Revisiting Goldilocks:
Reasonable Measures to Protect Trade Secrets in an Era of Enterprise Collaboration and Cybersecurity Risk Management

By

Steven R. Kursh, Ph.D., CSDP, CLP
Software Analysis Group
Cambridge, MA
s.kursh@softwareanalysisgroup.com

Pratik Patel, BS, MBA
Software Analysis Group
Cambridge, MA
p.patel@softwareanalysisgroup.com

ABSTRACT

Our objective in this paper is to provide frameworks and suggested policies that enterprises can use to protect their trade secrets in an era of increased collaborations and greater cybersecurity risks. We discuss how it is necessary for management at enterprises, particularly management involved with licensing activities within industry collaborations, to expand the scope of their reasonable measures to protect trade secrets beyond legal and compliance frameworks. The paper also reviews cybersecurity frameworks from the National Institute of Standards (NIST) and the International Standards Organization (ISO).

We review guidelines from the World Intellectual Property Organization (WIPO) and recommend that enterprises have a layered-security approach to ensure resiliency. Additionally, we discuss how enterprises operating in Europe and Canada face challenges managing personnel given privacy compliance laws and issues related to information security practices to avoid conflicts and ensure lawful practices. Consistent with our earlier research and findings from the Sedona Conference, an underlying theme throughout this paper is that enterprises need to balance protection of trade secrets without stifling innovation, complicating collaborations, or creating operational frictions with suppliers, customers, and other partners in their ecosystems.[1]

I. Introduction

Approximately three years ago in an article titled "The Goldilocks and Three Bears Dilemma: Adopting Reasonable Measures to Protect Trade Secrets in the New Work Environment,"[2] we explored the central challenge enterprises face when protecting trade secrets in an era of remote work: how much security and related measures were needed?

Since publication of the article, we have continued our research and in-the-field work related to reasonable measures and best practices. While the underlying question of "how much security and related measures" remains, the factors driving our assessment of reasonable measures at enterprises have become more complex. Many enterprises now actively participate in collaborations with other enterprises that impact product and service development, including, for example, within the software industry, customization and configuration of software at client and/or subscriber sites, support, and other activities. Additionally, cybersecurity has been more integral to building a secure and protective infrastructure.

Senior managers at enterprises, including management involved with licensing with other enterprises and with clients/customers, should be

1 *Sedona WG12 Commentary on the Governance and Management of Trade Secrets, Sedona Conference,* April 2022.

2 Kursh, Steven and Pratik Patel, "The Goldilocks and Three Bears Dilemma: Adopting Reasonable Measures to Protect Trade Secrets in the New Work Environment," *les Nouvelles, Journal of the Licensing Executives Society International,* Volume VLII, March 2022.

attuned to these changes. We suggest that they consider developing and implementing a consistent strategy for protection of confidential and proprietary information, including trade secrets, that can be used when structuring agreements and, more broadly, collaborative relationships with other enterprises, particularly in industry ecosystems.

Failing to do so may not only increase the risk of trade secret theft but also may significantly weaken an enterprise's position in legal disputes. Many of us are well aware that courts often require evidence that a company took active steps to protect its confidential and proprietary information, including trade secrets. Whatever practices your enterprise now follows, even though consistent with industry customs and practices, it may be time to take a look and consider making changes.

This article builds on our prior work by examining the evolution of reasonable measures and their growing intersection with cybersecurity frameworks and risk management. We remain mindful and ask please that you, too, remain mindful of the words from the Sedona WG12 Commentary on the Governance and Management of Trade Secrets: "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."[3] Nevertheless, many of us tasked with the development and implementation of policies to protect trade secrets must strive to meet the hurdle of being reasonable relative to industry customs and practices.

The remainder of this article is divided into three-related sections. First, we review trends that are driving the evolution of reasonable measures to protect trade secrets, including collaboration and cybersecurity with risk management. Second, we discuss possible frameworks and policies that enterprises can use to develop and implement reasonable measures to protect their trade secrets. Our discussion draws from recent work by the World Intellectual Property Organization (WIPO) that can be used to help determine "the what" that should be considered by enterprises. We also consider the how and provide a review of cybersecurity frameworks from the National Institute of Standards (NIST) and the International Standards Organization (ISO) as frameworks.

The last section of the article discusses our key recommendation – that enterprises develop and implement multilayered frameworks with policies that incorporate traditional compliance tools with cybersecurity and risk management.

II. Trends Driving Evolution of Reasonable Measures in the Protection of Trade Secrets

In our experience "reasonable measures" to protect trade secrets has been largely rooted in legal and compliance frameworks. "Reasonableness" was primarily assessed by a checklist of formal safeguards: confidentiality agreements, employee NDAs, and document labeling, for example, were central. These actions were viewed through the lens of legal defensibility that a company could prove it took steps consistent with its ongoing-business practices. This approach extended across traditional measures like physical security (e.g., access control), employment practices (e.g., background checks), and administrative controls (e.g., policies and procedures for information handling). These controls were sufficient for environments where data remained on-premises, access was hierarchical, and collaboration was tightly managed.

As we discussed in our first Goldilocks paper, the safeguards had to be updated to account for remote work, which grew rapidly during the COVID-19 pandemic.

Now, however, the landscape has further evolved, and reasonable measures need, accordingly, to evolve further beyond traditional safeguards and the suggested approaches that we discussed in the first paper.

Two key trends are driving the need for change and expansion of our approach regarding reasonable measures.

First, enterprises, reflecting the growth in global ecosystems and supply chains, are joining with other enterprises to collaborate in consortiums where confidential and proprietary information, including trade secrets are shared, creating in effect, multiple ongoing partnerships with multiple enterprises. In other words, instead of "one-to-one" as in traditional partnerships, management involved in licensing now have challenges related to, in the parlance of software engineering and databases, "many-to-many" relationships in collaborative ecosystems.

Second, consistent with customs and practices, many enterprises are expanding the scope of their efforts to consider cybersecurity and risk management. This shift as part of overall cybersecurity efforts includes robust incident response and recovery plans, vetting and managing vendor and third-party access, and maintaining comprehensive data governance frameworks that define how sensitive information is classified, stored, and monitored throughout its lifecycle.

3 *Sedona WG12 Commentary on the Governance and Management of Trade Secrets, Sedona Conference,* April 2022, p. vii.

Additionally, monitoring and auditing capabilities are now critical for detecting misuse and demonstrating ongoing stewardship.

We discuss these trends and provide suggested recommendations below.

III. Increasing Participation in Collaborations

Due to a combination of factors including, but not limited to global supply chains, the internet, focus on core competencies, and market demands for speed and innovation, enterprises are increasingly choosing to work in collaborations with other enterprises in industry ecosystems. These collaborations typically require multifaceted licensing negotiations and resulting agreements that significantly differ from the past. In effect, an enterprise may now have multiple partnerships with many other enterprises simultaneously that are part of an overall value chain. These relationships exceed the traditional partnership models of the past. Indeed, such ecosystems are becoming increasingly common in sectors where innovation, standardization, and joint problem-solving are critical. Hence, enterprise members often have to share confidential and proprietary information, including trade secrets, as part of enabling interoperability.

In our experience most enterprises often seek and maintain collaborations in response to market needs. Consistent with industry customs and practices, these collaborations often involve product development, product testing, sales, implementations, and services. Consider, for example, distribution networks for many enterprise software companies and how the implementation partners often require access to confidential and proprietary information, including trade secrets, to do their implementation work at licensees or in the case of SaaS, subscribers. Similarly, consider joint product development in the life sciences and other activities that often require complex licensing activities. Indeed, in order for ecosystem business models to work, they require per EY (Ernst & Young Global Limited)"...sharing the data, intellectual property and confidential information,"[4] an approach that runs counter to the core principles of protecting trade secrets.

The trend for enterprises to engage in collaborative ecosystems is well recognized. McKinsey notes, for example, how businesses can leverage digital ecosystems to drive growth and innovation.[5] The McKinsey article "...estimate(s) that at least a dozen sectors, including B2B services, mobility, travel and hospitality, health, and housing, are reinventing themselves as vast ecosystems, networks of networks that could add up to a $60 trillion integrated network economy by 2025."

McKinsey's findings are not unique. The Business Performance Innovation network (BPI) found in a survey that 44 percent of all businesses "...seek alliances for new ideas, insights and innovation." [6] We can expect to see more collaborations and new ecosystems being formed going forward.

Collaborations within ecosystems already exist in many industries.[7] In the automotive industry, for example, the Autonomous Vehicle Computing Consortium (AVCC)[8] requires members to share information to accelerate the mass production of safe and affordable vehicles with automated and assisted driving solutions. This collaboration has accelerated the development of autonomous systems, but it has required clear protocols to define what information is shared, how it is used, and how it is protected. Similarly, in pharmaceuticals and life sciences, consortiums like TransCelerate BioPharma bring together major drug companies to address common R&D challenges.[9] Likewise, in technology and semiconductors, organizations like the RISC-V Foundation facilitate collaboration on architecture standards, chip design, and manufacturing techniques.[10]

While collaborations clearly make sense from a corporate strategy perspective among other factors, the very nature of collaborations (aka consortiums) make trade secret protection inherently more complex. While partnerships raise many challenges in regard to trade secret protections, collaborations are even riskier since they involve broader risk surfaces with more ambiguity that requires clear business and operational governance.[11]

This is particularly true with collaborations involving software trade secrets. Many software-related trade secrets have become digitally fragmented and globally distributed by spanning among cloud platforms, remote workforces, and external partners. The notion of perfect protection is not realistic - it's dangerous, as it creates a false sense of security and leads to stagnation of reasonable measure approaches.

Indeed, in our experience the scope and nature of risks related to the loss of trade secrets for enterprises working within collaborations are much greater than with partnerships. More specifically, we

4 https://www.ey.com/en_gl/ecosystems/the-ceo-imperative-are-you-mastering-your-ecosystem-strategy.

5 https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/ecosystem-2-point-0-climbing-to-the-next-level.

6 https://bpinetwork.org/.

7 https://www.forbes.com/sites/katevitasek/2022/11/30/partnerships-three-data-backed-reasons-two-heads-are-better-than-one/.

8 https://avcc.org/.

9 https://www.transceleratebiopharmainc.com/.

10 https://riscv.org/.

11 https://widgets.weforum.org/blockchain-toolkit/pdf/consortium-governance.pdf.

see enterprises that are members of collaborations typically implementing robust legal frameworks and governance structures to safeguard trade secrets. This typically includes multilateral NDAs, clear definitions of ownership and licensing rights and audit controls. Failure by the collaboration members to implement the necessary governance measures may lead to misappropriation, IP disputes, and other challenges. Similarly, there may be reluctance among enterprise members to contribute, thus, undermining the value of the collaboration.

IV. Adding Risk-Management Frameworks to Compliance Approaches

During the past few years we have seen a shift to increased risk-management frameworks for protection of trade secrets that reinforces and complements the ongoing efforts focused on compliance. Reasonable measures are no longer defined by the mere existence of policies, but by whether those policies effectively help to mitigate many of the risks enterprises face. Cybersecurity is at the forefront of this shift, although as we noted in our earlier Goldilocks article reasonable measures are not equivalent to cybersecurity.

Instead, we are seeing increased use of cybersecurity tools as part of protecting confidential and proprietary information, including trade secrets. Hence, for example, we can expect that most enterprises use encryption, multifactor authentication, and endpoint protection. Reasonable measures may now, however, also imply a broader, more proactive approach that can assist in anticipation and prevention of potential losses of trade secrets. Three such approaches are:

1. **Threat modeling (e.g., STRIDE) to anticipate and pre-empt likely attack vectors;**[12]
2. **Data lifecycle management (e.g., Microsoft Purview,**[13] **data governance, data security, and risk and compliance solutions) to ensure sensitive data is classified, monitored, and properly retired; and**
3. **Human behavior risk mitigation (e.g., SANS Security Awareness Maturity Model)**[14] **to address the reality that employees—not just systems—are often the weakest link in security.**

Of course, the appropriate "reasonable measures" remains tied to an enterprise's technical maturity, governance discipline, and ability to demonstrate active stewardship of its trade secrets protection practices. Nevertheless, the impact of remote work, increased collaborations, cybersecurity, and other factors expands the potential for greater risks. Management at enterprises thus need to treat trade secret protection as a living process; they will then be appropriately positioned to defend their practices in the event of a breach or legal challenge.

V. Possible Risk Management Approaches and Resources

Fortunately, there are easily available resources to assist us in expanding the scope of protections with risk management approaches. The World Intellectual Property Organization (WIPO), which we referenced in our first Goldilocks article as a source of recommendations for protecting trade secrets, has since developed a comprehensive guide worth reading and referencing on a continual basis. The guide discusses the four steps in developing a trade secret protection plan:[15]

- **Step 1: Identify and value your "potential" trade secrets;**
- **Step 2: Determine the risks for your trade secrets;**
- **Step 3: Identify and apply reasonable measures to protect trade secrets; and**
- **Step 4: Monitor and react to misappropriation and leakages.**

This structure mirrors risk management frameworks and reinforces the idea that protection must be proactive, contextual, and continuously maintained.

There are also cybersecurity frameworks that can be of value in your efforts to develop and implement reasonable measures to encompass risk management with compliance. Stressing again that reasonable measures are not equivalent to cybersecurity, but that cybersecurity is relevant in regard to reasonable measures, there is an intersection between WIPO's work with modern cybersecurity frameworks such as NIST and ISO/IEC 27001 which reflects the growing recognition that intellectual property (IP) protection requires both legal safeguards and technical rigor.

WIPO provides guidelines for the legal protection of trade secrets, emphasizing confidentiality, access control, and remedies for misuse. In contrast, cybersecurity frameworks necessitate these principles by specifying how data should be protected in digital environments, through practices such as access management, encryption, monitoring, and response protocols.

12 https://www.jit.io/resources/app-security/stride-threat-model-a-complete-guide.

13 https://learn.microsoft.com/en-us/purview/.

14 https://www.darkreading.com/endpoint-security/managing-human-risk-discoveries-from-sans-2023-security-awareness-report.

15 https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/index.html.

NIST and ISO/IEC 27001 are internationally-respected standards that provide structured approaches to managing cybersecurity risk and information security. While they originate from different organizations, they share core similarities in purpose and structure. Both frameworks emphasize a risk-based approach to security, advocating for the identification, assessment, and mitigation of information security risks. Additionally, both promote the implementation of controls across governance, access management, incident response, and continual improvement.

NIST's five core functions of Identify, Protect, Detect, Respond, and Recover[16] broadly aligns to ISO 27001's Plan-Do-Check-Act (PDCA) cycle.[17] This allows enterprises to use NIST as a flexible practical guide since it does not have a formal certification process while relying on ISO 27001 certification for official assurance.[18]

The following table illustrates how ISO 27001 control areas align with the NIST Cybersecurity Framework, offering a framework for integrating trade secret protection into an enterprise's broader security program:

NIST Functions	ISO 27001 Example Requirements [19]
IDENTIFY	**Clause 4.1** - Understanding the Organization & Context: Identifies internal and external factors affecting security.
PROTECT	**Annex A.9** - Access Control: Role-based access and least privilege principles.
DETECT	**Control 8.15** - Logging Respond.
RESPOND	**Clause 8.2** - Information Security Risk Assessment.
RECOVER	**Annex A.5.29** - Business Continuity Planning: Ensures that organizations can recover from disruptions, including trade secret breaches.

In effect WIPO in combination with cybersecurity frameworks such as NIST and ISO 27001 bridges the compliance and risk management approaches. WIPO helps to define the "what" that must be protected while cybersecurity frameworks address part of the "how" to protect it. Together this what and how provides guidelines for enterprises seeking to develop and implement reasonable measures to protect trade secrets.

The reality is that all enterprises face the fundamental challenge of ensuring robust safeguards to protect trade secrets without stifling collaboration. Excessive access restrictions, rigid data controls, and overly cautious information-sharing policies can create operational friction for enterprises and hurt the core issue of creating stakeholder value. This is especially true for those enterprises that have research and development (R&D) environments, cross-functional teams, and external partnerships where agility and exchanging of information is essential and R&D/innovation centers with third-party enterprises and customers. Our approaches to protect trade secrets can go too far and inhibit the enterprise in addition to frustrating personnel. We fundamentally need to accept some risks to enable innovation and collaboration.

Similarly, many of us have seen enterprises that may often expose aspects of their trade secrets in sales presentations, technical support meetings, and other activities. Yet, such exposures are often inherent in the conduct of day-to-day business and are practically essential for many businesses to function.

The challenge for all of us is further complicated by increasing privacy expectations from employees and regulators. Enterprises must also now navigate between privacy compliance laws (i.e., Canada's Personal Information Protection and Electronic Documents Act[20] and Europe's GDPR[21]) and information security practices to avoid conflicts and ensure lawful practices. Managers at enterprises need to be aware of these privacy compliance laws and adopt their reasonable measures policies accordingly.

One of our major concerns is that some enterprises may go too far and create "security silos" that isolate knowledge or discourage collaboration. In our experience this happens when management effectively equates policies for reasonable measures with cybersecurity.

In fact, management must implement controls proportionate to the sensitivity and value of the trade secrets, while still enabling productive workflows. For

16 https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions.

17 https://gccertification.com/iso-27001-and-the-pdca-cycle-a-roadmap-to-information-security/.

18 https: //www.itgovernanceusa.com/iso27001-and-nist.

19 https://www.isms.online/iso-27001.

20 https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

21 https://www.eurofound.europa.eu/en/publications/2020/employee-monitoring-and-surveillance-challenges-digitalisation.

example, the practices that can be implemented for activities like marketing and sales presentations are not likely to be applicable with technical algorithms and software source code because the creation, use, and type of information is so different. This underscores the need for dynamic, scalable approaches without compromising a "reasonable measures" defensibility.

Some of the technology tools we use can also create hurdles and problems while providing important functionality and protections. Consider, for example, how data loss prevention (DLP) solutions, a form of technical control, from companies like Google and Microsoft are positioned as tools to "...protect your most sensitive data."[22] Indeed, DLP solutions can significantly reduce the risk of unauthorized sharing of trade secret information by automatically detecting, flagging, and restricting the movement of sensitive data across email, cloud storage, and collaboration platforms. Enterprises can also use DLP to enforce policies that prevent downloading, forwarding, or externally sharing documents marked as confidential. DLP can also provide audit trails for accountability.

Yet, while DLP technologies can be a beneficial component of a trade secret protection strategy, they are not foolproof. If anything, such solutions may provide a false sense of security and focus. Sophisticated users can easily bypass controls[23] through sanctioned or unsanctioned channels (e.g., screenshots, personal devices), and false positives or misclassifications can lead to blind spots. For instance, Google's DLP solution, while effective in many areas, has notable limitations such as its inability to analyze multimedia files or compressed archives, leaving gaps in protection for certain file formats.[24]

Hence, any tool—whether DLP, encryption, or endpoint protection, should be viewed as one layer in a multi-faceted defense strategy, not a silver bullet. Effective protection requires a combination of technology, process, and people working in concert. These tools should not be treated as a simple compliance checklist, but rather as components of a layered defense to protecting trade secrets.

This reality forces enterprises to confront a foundational trade-off: the more accessible information is for productivity and collaboration, the more difficult it becomes to secure fully that information. On one hand, businesses benefit from collaboration, but each access point increases the potential for leakage, theft, or inadvertent disclosure.

Using technical safeguards such as encryption, role-based access, data loss prevention, and zero-trust architecture are vital, but they come at a cost. These measures can introduce friction into workflows, delay decision-making, or inhibit creative collaboration. Striking the right balance requires continuous risk assessments, stakeholder alignment and a willingness to prioritize resilience over rigidity. Enterprises, moreover, should assess their "right balance" on a periodic basis when business situations change. As with the original Goldilocks fable with the porridge being too hot or too cold, managers are thus confronted with the tradeoff of too much security or too little security.

Keep in mind, too, that even enterprises with mature security postures and significant investments in trade secret protection are not immune to breaches. History has shown that technical controls and legal safeguards can be bypassed, especially by insiders or trusted actors. DuPont, for example, had extensive safeguards in place when an insider stole proprietary information about its Kevlar technology.[25] Similarly, Waymo (a subsidiary of Alphabet) faced trade secret theft when a former engineer downloaded thousands of confidential files before joining a competitor.[26] These cases highlight a crucial point, which is that no technical or legal system is foolproof. Insider threats, lapses in compliance, or sophisticated cyberattacks can bypass even the most advanced controls.

Interestingly, in our work we often find that senior managers at enterprises often equate trade secret theft or IP misappropriation with someone hacking. The label of "hacker" often comes to mind and dominates the conversation because hacking and data losses are in the news and hackers often are the "bad guy" in movies and television programs. However, while external cyber threats remain real and relevant, they are not the cause of most trade secret losses. This is another reason not to equate cybersecurity, where protection against hacking is paramount, with reasonable measures to protect trade secrets.

In reality, the most significant and persistent risks originate within the enterprise or through what was expected to be trusted third-party relationships.

In our experience the following threat actors consistently appear in trade secret litigation and breach investigations:

- **Insiders:** Employees, former employees, contractors, and consultants with legitimate access who misuse it intentionally or negligently;
- **Business Partners and Consortium Members:** Collaboration usually requires information sharing and creates risk exposure;

22 https://cloud.google.com/security/products/dlp.

23 https://timesofindia.indiatimes.com/blogs/voices/how-some-tech-savvy-employees-are-bypassing-data-leakage-prevention-measures/.

24 https://cloud.google.com/sensitive-data-protection/docs/supported-file-types.

25 https://www.justice.gov/archives/opa/pr/kolon-industries-inc-pleads-guilty-conspiring-steal-dupont-trade-secrets-involving-kevlar.

26 https://www.theguardian.com/technology/2017/feb/23/alphabet-sues-uber-self-driving-cars-technology-waymo-otto.

- **Competitors:** Competitors often recruit rival talent or obtain information through corporate espionage; and
- **Suppliers:** Outsourced service providers (e.g., manufacturing, development and marketing) often have access to confidential materials for them to fulfil their duties.

Ultimately, the goal is not to eliminate risk entirely, but to manage it grounded in reality. This means designing security practices that assume breaches are possible and structuring governance, response, and legal strategies around that truth.

It also means shifting the narrative from perfection to preparedness by using layered defenses, building a strong culture of confidentiality, and rapid cross-functionality incident response. It is crucial that when incidents occur the enterprise can respond decisively and demonstrate that it took reasonable, proportionate, and good-faith measures to protect its trade secrets.

VI. Practical Recommendations for a Balanced Approach

Achieving effective trade secret protection today requires a return to the "Goldilocks Principle of not too much, not too little, but just right." Overly aggressive controls can paralyze workflows and alienate teams, while overly permissive controls invite misappropriation and legal exposure. The key is balance, which can be achieved by implementing measures that are appropriate for the value and sensitivity of the trade secrets, the structure of the enterprise, and the external threat environment. Enterprises must actively tailor policies and defenses based on their risk tolerance, industry specific threats, competitive pressures, and regulatory exposure. They cannot simply copy others.

In our experience a layered-security approach provides the most resiliency. Such an approach combines risk management with compliance.

It would include, at a minimum, the following:

1. **Technical controls like encryption, access management and endpoint protection;**
2. **Procedural safeguards such as data classification, information handling policies, training and clear process for onboarding/offboarding; and**
3. **Legal instruments such as NDAs, trade secret acknowledgements and agreements with partners.**

Under this approach each layer compensates for gaps in the others, creating an environment where breaches must overcome multiple barriers. Effective enterprises ensure these layers work in concert where legal counsel, information technology, human resources, and business units are aligned on security objectives and operational impact.

Monitoring the measures taken by industry leaders and competitors also provides valuable guidance. Benchmarking against peers may also help validate an enterprise's efforts and possibly avoid outlier behavior that courts might deem unreasonable in litigation. Adopting industry accepted frameworks such as ISO 27001 certifications, SOC2 audits, or NIST CSF mapping can signal intentional, structured and repeatable steps to safeguard confidential information.

For insights into best practices, licensing management at enterprises may want to look to analyst firms like Gartner, Forrester, and IDC, which regularly publish trends and benchmarks on topics like zero-trust architecture and privileged access management for safeguarding trade secrets. The insights these companies provide may help enterprises to stay aligned with evolving standards and ensure their security position reflects current industry customs and practices. In our experience, regular security training, tabletop exercises, and auditing partner compliance are critical. Building a "need-to-know" culture, assigning clear ownership of trade secrets, and tracking granular access can further fortify defenses. Finally, investing in insider threat detection tools and incident response playbooks ensures preparedness when breaches occur.

The reality is that threat landscapes evolve constantly, driven by advances in attack methods and the sheer scale of interconnected ecosystems. Controls deemed sufficient today may be outdated tomorrow. This volatility makes static security plans inadequate and reinforces the need for ongoing iteration, particularly when an enterprise is participating in collaborations.

We would be remiss not to discuss the implications of AI and, accordingly, provide a cautionary note. Looking ahead, enterprise management should consider future proofing their trade secret protection policies in an era increasingly shaped by AI and machine learning. With the rise of generative AI platforms that are used for coding and data analysis, trade secrets can be unknowingly embedded into AI prompts and training datasets. Enterprises, particularly those that develop, license, support or otherwise work with software as a core portion of their business should establish AI usage policies that prohibit the inclusion of sensitive, confidential, or proprietary information in prompts submitted to publicly available AI models (e.g., ChatGPT and Copilot). They must also evaluate partners and vendors for how they handle AI, ensuring agreements that explicitly address data confidentiality, ownership, and training model restrictions. ■