks or obstacles to compliance need to be assessed; in some cases, new solutions may need to be designed to adapt to changed circumstances.

While there is no one-size-fits-all approach for implementing these compliance elements, special attention should be given to the teams or persons responsible for compliance, attorney-client privilege issues, and whether business records should be purposefully created and recorded regarding the periodic compliance efforts, findings, and any responsive actions.

a. Internal issues and variations

Ensuring the workforce understands what is secret and how to protect it is an essential aspect of compliance. Not every employee or contingent worker, however, may need to know the same degree of detail about what the company desires to maintain as a secret. This may depend on the nature of each of the staff's roles and responsibilities with respect to the products and services in which the trade secrets are embedded.

For example, in a chemical manufacturing process for manufacturing X product, the marketing, sales, finance, and even the shift operators running the software to make product X should know that the process for manufacturing product X generally contains one or more of the company's secrets; while

other members of the technical staff such as process engineers and chemists may need to know much more detailed information about the secrets associated with manufacturing X; such as, for example, the importance and secrecy concerning each of the critical steps, conditions, or ingredients used in the process. If the trade secrets have been identified with some degree of detail, then this type of sequential need-to-know instruction may be more easily accomplished than if the trade secrets involved in manufacturing product X have not been identified to such a detailed level. In other situations where little detail has been shared, compliance may be effectively achieved by informing all staff that the manufacturing process for product X contains trade secrets and the only information that staff may disclose to others is what is disclosed on the company's webpage concerning product X.

Different "groups" or divisions may require different approaches to encouraging compliance. Some companies may want R&D personnel to collaborate internally across product lines, for example, in efforts to improve or discover new processes and products, while others may direct that R&D personnel focus on only one product. Similarly, the purchasing department may need to know specific aspects of current or planned trade secrets to acquire the correct raw materials, tools, supplies, or services but may not need to learn about manufacturing processes, other than to estimate the timing of needed supplies. One group within the company may be encouraged to be open within the company's four walls or within certain protected third-party relationships (e.g., a joint development partner under a nondisclosure agreement), while another group might be given very strict rules regarding disclosures internally and externally (e.g., purchasing may be aware of trade secrets related to raw materials, but it may be prohibited from making any disclosure to a third party without a supervisor's prior approval). Each of these choices may be appropriate for a particular

company and particular trade secrets—but the decision of how to manage particular information needs to be made as part of an overall strategy, rather than as a "catch-up" decision.

Despite best efforts in the designing and implementation stage,[42] a company may come to realize compliance is suffering because the measures' requirements are too complicated, restrictive, or cumbersome. If this happens, the stakeholders and program leader should consider whether changes will improve compliance and still adequately protect the secrets, or whether the measures are necessary and worth the extra effort.[43] The decision needs to be carefully communicated to the relevant stakeholders and those who will be operating under the program.

b. Third-party issues

Companies need to decide whether contracts alone provide adequate protections for trade secrets entrusted to third parties, or if the company also needs to encourage or monitor compliance in specific ways. For supply chain partners, many companies will want to impose specific requirements (e.g., individual confidentiality agreements from the third party's employees, training for the third party's staff, segregation of the company's secret information, or periodic compliance audits).

Licensees and collaboration partners present related but different risks. Some licensed information can be at the heart of a company's competitive advantage; so can some information presented as part of a collaboration. The contracts for these relationships should typically include multiple protective provisions (e.g., confidentiality, limited use, nontransfer or nonassignability, termination rights after a change in control, audit

42. *See supra* Section III.B.2 (Choosing appropriate measures based on the assessment).

43. *See infra* Section IV.C (Periodic Assessments and Improvements).

rights, and dispute resolution provisions). For collaboration partners, there is added complexity, since technical people from more than one company will be working together. This can also happen in a more limited way as a part of know-how transfer to a licensee. The counterparty may want to disclose and discuss novel discoveries or ask probing questions due to curiosity or a desire to further the project's goals. In any case, these situations are fraught with the potential for unintended disclosure and therefore need careful management. Encouraging and monitoring compliance in these relationships can involve a delicate balance between protecting secrets and meeting the objective of the contract and the parties.

Attention should also be given to the question of whether a supplier or other third party to whom disclosures will be made will in turn have a business need to disclose information to others in order to perform under the contract. If so, both contracts and processes will need to be crafted to control those onward disclosures and ensure that those who will receive information from the contracting party become obligated to treat it as confidential. Otherwise, the information may be fatally compromised.[44]

---

44. *See, e.g.*, Turret Labs USA, Inc. v. CargoSpring, LLC, No. 21-952, 2022 WL 701161 (2d Cir. March 9, 2022). In *Turret Labs*, the court affirmed a summary order dismissing trade secrets complaint where plaintiff had authorized its exclusive licensee to grant access to other users to access and use plaintiff's software without imposing any requirement that licensee limit the further users only to those who had entered into agreements to safeguard and not reverse engineer the computer program. The court found that these contractual failings were not overcome by the fact that plaintiff had taken other measures to protect the secrets while they were solely under its control, accepting the district court's finding that the circumstances were akin to "a Plaintiff having pleaded that he locked all the upstairs windows of his house, while remaining silent on whether the front and back doors were left wide open."

If specific notice or confidentiality marking requirements have been agreed to, they need to be communicated and followed to avoid a risk of being found to have forfeited protection.[45]

Contractual obligations to return or destroy confidential information may present some practical implementation issues, particularly at the conclusion of the collaboration. Most confidentiality obligations contain a requirement (either automatic or upon request of the disclosing party) to return or destroy confidential information at the conclusion of the project or termination of the agreement. However, in practice, it may not always be clear exactly when these contracts have "ended" until long after it has occurred. Further, "destruction" of digital data, even by parties acting in good faith, can become enormously expensive, and less burdensome requirements may be appropriate in particular situations (such as a requirement to render certain information "inaccessible through ordinary means"). Companies should be mindful of such clauses and act appropriately for their particular situation.

c. Managing disclosures to government entities

In many industries, occasions may arise where disclosures of confidential information to regulators or government entities may be important or even required. Disclosure can present numerous challenges for companies that want or need to be compliant with government requests for information while at the same time protecting the trade secret nature of that information. The primary challenge is that most government activity is accessible to the public and, under the Freedom of Information Act and various state law analogs, most documents in the

45. Convolve, Inc. v. Compaq Comput. Corp., 527 F. App'x 910, 924–25 (Fed. Cir. 2013). *See infra* note 61 for relevant discussion.

government's possession are susceptible to public disclosure upon request. At least one court has held that the Defend Trade Secrets Act does not provide an exemption from its state's public records law's disclosure requirements, which may mandate that certain disclosures be made available to the public.[46] Further, a governmental agency (or an individual inside the agency) may publish the information inadvertently or even purposefully with little or no availability of recourse to the owner of the information.[47] Thus, the guiding principle, whenever possible, will often be to avoid disclosure of trade secrets to the government.

However, this approach is not always feasible, particularly in the context of government funded projects, government investigations, certain regulated industries, and company referrals to the government for criminal prosecutions of trade secret theft. For example, when seeking government funding for an R&D project (or complying with the government conditions after receiving government funding), it may be impossible to avoid disclosing information that is commingled with some trade secrets. Other examples may include requirements for the submission of performance data, metrics, or safety or other information.

In making disclosures, the company should ensure that it is compliant with the government mandate, regulations, or

46. Fast Enterprises, LLC v. Pollack, No. 16-cv-12149-ADB, 2018 WL 4539685 (D. Mass. Sept. 21, 2018) (holding that the DTSA does not override the applicable Massachusetts public records laws, which mandate disclosure unless the information is "specifically or by necessary implication exempted from disclosure by statute").

47. While the Theft of Trade Secrets Act, 18 U.S.C. § 1905, enacted in 1948, provides for criminal penalties for the disclosure of trade secrets by federal employees except as permitted by law, it does not provide for injunctive relief or civil penalties.

request but not overinclusive in exposing trade secrets not required to be disclosed by law. When trade secrets or confidential business information are disclosed, the company needs to be sure to properly designate its disclosure as such and be prepared to support the designations factually.[48]

In addition, companies may receive subpoenas for witness testimony or documents in connection with regulatory and government investigations in which it is not a target but has relevant information. This can occur in the U.S. and, for multinational companies, in foreign jurisdictions as well. This can be particularly complex for a company in the context of cross-border disputes. Companies should be aware that such disclosures may be subject to disclosure in litigation or in response to requests by third parties and should consider whether particular disclosures can be appropriately limited or designated as not for disclosure.

When a company makes the decision to refer a matter for criminal investigation and prosecution, the company must also carefully consider what information it provides voluntarily or

48. *See* Freedom of Information Act, 5 U.S.C. § 552(b)(4) (the "confidential information" exemption) and (5) (the "trade secrets" exemption, amended by OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524). *See also* Food Marketing Inst. v. Argus Leader Media, 139 S. Ct. 2356, 2366 (2019) (discussing differences between the "Trade Secret" exemption under the Freedom of Information Act, Section 5 and the "Confidential Information" exemption; to gain the benefit of a requested exemption the company needs to be able to offer a factual basis for doing so). *Cf.* Sepro Corp. v. Fla. Dep't of Envtl. Prot., 839 So. 2d 781, 783 (Fla. Dist. Ct. App. 2003) ("[Under Florida statutory law], the failure to identify information furnished to a state agency as putatively exempt from public disclosure effectively destroys any confidential character it might otherwise have enjoyed as a trade secret."). For a further discussion on identifying information as trade secret that may be also useful in connection with government disclosures, see *Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases*, *supra* note 21.

subject to subpoena. In some cases, voluntary production will not be entitled to as robust confidentiality protections as information that is produced subject to a subpoena. The company should carefully review any protective orders in place to determine what, whether, and how its trade secret information will be used and safeguarded during and after the conclusion of the matter. In other circumstances, the government may seek to compel third-party disclosures for its own investigation (e.g., into an automobile safety issue that involves an automaker's secrets) or for a "public purpose" (e.g., the federal government considering compelling disclosure of manufacturing methods of vaccines in a pandemic). The producing party should make similar evaluations of applicable confidentiality safeguards in deciding how to proceed.

In situations where trade secrets and other sensitive information must or, in the judgment of the trade secret owner, should be disclosed to a government agency, various strategies can be utilized to make the required disclosure while still protecting (in a reasonably reliable way) the confidentiality of the secrets.[49] These strategies should be considered and established *before* any such information is disclosed.

The most important considerations in making any government disclosure are understanding (1) the nature and scope of the government request, including whether compliance is voluntary or mandatory; (2) the protective measures in place or that may be lawfully requested by the disclosing party (protective order, confidentiality agreement, or other safeguards); (3) the protocols for securely storing, segregating, accessing, and

49. *See* Elizabeth A. Rowe, *Striking a Balance: When Should Trade Secret Law Shield Disclosures to the Government?*, 96 IOWA L. REV. 791 (2011), for a deep discussion of the concerns of disclosures to the government, case law surrounding private parties seeking to protect the disclosed information, and Professor Rowe's arguments for balancing the competing interests.

destroying the information, particularly if the information is in digital form or on hard drives or other devices; and (4) restrictions on current and future uses or disclosures of the information and the related need for the disclosing party to designate the provided information as being subject to available restrictions.

If the pending disclosure is related to a governmental body in connection with grant funding or a collaborative R&D project involving a governmental body, there are occasions when some governmental bodies will enter into a confidentiality arrangement, which may include a protocol to be followed for confidential disclosures. Such procedures are not, however, always available to disclosing parties.

Many companies identify a select person(s) through whom all disclosures to the government will be made or require that certain persons review disclosures before made. This is especially important in a research or collaborative situation where there are often regular discussions with government representatives that include providing data, reports, and presentations.

Depending on the jurisdiction and applicable law and agency rules, companies can seek reasonable time, safeguards and protocols, and restrictive measures to ensure the information is protected and returned. Seeking confidential treatment for information that is being or has been disclosed to a government usually consists of specifically identifying all information (line by line) in the document sought to be released or disclosed and providing the justification for its confidential treatment. It is rarely acceptable to indicate an entire document is to be treated confidentially; rather each word, graph or sentence that contains the highly sensitive information is marked. The justification for the confidentiality or trade secret designations varies based on the governing law and the context, but it typically requires balancing the disclosing party's intellectual

property rights and the potential loss to competitive advantage if a trade secret is disclosed, and the extent to which the nonredacted information for release satisfies the overarching right of the public to know.

Companies may also be required or may need to consider making filings with state governments. In doing so, companies need to investigate differences between state law approaches to protecting filed information and should not assume that all state laws are the same or are the same as federal statutes. State laws vary, for example, on matters such as when the submitter will be apprised of any request for disclosure, whether the submitter is permitted or required to intervene to prevent disclosure, whether an agency or a court makes initial decisions regarding disclosure, whether a stay of disclosure is automatic pending final decision, whether exemptions are categorical, and what burdens the submitter and the party requesting information must satisfy.[50] Close attention to differences in relevant disclosure schemes may assist a submitter in determining whether to submit particular information at all in particular jurisdictions and how to designate the information if disclosed.

Further, disclosures of information to third parties who may themselves need to make government disclosures should be

50. *Compare, e.g.*, Long v. City of Burlington, 199 A.3d 542, 550–51 (Vt. 2018) (holding that if the *agency* receiving information establishes that it is a trade secret, the information is "exempt" from disclosure since, among other things, otherwise "contractors and service providers may decline to cooperate with the state") and Lyft, Inc. v. City of Seattle, 418 P.3d 102, 115 (Wash. 2018) (construing Washington's Public Records Act not to include a categorical exemption for trade secrets and to require production unless the *filers* establish *both* that "public records disclosure would clearly not be in the public interest *and* that disclosure would substantially and irreparably damage any person or would substantially and irreparably damage vital government functions," and remanding for further proceedings). Both schemes differ from the Freedom of Information Act scheme.

accompanied by guidance to the third parties about how to make those filings in a way that protects the information. Otherwise, the third party may fail to claim confidential treatment, irretrievably exposing the information to the public.[51]

No matter how or why the information is disclosed, taking additional steps to prepare an inventory of what was provided to the government, marking the information as confidential, and providing a cover letter with any appropriate requests and designations under the Freedom of Information Act or other applicable laws is important. This should be done upon each disclosure (not after the fact).

Some companies may, on assessing these challenges and variations in applicable law, determine as a business matter not to voluntarily share particular information in specific jurisdictions, a decision that likely will have business consequences that will need to be evaluated by company strategists.

d. Responsible persons for managing compliance

A company's management of its compliance and enforcement efforts, like the overall management of its program, does not necessarily need to be centralized, as described above. But it is important as a practical matter that all relevant business leaders communicate and coordinate with each other in managing compliance issues to ensure consistency.

51. *See, e.g.*, M.C. Dean, Inc. v. City of Miami Beach, 199 F. Supp. 3d 1349 (S.D. Fla. 2016) (subcontractor's failure to impose confidentiality restrictions on contractor to which it disclosed information had no claim for misappropriation or redaction when contractor filed information with the city without designating it as confidential; failure to designate filing as confidential permitted the city to make the information available to requestors without redactions).

3. Monitor and assess compliance

Regardless of how a company's program may be designed and implemented, it is helpful to have good management systems in place to organize, monitor, and deal with ongoing compliance. Some of these may be electronic and automatic. Others may involve periodic meetings, analysis, or even performance metrics or audits of staff or third parties. Examples of monitoring and measurement activities that can help to ensure that the various elements of a company's program are regularly carried out include the following:

- *Audits.* Routine or periodic internal auditing of controls and employee team compliance with all or specific protective measures can be used. Audits can target several items, e.g., completion rates of mandatory training sessions, physical measures (are the doors and file cabinets locked, are visitors being escorted, are cameras being used in restricted areas), or contracts (are confidentiality agreement requirements being adhered to, are confidentiality agreements with ongoing relationships current or expired, and do they cover the discussions or activities taking place today). These reviews or audits can be conducted in a spot check or comprehensive manner, randomly or routinely, focused on specific measures or all measures. The most important part of these audits or reviews is that there is follow up. If breaches or lapses are discovered, some kind of mitigating or corrective action should be taken or some communication issued to encourage compliance.
- *IT threat monitoring.* Technologies exist today to perform internal and online IT threat monitoring (e.g., unusual download behavior, specific drive or file access, or cyber breaches). Some electronic

technologies can log activity associated with sensitive files or folders (e.g., access, open, edit, save, copy, or sent). Artificial intelligence, predictive coding, and behavioral analytics can be used to identify possible threats to or losses of the company's trade secrets. Some of these technologies are sophisticated and expensive, some less so. Depending on the trade secrets and circumstances, these systems can be very valuable in monitoring trade secrets and flagging risky or suspect behavior or digital transactions. On the other hand, use of these technologies (like most other measures) is not a necessity to have an overall program that provides effective protection, let alone demonstrate that the company took appropriate reasonable measures.[52]

- *Contracts and processes review.* Companies can and should periodically review and update the forms of contracts, employment agreements, and terms and conditions on purchase orders and invoices, as well as the processes (and compliance with processes) required for appropriate reviews of the same before execution to ensure trade secret and other intellectual property rights are protected. Such process reviews also can help maintain conformity of language and terms, which is an important trade secrets compliance element, as well as one relevant to reasonable measures effectiveness. Contracts for a collaborative relationship in which both sides receive and disclose information, especially when the parties are working on R&D together, require careful and thoughtful attention, particularly understanding the technology

52. *See Sedona Employment Life Cycle Commentary*, *supra* note 8.

involved and the way the business and R&D personnel intend to work together with the counterparty, so that the terms of the contract allow for a successful collaboration while also protecting the secrets. Confidentiality marking requirements should be assessed for workability.[53] Companies should also consider, in particular, whether a time-bounded confidentiality obligation (e.g., for ten years) is appropriate or necessary from a business standpoint for particular information, and the consequences for such limitations legally.

- *Metrics (Key Performance Indicators).* Documented performance metrics can be used to measure items such as whether policies, procedures, and records requirements are being followed, the number of breaches or noncompliance incidents, and the understanding, capabilities, and performance of employees in complying with the company's program.
- *Monitoring of third parties.* Due diligence and monitoring of contractors and third-party business partners as to their understanding, capabilities, and performance in complying with the company's program or contractual secrecy obligations can be conducted. Depending on the secrets and the third parties, this can include periodic physical or digital audits of the third party. This can further include a vendor management office or procurement program that evaluates the effectiveness of a vendor's internal security controls before vendor contracts are executed, followed up by annual audits and updates to address new standards and technology.

53. *See infra* Appendix A, n. 61 for further discussion.

- *Trojan horses.* Intentional typos and distinct markings on key documents or code can be used to prove trade secret misappropriation if the document (or portions of the document) shows up in the hands of a third party or on an employee's personal device.
- *Trade Secret Protection Program Testing.* Certification and ongoing analysis of the company's protections can be conducted, including periodic testing and program reevaluation to show that a program is both a policy and a practice. Some third-party certifications can both improve the program and monitor compliance through external certifying audits with formal or informal standards, such as the NIST Cybersecurity Framework.[54] Some of these internal compliance efforts may also augment efforts to demonstrate the reasonableness of the program's measures in future litigation.
- *Data protection systems testing.* Desktop or tabletop exercises can be run to test the company's data protection systems. Examples of this include simulations

54. *See generally* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Version 1.1 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. The NIST Cybersecurity Framework ("Framework") "focuses on using business drivers to guide cybersecurity activities and consider[s] cybersecurity risks as part of the organization's risk management processes." *Id.* at v. Further, the Framework provides a common mechanism for organizations to: "1) Describe their current cybersecurity posture; 2) Describe their target state for cybersecurity; 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process; 4) Assess progress toward the target state; 5) Communicate among internal and external stakeholders about cybersecurity risk." *Id.* at 2. Ultimately, the Framework is a "risk-based approach to managing cybersecurity risk." *Id.* at 3; *see also* NAT'L INST. OF STANDARDS & TECH., CYBERSECURITY FRAMEWORK, https://www.nist.gov/cyberframework (last visited May 31, 2023).

of trade secret security breaches, hiring "hackers" to try to breach security controls, designating a "red team" and a "blue team" of employees to carry out and defend against a simulated attack, or practicing response procedures in the event of a breach. These disaster response exercises should also address physical or natural disasters such as earthquakes, fire, hurricanes, tsunamis, or even pandemics.

- *Monitoring of publicly available information.* Systems can be established to monitor for disclosures or losses of the company's secrets through periodic searches of the internet, social media, patent applications, and other publications. Establishing routine open-source intelligence searches to capture the company's secrets is a simple yet surprisingly effective way to uncover potential or actual losses—and to help companies reassess whether information they had previously claimed as a trade secret is now known within the relevant industry through legitimate means.

C. Periodic Assessment and Improvements

Change is constant. The trade secrets themselves, their value to the business, the risks of loss, and the effectiveness of measures to protect secrets can all change over time. Indeed, some trade secrets have a short life because a patent is filed, competitors develop the same secret on their own, the secret has been disclosed (purposefully or inadvertently), and many other reasons even if the program is quite sound. With respect to a program and risk mitigation, these changes can bring significant threat of loss. An undertaking to assess, evaluate, and update a company's program on a regular basis, for example, once a year, can be an important step in maintaining reasonable and

effective protections and in prompting compliance on a continuing basis.

As discussed above, special attention should be given to the positions or teams responsible for such reviews and potential program changes, attorney-client privilege issues, and whether business records should be purposefully created and recorded.

1. Assess changes in secrets: their value and risks

Periodic review and assessment of the company's trade secret portfolio (specifically identified or not), as well as the relative value of the secrets is an important item to begin a periodic review. Has the technology, apparatus, product, or business practice changed or been completely replaced? Has the value of it changed (either by increasing or decreasing in value)? Have new trade secrets been created? If so, what is their value? Consider any changes to the company's business strategy, locations, structure, and practices. Do these changes impact the secrets?

Based on an understanding of these changes, an updated risk assessment is the next important item in a periodic review. How have the risks changed? Has the potential impact of the risks, if realized, changed? Has technology (particularly IT and cyber practices) increased or decreased the risks? How do changes in the company's business strategy, locations, structure, or practices impact risks to trade secrets?

2. Review the effectiveness and relevance of measures in the program

With the assessment in hand, the company should review its program's elements and measures, evaluate compliance internally and by any third parties, examine any problems that have arisen (e.g., adaptations to or circumventions of measures, compliance failures, breach incidents, or material trade secret loss). In light of these trade secret, value, risk, and compliance

assessments, a company can evaluate the effectiveness and adequacy of its program to protect the secrets under these "new" circumstances. This evaluation should also include the relevance of each measure. Given certain combinations in the changes, some measures may be found to provide very little protection and therefore can be stopped as irrelevant or ineffective.

3. Adapt, update, and improve the program as necessary

With the assessment and evaluation completed, the company can then make any adaptations, improvements, or additions to the program to protect its then-current trade secrets within the context of the then-current circumstances. Note that this kind of evaluation can result in determining the plan is overkill in some areas (leading to removing some measures from the program), as well as determining that it is lacking in others (leading to entirely new measures being added). Improvements could also be directed to modifying existing measures or wholly focused on compliance with the program that exists.

Some may argue that this assess, evaluate, and adapt exercise (resulting in changes to the program) may open the company up to attack in an enforcement action. Specifically, a defendant may posit that the program should have been designed this way from the beginning, or that taking away a measure destroyed the program's reasonableness. Of course, making no changes to a program once implemented raises a similar risk: that because of changes to the secrets, the values, or the risks, the program was no longer adequate and no longer reasonable under the circumstances to protect the secrets. In light of this kind of Catch-22 situation, assessing, updating, and adapting to *actually* protect the secrets is generally the wiser—and more reasonable—course of action.

If significant improvements (whether implemented at one time or sequentially) in the program are implemented, such as, for example, new rules for working at home and accessing trade secrets, it may be advisable to articulate the rationale for the improvements and why they were not implemented previously. This may be useful in an enforcement proceeding to rebut any defendant challenge that the need for the improvement is evidence that the prior program was not reasonable. Pointing out the rationale for the improvements and why it is being made at a particular time (e.g., we discovered that x safeguard was not as effective as we had wanted and that the new improvement addresses the safeguard) will be better evidence that the effectiveness of the existing program was being monitored and improved. While it shows that the prior program was not perfect, it was reasonable, and reasonable improvements were made.

V. ENFORCEMENT OF THE TRADE SECRET PROTECTION PROGRAM

A company's approach in taking action against noncompliance, breaches, and potential losses can itself be evidence of reasonable measures to protect its trade secrets—or conversely, unhelpful counterevidence if these are not done.[55] Indeed, enforcing protections against breaches when necessary,[56] along with regularly monitoring, measuring, and enhancing the program over time, can all be vital not only in demonstrating the program is reasonable, but also in actually reducing the likelihood that trade secrets will be lost in the first place.

A. Ensuring that the company learns of noncompliance, breaches, and losses

A company can do nothing about an incident of noncompliance, breach, or loss if it does not know it happened. The company should take proactive measures to learn of any such incidents. Monitoring compliance should reveal problems as they arise. Losses can be identified through internal investigations and audits, audits of third parties, regular internet, literature, or patent searches, and software to monitor digital and system transactions. A culture of compliance should lead to "see something, say something" behavior, which might expose incidents or near misses that monitoring alone might not reveal—as well as self-disclosure of mistakes made by an employee.

---

55. For example, allowing computers with an out-of-date operating system and that had not had a security update in three years to connect to a company's network has been cited by the Federal Trade Commission as evidence of failure to provide reasonable protections for confidential customer data. Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 241 (3d Cir. 2015).

56. *See, e.g.*, Pre-Paid Legal Servs., Inc. v. Harrell, No. CIV-06-019-JHP, 2008 WL 111319, at *11–12 (E.D. Okla. Jan. 8, 2008).

B. Incident response

Whenever there is a suspected or actual material lapse in compliance, a breach, or other loss, the company should have a plan in place for how to react or respond. Quick action is helpful and, in some instances, may be necessary in order to (1) prevent additional losses; (2) demonstrate reasonable measures in an enforcement proceeding; and (3) quickly secure meaningful judicial relief such as a temporary restraining order or preliminary injunction.[57] A response plan should provide for: (1) prompt steps to secure the trade secrets; (2) procedures for conducting a comprehensive investigation; and (3) corrective measures, including an evaluation of whether employee discipline or termination or legal action is appropriate.

The exact contours of efforts to secure the trade secrets will vary depending on the situation. For example, it may involve shutting down an employee's or third party's access to the company's facilities and IT systems. It may include wiping any device that is in the individual's control (recognizing, however, that evidence may be lost in the process) or requesting its prompt return. It could also include approaching a former employee or third party to request return of information or equipment, together with assurances sufficient to protect the information going forward. It could involve agreeing on the appointment of a forensic specialist to image and delete or render inaccessible trade secret information, or working separately with such a specialist to analyze usage and access patterns. A full investigation may be followed by one or more of these steps before litigation is commenced.

57. Alamar Biosciences, Inc. v. Difco Labs., Inc., No. Civ-S-941856 DFL PAN, 1995 WL 912345, at *6 (E.D. Cal. Oct. 13, 1995) (4-year delay was inexcusable).

1. Conduct an investigation

Whenever there has been a material or repeated lapse in compliance, a breach, or other incident where there was an actual or potential information loss, an investigation should be conducted. The process should seek to preserve relevant evidence and determine what happened, why it happened, who was involved, whether the breach of compliance was deliberate, inadvertent, or due to a system deficiency, and the nature and impact of the loss. It is often wise to include in-house or outside counsel in any investigation to protect communications as privileged and, if it were to lead to a dispute or enforcement action, establish work-product protection.

Early investigation could reveal vulnerabilities or gaps in the overall program or specific measures that may need updates or improvements. It may provide key information related to compliance and potential gaps or weaknesses in the company's monitoring efforts. Most importantly, the company can make an informed judgment about what, if anything, has been lost, how it was lost, and what to do about it.

2. Take corrective action

Based on the results of the investigation, leadership (often with the advice of counsel) should determine what remedial actions should be taken. Depending on the circumstances, this may range from very modest and discreet steps (e.g., secure the trade secrets and modify aspects of the program), to additional employee training or employee discipline, up to seeking formal remedies (e.g., temporary restraining order or preliminary injunction).

An incident response plan should be followed carefully and expeditiously in the event of a cyber breach or other trade secret theft or loss. Such a plan can be instrumental in dealing

promptly and comprehensively with incidents, as well as limiting and containing the damage.

a. Employee incidents[58]

Employee incidents can range from a serious or a repeated failure to comply with specific security measures (e.g., failure to put away or lock confidential information), to loss or theft of a company computer while traveling, to risky cyber behaviors leading to a breach, to unauthorized download of documents or secrets or transfer of such materials to third parties. Discipline and enforcement actions are similarly broad in range, including general employee reminders, formal and specific reprimands, suspension with or without pay, termination of employment, or the filing of a lawsuit. "Near-miss" emails to all employees for immaterial lapses or mistakes are often effective at both making a memorable impression on the offending employee and a reminder to all other employees to be vigilant.

b. Third-party incidents

If a third party is a strategic collaborator, the incident often needs to be handled diplomatically. In some situations, a gentle but firm reminder that trade secret documents are not to be printed or shared with those outside of the "approved" team can have the intended compliance effect without poisoning the relationship. Providing this kind of reminder is also a significant demonstration of the company's commitment to protecting its information and ensuring compliance. More serious incidents may require engagement of management and often company counsel. The type or level of reaction to intentional breaches or reckless behaviors leading to losses or public disclosures may be used later to demonstrate the value that the owner places on

58. *See Sedona Employment Life Cycle Commentary*, *supra* note 8.

the secrets at issue or on the owner's conviction that compliance with the contract or other measure is important.

c. Legal action

Pursuing legal remedies such as using demand letters, filing civil litigation, or pursuing criminal prosecution may be necessary to stop or seek redress in the event of a theft or misappropriation of trade secrets. Cease-and-desist letters and demand notices are often viewed as aggressive actions and do not always need to be the first reaction to such a serious incident. However, if it is imperative that a behavior stop to mitigate further harm, it may be necessary to quickly escalate the response. As noted above, seeking emergency relief from a court is sometimes the appropriate action. Such relief could include seeking a temporary restraining order or a preliminary injunction or even, where all of the detailed statutory elements are satisfied, pursuing a seizure remedy under the Defend Trade Secrets Act. The exact scope of the remedies available will vary by jurisdiction and factual circumstances.[59]

59. *See* The Sedona Conference, *Commentary on Equitable Remedies in Trade Secret Litigation*, 23 SEDONA CONF. J. 591 (2022), https://thesedonaconference.org/publication/Commentary_on_Equitable_Remedies_in_Trade_Secret_Litigation; The Sedona Conference, *Commentary on Monetary Remedies in Trade Secret Litigation*, 24 SEDONA CONF. J. 349 (2023), https://thesedonaconference.org/publication/Commentary_on_Monetary_Remedies_in_Trade_Secret_Litigation.

APPENDIX A—EXAMPLES OF MEASURES COMPANIES HAVE USED TO PROTECT THEIR TRADE SECRETS

In this Appendix we provide examples of measures a company may consider when developing a Trade Secret Management Program to protect its trade secrets, drawn from collective experience and case law. However, any company's program should be designed based on its unique circumstances dictated by the nature of its secrets, their value, and the risk environment in which the business operates. That a company uses all, none, or some of these measures is not determinative of whether it has deployed "reasonable measures" or efforts to protect its trade secrets. Therefore, this is offered as a starting place, meant to spark discussion and consideration as a program is designed and developed.

A. Policies, procedures, and records

- *Confidentiality, limited use, and material transfer contracts*. Contracts with employees, contractors, joint-venture partners, third-party suppliers, and customers with access to the company's trade secrets, which require confidential treatment, nondisclosure, and use for only specified purposes, are typically a necessary—but not always sufficient—basis on which to prevent unauthorized disclosure and use of trade secrets. Depending on the circumstances and the jurisdiction, it can also be important to specify in such contracts any ongoing compliance monitoring, access, or auditing that the company intends to carry out, including with respect to particular activities such as email, network and internet use, social media, or personal communications. Carefully constructed agreements can themselves be part of a "training" effort by clarifying what the contracting

party's obligations are and what information is to be protected.

- *Third-party diligence procedures and contractual requirements.* In addition to conducting due diligence into third parties who will be permitted to receive disclosures of trade secrets (e.g., tollers, suppliers, vendors, licensees, potential business partners or collaborators, and those evaluating a business for a potential transaction), companies may want to consider special contractual measures with such parties. For example, a company may require (in express terms in the third-party contract) that the third party take certain actions (e.g., limit access to the trade secret to specific individuals, restrict post-disclosure activities of those individuals, provide secrecy training to those with access, allow audits by the trade secret owner, or report apparent violations). Some companies find it helpful to negotiate the right to require individuals at the third party who will have access to information to personally sign confidentiality obligations, or at the least, certify that they have been apprised of the obligations. Some disclosing parties may negotiate audit rights during the relationship or after its termination, require annual training and certification of compliance, and implement closeout procedures for when the relationship ends. Specifying how information will be shared (such as on a shared drive or server controlled by the disclosing party) and how information will be handled once the relationship ends can limit misuse.
- *Confidentiality marking requirements.* Confidentiality markings have been mentioned specifically in some

court cases as evidence of reasonable measures.[60] Consider, however, whether marking every single email, letter, or item as "confidential" is workable in some situations and whether it provides any actual value to the internal company audience. Broad adoption of a confidentiality designation, even for clearly nonconfidential information, may confuse rather than aid employees in understanding how to handle the information the company truly intends to protect. Similar confusion may arise in matters of technical collaboration. If collaboration is expected to span many meetings and both oral and written communications, especially over an extended period of time, requiring specific written notice of what disclosures, oral or written, are to be treated as confidential may initially appear to be desirable, but it can become unwieldy in practice and may lead to a lack of compliance, which can be problematic. Consider the risk to the producing party of agreeing to unworkable procedures or failing to designate information in accordance with contractual requirements.[61] "Escape

60. *E.g.*, Aetna, Inc. v. Fluegel, No. CV074033345S, 2008 WL 544504, at *14 (Conn. Super. Ct. Feb. 7, 2008).

61. It is common for information-sharing arrangements (e.g., confidentiality agreements) to impose some obligations on the trade secret owner to identify information as a trade secret during the course of the information exchange. In these situations, failure to follow these agreed procedures has been found to be a forfeiture of protection. *See, e.g.*, Convolve, Inc. v. Compaq Comput. Corp., 527 F. App'x 910, 924–25 (Fed. Cir. 2013) (granting summary judgment for defendant on trade secret claim where contract unambiguously required trade secret owner to confirm in writing within twenty days that transferred information was confidential and plaintiff had failed to do so); *see also* HCC Ins. Holdings, Inc. v. Flowers, 237 F. Supp. 3d 1341, 1351–52 (N.D. Ga. 2017). Contracting parties will want to be sure that any such

valves" can be built into some contracts, through such means as saying that this type of information "should be treated as confidential, whether or not marked as such," or that information the receiving party "knew or should have known" is confidential should be treated as confidential. Such statements can be backed up by training as well as, in the case of third parties, by looking at what information the third party itself views as confidential in its own business.

- *Post-employment or post-transaction restrictions* with employees, key consultants, departing business owners, business partners, and third parties that limit the ability to compete in a defined way (including restrictions on pursuing particular customers) once the relationship ends can be a strong tool to protect trade secrets. The enforceability of noncompete and related agreements depends on state-specific legal requirements, which are evolving rapidly and range from outright prohibitions on the use of noncompete agreements with departing employees (California, Oklahoma, and North Dakota) to specific limitations both on the permissible content of such agreements and the employees with which they can be used; some states also require specific notice and other formal requirements. The federal government is also assessing potential limitations on the use of noncompete agreements, so this is an area the legal team must review and provide guidance regarding

formalities are workable before agreeing to them and to follow the procedures to which they have agreed.

the latest developments and requirements.[62] Where permitted by law, noncompete and other restrictive agreements should be reasonably limited in scope, duration, and geography in order to be enforceable; specific "consideration" for the agreement may be required by law or may be desirable to enhance enforcement. A contract that imposes sweeping prohibitions may be rejected by courts as an impermissible restraint on trade and held to be unenforceable. A narrower contract may be more enforceable. For example, post-separation restrictions on soliciting the business of particular customers about which trade secret information has been provided may serve the company's needs without prohibiting competition for all other customers and may be more likely to be enforced than a broad noncompete agreement. On the other hand, a contract that is too narrow in scope, duration, or geography may be enforceable but may provide little practical protection to the company. The use of any restrictive covenants as a way of protecting trade secrets needs to be gauged against the changing legal landscape, the nature of the information to be protected, the company's organizational needs, the impact on the party to be restrained, and the public interest. Balancing provisions that are truly designed to protect the company's interest in its trade secrets while allowing the receiving person to

62. The Federal Trade Commission in January proposed a new rule that would ban employers from imposing noncompetes on their workers. The public comment period on the proposed rule ended on April 19, 2023. Press release, Federal Trade Commission, FTC Proposes Rule to Ban Noncompete Clauses, Which Hurt Workers and Harm Competition, https://www.ftc.gov/legal-library/browse/federal-register-notices/non-compete-clause-rulemaking .

continue to make a living or permitting the receiving company to continue to conduct its business without using trade secrets will generally enhance the likelihood of enforceability and protection.

- *Employee or third-party codes of conduct.* A company's expectations and requirements for how employees and third parties should protect and use its trade secrets, and how the company may enforce or otherwise manage compliance, are often expanded upon in more detailed policy and procedure documents. These policies and procedures can be incorporated by reference into the employees' and third parties' legal agreements with the company, sometimes by reference to the company's employee handbook or an employee or third-party code of conduct.[63] Companies should be mindful, however, of the tension between the often-used statement that a "code of conduct is not a contract" and a later desire to point to the code of conduct as a commitment by the employee. The code of conduct can be a useful training and reminder document; it can also be incorporated into a larger contract where appropriate.
- *Document management, retention, storage, protection, and destruction policies.* Document retention, storage, and destruction policies can be practical ways to help restrict the access to and use of confidential information. Examples include limiting the number of copies and numbering and controlling permitted copies, requiring shredding when copies are no

63. *See Sedona Employment Life Cycle Commentary*, *supra* note 8.

longer needed,[64] providing for (and requiring) locked storage for hard-copy documents (individual desks and file storage), observing and enforcing "clean desk" rules (all confidential information is required to be locked away when not in use), and segregating the trade secret into several documents so that if one is taken, the entire trade secret is not taken. When the sharing of trade secret information includes third parties, for example, in a joint venture arrangement or evaluating a prospective business relationship, document management may include storing all shared documents on a server controlled by the disclosing party. Where this approach is not feasible, the parties should agree on processes governing the return or destruction of shared trade secret information at the termination of the relationship or processes for rendering them no longer readily accessible, taking into account the costs of such measures.

- *Electronic Communications and Social Media Policies.* Many companies permit the use of personal devices on company networks and premises. Others prohibit the use of personal devices but permit commingling of personal and business information on corporate-issued devices and cloud storage, including the use of third-party communication platforms such as WeChat and WhatsApp. The approach may differ by region within a multinational company where privacy and data governance laws differ and impose regional constraints on such policies and practices.

64. Some industries are subject to special legal requirements for the preservation of information for specific periods by law or regulation. Those requirements are outside the scope of this discussion.

Whatever framework a company adopts, customized policies and processes should be developed to ensure adequate security and protection of company data, including trade secret information. This framework should also balance the personal convenience of messaging apps with the corresponding lack of visibility and controls from widespread use of such applications on company devices.

- *Human resources and compensation policies and procedures.* There are also practical steps that human resources personnel can take to promote trade secret protection and compliance when employees and contractors begin and finish their work for the company. Offer letters, employee covenants, and onboarding processing can also be used to emphasize both the company's policy and intent not to disclose, use, or learn any confidential information or trade secrets of prior employers, flag potential conflicting confidential information knowledge of a particular employee's former employer, and trigger management of the issue. It can be useful to conduct onboarding training about trade secrets, confidentiality, and the program aspects applicable to the employee. Involving senior managers in the training programs can emphasize the company's commitment to the program (in other words, it is not just "make work"); involving lower-level employees in the training programs can help identify practical challenges or recurring questions. Documenting that staff has undergone training is a useful and often compelling step in enforcement proceedings. Exit interviews and procedures are also useful to ensure that (a) company documentation and equipment have in fact been returned and (b) the employee is

reminded and has acknowledged (sometimes in a separation agreement) his or her ongoing obligations to maintain the confidentiality of the company's trade secrets and other information. Some companies also tie incentive compensation to employees' completion of ongoing training on trade secret protection, or other compliance metrics.

- *Remote work policies.* Increasingly, particularly resulting from the COVID-19 pandemic, employees are working remotely and in less traditional workplaces. This could result in a variety of working situations, from a home office, to the home's kitchen, to a "rent-a-space" desk in a shared work environment, to hotel rooms and hotel common areas, to the road, including cars, trains, planes, rest stops, airports, and restaurants. These changes require a different approach to security and trade secret protection. Companies should consider questions such as: how safe is the internet access available to the employee; who is present when or where he or she is working; how easily could other people see, learn, or steal information; how secure are the employee's devices (computer, phone, tablet) when not in use; should the remote worker have his or her own locking file cabinet or shredder for physical document storage or destruction; should the company collect corporate-issued devices and hard-copy documents via mail or require drop-off, and adapt its exit processes accordingly. Companies can then develop or provide appropriate policies, tools, equipment, guidance, and training to help employees protect trade secrets in these circumstances.

B. Training and capacity building

Trade secret jurisprudence has noted—in finding that "reasonable measures" were insufficient—that a company had failed even to inform employees "what, if anything, [the company] considered confidential."[65] Periodic training, management guidance, and other capacity building for employees, contractors, and even business partners can be a helpful way of focusing attention on the importance of a company's trade secrets and how to protect them, and promoting ongoing compliance. Similar training for outside consultants, temporary or other contingent workers, and workers in shared, coemployment (secondment) situations who have access to a company's trade secrets may also be called for.[66]

Some companies find that active reminders via company network or email notices, in-person events, or even video or social media messaging to be helpful ways of building trade secret protection awareness and compliance, despite the information overloads that many employees and workers experience.[67] Some companies also build websites or other mobile platforms to provide training and policies, compliance requirements, case studies illustrating successful and ineffective controls, and other resources on trade secret protection for employees to access at all times. Regardless of a company's training roadmap, it may be more effective when such efforts are integrated into the company's broader messaging around physical and digital security,

65. *E.g.*, MBL (USA) Corp. v. Diekman, 445 N.E.2d 418, 425 (Ill. App. Ct. 1983).

66. Whenever this *Commentary* refers to "employee," one should consider its applicability for other types of workers who are not in a formal "W-2" type employee relationship with the company, but who are working alongside full-time employees performing similar services and work on behalf of the company, with similar access to the company's trade secrets.

67. *See Sedona Employment Life Cycle Commentary*, *supra* note 8.

environment, health and safety, travel, ethics and compliance, and diversity and inclusion.

C. Physical controls

Physical controls (e.g., locks, doors, walls, or gates) have been a staple in protecting trade secrets for a long time. Physical measures are, simply stated, creating restricted access to trade secrets to those who have a "need to know."

- *Physical barriers.* Campus gates, entrance door locks, visitor management systems (visitor logs, escort rules, security, or visitor badges), and security staff provide a first line of defense by restricting access of the public or nonauthorized personnel to its offices, laboratories, manufacturing floor, files, and records. Similarly, but on a smaller or more specific scale, safes, locked file cabinets, locked storage areas, or specific rooms or areas that are locked further restrict access to the secrets. Other kinds of physical barriers include curtains or screens around portions of the R&D lab or manufacturing floor, and the prevention of mobile phones, cameras, and other recording equipment on premises to restrict the ability of anyone without a need to know to see, record, or otherwise gather details about the trade-secret-protected device, product, or mechanism. Metal detectors can be used to check for unauthorized devices or materials both entering and leaving facilities. "Clean desk" policies (discussed above) and document shredding requirements are another form of physical protection—keeping the information put away on a regular and consistent basis.
- *Data and asset localization.* Another physical security measure that can be very effective for some

companies and some trade secrets is requiring that all assets and data remain on campus. But for many companies and trade secrets, this is not realistic or feasible, due to factors such as employee travel, work performed by employees on client or other business partner's sites, and remote workers who may be working from home or other locations. Employees need to be sensitized to the risks involved in removing assets and data from the company's physical locations and required to take measures to protect it when they do. These measures are most often common sense (locking the car and keeping a close eye on belongings when traveling, not sharing a work computer with other family members if working remotely), and measures commonly used on campus (such as locking a home office or otherwise securing files when not in use when working from home) can be adapted for the remote work situation. Such measures can be useful in protecting certain kinds of equipment, physical components, documents, and other physical embodiments or repositories of trade secrets.

- *Coded ingredients.* Where Occupational Safety and Health Administration (OSHA) and related requirements permit, referring to ingredients by code names—x drops of ingredient A, 2 milliliters of ingredient B—can help preserve confidentiality and limit access to the entire formula.
- *Physical segmentation.* A manufacturing company may benefit from a risk mitigation standpoint by physically isolating various portions of a proprietary manufacturing or assembly process in distinct, separate locations, so that a single breach will not expose all of the related trade secrets. Similarly, when

designing and building a new facility, a company can hire multiple engineering firms or contractors, each responsible for different aspects of the project, which makes them responsible for different trade secrets or aspects of a trade secret. By so segregating, no one firm has access to or knowledge of the entire secret or all of the secrets. A company might also in-source the final or critical part of the assembly or installation for the project to further segregate and protect the trade secret or set of secrets. These tactics and strategies may be on the more extreme end of the spectrum; however, they may be important to consider when building in jurisdictions around the world where intellectual property rights are not well respected.

- *Black Box*. Another strong physical protection is utilizing a "black box" approach. This entails encasing the trade secret to hide it or its critical elements. The black box approach can apply on small or large scales—all depending on the secret to be protected. One example is the operations floor machinery, which can be obscured from view by physical implants such as curtains. Another example is a small component encased in plastic that cannot be opened without destroying the component. The objective is to encase the trade secret in such a way that it cannot be reverse engineered. This technique can be utilized in any number of situations. One company has used this technique to protect a manufacturing process for several decades (rather than patent it for only 20 years). Some companies use this technique to protect the more critical steps of manufacturing processes in countries without mature intellectual property enforcement regimes.

- *Clean Room.* Clean-room procedures are a proactive effort to shield a company's independent development of competing products from future claims of contamination, or improper use of a third party's trade secrets in connection with that development. While clean rooms are expensive, time and resource intensive, and require extensive planning and coordination, they can be particularly helpful where a company's independent development may later be challenged, such as in the context of joint development with suppliers, where a company had previously codeveloped a product or raw material with a supplier and later decides to in-source that product or raw materials. It can also be helpful in the talent recruitment context, where the company has hired several key inventors from a single competitor, who are then assigned to collaborate on developing a competing product, or where a consulting arrangement ends prematurely or disruptively and the company continues with product development.

  In order to be "clean," clean rooms include (1) a specification team comprised of experts who may have knowledge of third-party trade secrets and who identify the functionality or other requirements for the competing product; (2) a screening team that serves to review and filter the information provided from the specification team to the development team, and ensures that procedures are followed to protect information flows in and out of the clean room; and (3) a development team that is physically and digitally isolated in the clean room, is only allowed access to the specifications, and is responsible for the actual design of the competing product. Former employees of competitors and others who may have

> access to third-party trade secret information are excluded from the screening and development teams. Appropriately staffing these teams, maintaining well-documented procedures and records, and ensuring compliance at all stages of the process is important for clean rooms to have the intended safeguard effect.[68]

D. Electronic and information technology security measures

In light of the pervasive risks to electronically stored information and severe consequences of unauthorized access to that information, many companies are presently focusing significant investment and effort in upgrading their information technology systems and infrastructures to deal with and combat the growing risk of cybersecurity threats. Electronic security measures have long been recognized by courts among the "reasonable measures" that can be effective tools for protecting trade secrets and promoting ongoing compliance.[69]

Electronic security controls can be helpful in protecting all kinds of confidential business and technical information in digital form, particularly if these controls are implemented with an understanding of what a company's trade secrets are, where they are held in the company, and what the likely cyber risks for those trade secrets are. Electronic security measures that help to

---

68. *See, e.g.*, Patriot Homes Inc. v. Forest River Hous., Inc., No. 3:05-cv-471 AS, 2007 WL 2782272, at *4 (N.D. Ind. Sept. 20, 2007) (finding a clean room ineffective where months after its creation, "the 'clean room' was still tainted").

69. *See, e.g.*, Revzip, LLC v. McDonnell, No. 3:19-cv-191, 2020 WL 1929523, at *8 (W.D. Pa. Apr. 21, 2020) (denying motion to dismiss alleging failure to state a trade secret claim and explaining that "a reasonable extension of physical security measures is electronic or computer security measures such as password protection").

protect trade secrets and promote compliance can include elements such as the following:

- *Passwords*. Password protection can be established for hard drives of laptops and other machines as well as for access to a system, server, or to specific files, folders, or drives. Password-type protections increasingly involve password strengthening requirements (which may include length, upper and lower case, numerals, and nonalphabetic characters, and renewing on a regular basis).[70] Multifactor identification that uses more than one form of identification (i.e., something you are given plus something you know, or a password plus authentication via text or phone call) is increasingly common, particularly for remote access or for administrative access to systems and data. Biometrics (which may itself be addressed by regulatory requirements, e.g., the Illinois Biometric Information Privacy Act or the proposed federal Commercial Facial Recognition Privacy Act) are also increasingly being used to strengthen access controls.
- *Access controls*. Access controls can be used to limit or segregate use, copying, and transmission of trade secrets by limiting access to certain files, folders, drives, systems, or servers, or by limiting the ability to print, download, alter, or transmit certain files or folders. "Rights Management" technology can be deployed that limits access to authorized individuals only, and so even if content is accidentally shared, such technology will prevent unauthorized viewing

70. Standards for what constitutes a "strong" password change over time. Accordingly, this *Commentary* does not offer specific guidance.

of document contents. The Supreme Court recently determined in the criminal context that the protections afforded by the Computer Fraud and Abuse Act against those who exceed "authorized access" to a computer system do not apply if the defendant had been authorized to access the portion of the computer system from which the alleged taking occurred.[71] As such, some companies may decide to establish separate servers or drives for storing the most sensitive information and restrict access to those locations to only a small number of employees. Companies sharing trade secrets with entities outside the United States may similarly choose to store their trade secret data on servers or drives physically located in the United States so that, among other reasons, access to those locations in furtherance of misappropriation may be found to have occurred "in" the United States for purposes of the Defend Trade Secrets and Economic Espionage Acts.

- *Data loss prevention software*. Data loss prevention software is used by many companies to manage and monitor user activity across systems and networks, and even to and from cloud environments. Data loss prevention solutions can be fine-tuned to look for particular data types and elements and alert when unauthorized use or transmission is suspected. File level activity logging can also be enabled and does not necessarily require the purchase of expensive data loss prevention software. Employees should typically know (and some state law requires notice) that they are being watched closely. But they should

71. Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021).

generally not know exactly how they are being watched, or how monitoring systems work.[72] If they do, they could try to work around the system and find holes. For example, an employee with frequent confidentiality policy violations could be testing the bounds of the system.

- *Encryption*. Encryption of particular files, computer discs, servers, email traffic, and other items can protect company trade secrets even if there is unauthorized access. Enabling and requiring the use of VPN or other encrypted or protected access to the company's system via the internet can provide effective protection for data when not within the protection of the company's four walls.
- *Network segregation*. Network segregation can be used to limit the places where particular trade secrets or other confidential information is held. Also, to reduce risk, trade secrets can be strategically segregated rather than aggregated in a single, centralized network location where a breach could be severely problematic.
- *Firewalls*. Firewalls are used to prevent unauthorized external access to a company's networks, servers, computers, and files.
- *Email filters*. Email filters are used to restrict communications from suspect or spam senders, or with risky or suspicious attachments, files, or web links, guarding against "phishing" and malware attempts. These security services usually also provide filters or protections from visiting potentially risky or suspicious sites (via link or otherwise) that could lead to similar

72. *See Sedona Employment Life Cycle Commentary*, *supra* note 8.

introductions of malware and other attacks that could make the company's digital systems vulnerable and pose a risk to trade secrets and other confidential information.

- *Antivirus and software updates.* Antivirus or antimalware software and regular software updates can guard against cyberattacks, phishing, and other security lapses that increase the risk profile and vulnerability of a cyberattack and could compromise confidentiality.
- *Cybersecurity training*. Cybersecurity training for staff should be considered even when sophisticated and up-to-date email filters and antivirus or antimalware software is in place. Staff that has been sensitized to cybersecurity issues and flags can provide the final line of defense for avoiding risky emails (still one of the most common forms of attack and network compromise) and internet use as well as reporting oddities to be investigated.
- *Protections for travel to insecure locations.* For travel to jurisdictions around the world where intellectual property legal regimes are not well established, or concerns arise around loss or tampering of corporate devices, some companies have plans in place or special "burner" or one-time-use devices on hand in advance to provide traveling employees with the access and information they need for the business purposes of the trip, while protecting the rest of the company's secrets and other information.
- *Automatic backup*. Automatic backup of digital information in the event of a catastrophic event (e.g., weather, accident, fire, or cyberattack) can prevent the loss of company trade secrets.

- *USB drives and other portable device restrictions*. Restrictions on the use of USB drives and other portable storage devices, which may include prohibiting the use of such devices or the blocking of USB ports altogether, can be used to protect information against theft, malware, or device damage (e.g., "USB killers") and unauthorized copying and downloading (even by employees who have no bad intentions).
- *Cloud-based data storage*. Cloud-based data storage raises some potential risks. First, consider the company seeking to move its data storage to the cloud. Due diligence on both the cloud storage provider and the tools to interface with the cloud are key to an understanding of how and where data is (or can be) stored, backed up, accessed, and shared (and thus how it can be protected or lost). A company may believe it has good controls over the internet, firewalls, passwords, encryption, and permissions to file, folder, or storage systems, only to learn that employees can "share" files or folders with anyone who has an email address. Second, companies should consider whether employees' use of publicly available cloud-based storage or group collaboration applications (e.g., Google Drive, Dropbox, Slack, BOX, Monday, Teams, SharePoint, or GLIP) is aligned with company goals and processes. Many employees use these products without permission and introduce significant risk. They may be doing so with the best of intentions to build efficiency for their team or a project, or at the request of an outside party. But few will investigate or understand the privacy implications, ownership rights, and other risks to information shared through or stored in such applications. Similarly, location of cloud servers outside the

United States may raise specific security considerations. Many companies develop policies around the use of cloud-based storage and group collaboration applications for confidential information to avoid these risks.

- *High-risk websites and applications*. High-risk websites and certain domains create significant security risk and vulnerability to trade secret theft, fraud, and espionage, along with opportunities for employees to engage in unauthorized or illicit activity on corporate devices, systems, and networks. Consideration should be given to prohibiting the use of any such websites and applications absent prior approval, whitelisting certain applications (as having been vetted and safe to use), or blacklisting specific applications. If cloud-based storage applications are used, consideration should be given to logging all electronic data transfer activity. Also, companies using such services must be sure that the activity is shut down and the information is removed at the end of any project for which the service is used.
- *Personal device and mobile phone restrictions*. Restrictions on personal devices used for company business under a "bring-your-own-device" (BYOD) policy can be used to control the potential avenues through which trade secrets and other confidential information can be accessed, transferred, photographed, recorded, or used in unauthorized ways. Even if photos or recordings on personal devices have a legitimate business purpose, providing protocols for transferring such recordings to the company's encrypted, protected systems as quickly and as safely as possible can mitigate the risk of use of such devices. Consideration should also be given to

whether and which personal devices (home computers, personal mobile or smart phones, tablets, and pads) should be permitted or prohibited for company business and information. For example, employees may have a desire to "work on it at home" or to use a personal computer with which they have a higher comfort level, even though such an approach could result in leakage of secrets to areas where other digital protections are lacking.[73]

- *Software app whitelisting or blacklisting*. The whitelisting or blacklisting of particular software apps as part of a company's policy can limit the potential risks from untested or unknown computer programs operating on the company's systems. In addition to cloud-based storage discussed above, other applications may create or introduce vulnerabilities to the overall system security. Whitelists and blacklists should be updated regularly.
- *Managing work-from-home risks.* Working from home has become increasingly common and brings additional and different risks to manage. Among other things, companies should evaluate the systems used by remote workers to communicate and access company resources to determine if the connections are secure, whether the data should be encrypted, and whether security systems can effectively support the increased traffic. Companies should consider the value of other potential security measures specific to the circumstances of the remote workforce. Examples of these additional measures include:

73. Similar issues with personal devices are more acute in remote working situations.

prohibiting or restricting the printing of sensitive information, requiring control over hard-copy documents, ensuring that corporate resources are used only by employees and only for authorized uses, discouraging commingling of personal and work-related devices and data, and ensuring appropriate physical access controls are in place in an employee's home.

- *Information retention policies*. Information retention policies, standards, and technology solutions should be considered, not just to comply with any applicable legal and regulatory requirements, but to limit sensitive trade secret information languishing in email storage, file shares, and other repositories. Establishing protocols to purge data when no longer needed can reduce the risk of unauthorized loss or disclosure of sensitive information.

E. Contracts

For contracts, a three-prong approach is often valuable. First, review who has access to information and secrets of the company and determine if valid contracts exist for all such persons or entities. Second, review the terms and conditions of these contracts (and the company's "form" contracts) to determine whether they are strong and appropriate to protect the specific secrets being disclosed in the particular context with the particular receiving party. Consider the possibility that the receiving party is acquired by a competitor or enters into a business transaction with a competitor—does this terminate or alter the information access arrangement? If employee agreements with current employees are inadequate in light of, for example, changes in the employee's access to trade secrets, counsel should be consulted to ensure that any amendments or new contracts will be enforceable, including, for example, whether they require

additional or new consideration. Third, tailor agreements (especially form agreements) to the particular situation and third party. It does no good to have a host of protective measures in an agreement if they are not and, realistically, will not be implemented by a particular third party.

APPENDIX B—EXAMPLES OF HOW REASONABLE MEASURES MAY DIFFER BASED ON FACTORS LIKE THE INDUSTRY, SIZE, MATURITY, AND GEOGRAPHIC FOOTPRINT OF THE COMPANY

Below are some examples of various hypothetical businesses, highlighting how their differences may affect their approach to a trade secret strategy and operational plan. These examples are not intended to be exhaustive and are presented to illustrate a range of business situations and factors for consideration.

Given the great variation in nature of the secrets, their value, and the risk environment from one company to the next, even if two companies are in the same industry or of similar general types, the following illustrative examples should not be misinterpreted to create perfect examples of programs or categories of companies with similar requirements to be compared against either other.

When it comes to Trade Secret Management Programs, no one size fits all.[74]

A. Small technology start-up

A small technology start-up typically has limited resources (venture capital or self-funded) and is in the early stage of

74. Tax Track Sys. Corp. v. New Inv. World, Inc., 478 F.3d 783, 787 (7th Cir. 2007) ("The question here is how much effort to keep information confidential is enough to be considered reasonable? Courts evaluate this question on a case-by-case basis, considering the efforts taken and the costs, benefits, and practicalities of the circumstances. . . . Typically, what measures are reasonable in a given case is an issue for a jury. In some circumstances, however, it may be readily apparent that reasonable measures simply were not taken.") (internal citations omitted); Data Gen. Corp. v. Grumman Sys. Support Corp., 825 F. Supp. 340, 359 (D. Mass. 1993) ("Whether reasonable steps have been taken depends on the circumstances of each case, including the nature of the information sought to be protected and the conduct of the parties.").

product development and commercialization. The team collaborates in an open, information-sharing environment, and the company has little corporate infrastructure or experience with trade secret protection. All team members are involved in all phases of the business, including R&D, product evaluation and testing, and customer and investor meetings. All confidential information is accessible to and shared by the team, and trade secrets have not been specifically identified, classified, or valued.

The team may want to start by developing a trade secret policy and deciding on the roles and responsibilities of team members for implementing trade secret protection protocols. Then the team may determine what resources it can afford to allocate to trade secret protection and develop an operational and financial plan that optimizes cost and risk. Protective measures tailored to the risk will be important, likely focusing on physical and IT security, employee mobility, and third-party interactions. The risk of trade secret loss through employee departures and information sharing with suppliers, potential customers, and partners and through disclosures in the specifications and examples of patent applications may be particularly significant, and so focusing protective measures on contracts, information-sharing protocols, employee exit processes and, where applicable, patent or other intellectual property strategy will be important. The team may also focus on knowledge management—including how to classify, label, share, and print valuable files along with developing role-based access controls.

B. Midsize expanding company

This company has successfully commercialized its first phase of products, is expanding sales volume and geographic scope, and is undertaking new research and development for next-generation products. Additional manufacturing and sales facilities are being built and staffed. The company is developing an internet presence to communicate with customers, third-

party contractors, and suppliers. The company is currently using a general confidentiality protocol for all its confidential information, including trade secrets, and internal access to trade secrets is not highly segmented or restricted. The company is beginning to identify, classify, and value its trade secrets, as well as potentially even documenting negative trade secrets.

The company has a three-year strategic and operational plan that contemplates the need for additional trade secret protection measures. In addition to technical trade secrets, the company is developing business trade secrets relating to special customer and supplier requirements and needs. The company is evaluating new technologies for next-generation products and is also evaluating other companies as potential acquisition candidates. The company finances are sound, but many issues are competing for limited resources.

The company may want to develop a clear business consensus and financial plan for the additional trade secret protections by conducting a risk-benefit analysis, including return on investment for additional protections, both physical and cyber, and whether to move from a general confidentiality protection model to specific identification, valuation, and access restrictions for trade secrets. The company may wish to examine its cybersecurity and trade secret protection culture collectively and find ways to enhance server and cloud security, access, and monitoring. The company may develop training and awareness campaigns on trade secret protection. Business and technology managers may want to consider how they plan to manage the acquisition of third-party trade secrets, and how to integrate and segregate new employees to avoid contamination or infiltration issues. The company may want to examine its document management practices and whether to increase access restrictions for new employees or acquired companies. The company may want to evaluate and clarify the roles and responsibilities of key stakeholders for each aspect of its trade secret

protection program, consider having dedicated positions and resources, and empower stakeholders to address noncompliance issues. If the company is considering developing a patent portfolio, patent efforts need to be coordinated with trade secret protection measures.

C. Data-driven technology company

This company may be in the software, biopharma, on-demand services, or medical device field. The company is established, with mature policies and processes. The company manufactures and sells products and services and is accelerating its business growth to incorporate smart technology employing big data, artificial intelligence, and predictive modeling to complement existing commercial products. The company has robust physical and cyber protection for existing businesses but may desire to modify its program to deal with its new business model, which requires protection schemes for large data sets. The company has not inventoried its trade secrets by business, but some trade secrets cross over from high-profit to lower-profit businesses.

The company may want to conduct a trade secret inventory and classification by product and business to determine risk of loss by licensing or divestiture. The company may also want to decide on trade secret valuation and licensing strategies. The company may wish to invest in additional technology to impose greater access controls, monitoring, and forensic capability around its highest value data sets. With the increasing complexity and diversification of its business models, the company may want to design a dynamic protection plan that can be flexible with business changes but maintain effective controls around data when it is at rest and in transit. The company may want to evolve its employee mobility processes to further protect against data infiltration and exfiltration. As the company builds a larger intellectual property portfolio, coordination of efforts

with respect to protecting information that will be the subject of copyright and patent protection may become even more important.

D. Established, large multinational company

This is a Fortune 300 multinational company, with tens of thousands of employees and contingent workers across the globe, and manufacturing and sales sites in most industrial regions. This company has many business units that share some core technologies, personnel, and functions but generally operate as independent businesses with significant revenues. The company has research and development in multiple locations, and scientists and engineers often work collaboratively and remotely on projects at different locations. The company has a complex supply chain, and in some respects is vertically integrated from raw materials to finished products. The company is publicly traded and subject to global, complex regulatory regimes. The company has a layered management and operational structure, where decisions are made by multidisciplinary teams. Some trade secrets are identified and classified in some business units, but not in all. Some business units are not completely integrated in all company systems, since they have been recently acquired and have different historical systems and corporate cultures.

This company's business case demonstrates many possible trade secret protection circumstances and complexities. The company may want to conduct a business-by-business and location-by-location differentiated assessment of its current physical and cybersecurity systems and third-party contracts to determine strengths and vulnerabilities to be considered for additional resources, management, and prioritization of the most important issues and costs. Information shared in some countries may require particular confidentiality marking or other country-specific legal controls. Or the company may want

to consider making all of its information accessible only on servers it controls located in the United States. Since the company is large and complex, it may be expected to implement a fairly robust system of reasonable measures to protect its trade secrets. Accordingly, the assessment may also include evaluation of trade secret identification and value methodologies, cost of protection methodologies, trade secret authorization and access segmentation, trade secret education and training, and monitoring, compliance, and enforcement protocols, as well as coordination with other components of the company's overall intellectual property strategies and portfolio building.

Although every situation is different, the company may wish to look externally to evaluate how other similarly situated companies in its industry are protecting their trade secrets (e.g., establishing a dedicated chief security officer) and dealing with similar issues, if such guidance is available. The company may wish to evaluate available trade secret protection software, monitoring, and cybersecurity products and services, and may want to avoid operation and research locations that may possess more trade secret risk. The company may want to audit its third-party contracts to determine if they pose a risk of trade secret leakage and there is a need to redesign contracts and protocols to enhance security.

The company may also wish to evaluate the effectiveness of those current employees tasked with responsibility for different aspects of the program and decide whether changes may be needed to effectuate a multidisciplinary team approach. The company may want to evaluate its key trade secrets and revisit how they are classified, valued, printed, stored, transmitted, and controlled at each facility to aid in its decision process concerning additional or remedial physical and cybersecurity methods that it may desire to implement.