Trade Secret Protection in Corporate Information Flows: From "Reasonable Steps" to Evidence-Ready Digital Governance

Hisham Jadallah Mansour Shakhatreh[1]

[1]*Ph.D. (Law), Assistant Professor, Middle East University, Jordan, ORCID: https://orcid.org/0000-0001-8693-5744*

Citation:
Shakhatreh, H. (2025). Trade Secret Protection in Corporate Information Flows: From "Reasonable Steps" to Evidence-Ready Digital Governance. *Public Administration and Law Review*, (4(24), 50–59. https://doi.org/10.36690/2674-5216-2025-4-50-59

Received: November 23, 2025
Approved: December 29, 2025
Published: December 31, 2025

Abstract. *Corporate information flows have become the primary environment in which economically valuable knowledge is created, refined, exchanged, and stored, increasingly via cloud collaboration and multi-platform work practices. As a result, many high-value intangibles are protected less by registration and more by sustained confidentiality governance that can be proven in dispute settings. This article develops an evidence-oriented governance model for protecting trade secrets in corporate information flows by translating legal protectability criteria into lifecycle controls, role responsibilities, and remedy-ready documentation. The study applies doctrinal analysis of trade secret standards under TRIPS and the EU Trade Secrets Directive, complemented by a structured review of governance-oriented guidance on "reasonable steps" and by synthesis with contemporary cybersecurity governance frameworks. We then map legal elements to operational controls, define an evidence readiness pack, and contextualize the model with recent threat and breach-cost statistics. The results show that trade secret enforceability depends on continuity of controls across the information lifecycle, not on isolated legal declarations. The strongest operational posture combines: legal routing and asset tiering, least-privilege access and controlled sharing pathways, third-party boundary controls, and incident-time legal hold and reproducible proof artifacts. Empirical indicators underscore scale pressure: the global average cost of a data breach reached USD 4.88 million in 2024, while compromised credentials remained a major initial access vector in recent breach datasets. Future research should validate sector-specific indicator sets against incident datasets, test which evidence artifacts most influence remedy outcomes, and examine how AI-enabled workflows reshape confidentiality boundaries and "reasonable steps" expectations.*

Keywords: *corporate information flows; trade secrets; reasonable steps; confidentiality governance; lifecycle controls; access management; cloud collaboration; third-party risk; evidence readiness; incident response; enforcement remedies; cybersecurity governance.*

JEL Classification*: K11, K12, K22, K24, K33, L14, L86, M15, O34*
Formulas: 0; fig.: 0; table: 6; bibl.: 14

Introduction. Corporate information flows structure how knowledge assets move across functions, platforms, and organizational boundaries. In such flows, the most valuable information frequently is not intended for public disclosure or formal registration; instead, it derives value from controlled accessibility and contextual integrity. This framing implies that trade secret protection is best understood as an operational status supported by consistent governance, rather than a label applied only at the moment of dispute. The attached chapter conceptualizes this environment as an "IP control environment" that requires both legal routing of information types and continuity of controls across the lifecycle.

This article extends that foundation by integrating additional legal and governance sources and by adding empirical context from recent threat and breach-cost reporting. The goal is to show how "reasonable steps" can be operationalized into measurable controls and evidence artifacts that strengthen enforceability under contemporary digital risk conditions.

Literature review. Recent scholarship increasingly treats trade secrets not as static "information items," but as assets embedded in organizational information flows, including creation, refinement, internal circulation, and controlled external sharing. Within this perspective, protectability depends on whether the organization can maintain controlled accessibility across routine work practices and document that control in a manner that is credible in adversarial settings. The attached chapter frames corporate information flows as an IP control environment and argues that enforceability improves when "reasonable steps" are implemented continuously across lifecycle stages rather than reconstructed after an incident (Shakhatreh, 2024).

This flow-based view is legally significant because it aligns with how courts evaluate secrecy in practice, namely through observable restrictions, governance consistency, and the plausibility of the claimant's confidentiality narrative.

The doctrinal foundation is relatively convergent. Under TRIPS Article 39, undisclosed information is protectable when it is secret, commercially valuable because of secrecy, and subject to reasonable steps to keep it secret (World Trade Organization, 1994). The EU Trade Secrets Directive (Directive (EU) 2016/943) adopts the same three-part structure and clarifies that unlawful use or disclosure may follow from breaches of confidentiality agreements or duties limiting use, which makes internal governance and third-party boundary controls central to liability narratives (European Parliament & Council, 2016).

In the United States, the Defend Trade Secrets Act of 2016 provides a federal civil cause of action for misappropriation and reinforces the practical need for evidence-ready secrecy governance, including rapid response capability and carefully managed disclosure during litigation (U.S. Congress, 2016; 18 U.S.C. § 1836). Across these regimes, the shared implication is that trade secret protection is not merely asserted, it is

operationally demonstrated.

A prominent strand in the literature operationalizes "reasonable steps" as a proportionate control architecture calibrated to asset value, threat exposure, and organizational context. WIPO explicitly emphasizes that reasonable steps should be understood as a practical management discipline translated into identifiable technical, physical, and documentary measures, rather than generic confidentiality slogans (World Intellectual Property Organization, 2019). The attached chapter advances the same logic by translating the legal test into control families and minimum proof artifacts, stressing that disputes often turn on whether controls were real, consistent, and proportionate (Shakhatreh, 2024).

This evidence orientation is crucial because trade secret litigation typically requires the claimant to define the secret with sufficient specificity while also maintaining confidentiality. As a result, the most defensible approaches treat documentation as part of the protection mechanism itself, including classification decisions, access matrices, training attestations, contractual instruments, monitoring records, and incident response artifacts.

Table 1 compares how major legal regimes structure the protectability test and which governance elements most directly support the "reasonable steps" requirement.

Table 1. Comparative legal baseline for trade secret protectability and governance emphasis

Regime	Protectability elements	Practical governance emphasis
TRIPS	Secrecy; commercial value because of secrecy; reasonable steps	Proportionate controls and demonstrable restriction of access
EU	Same three-part test, plus harmonized remedies and duty-based unlawful use/disclosure	Lifecycle continuity, third-party duties, confidentiality-preserving procedures
United States (federal)	Misappropriation cause of action under DTSA, aligned in practice with reasonable measures expectations	Evidence readiness, rapid response, controlled disclosure, litigation preparedness

Sources: (*World Trade Organization, 1994; Directive (EU) 2016/943; DTSA 2016; 18 U.S.C. § 1836)*

Table 1 indicates doctrinal convergence on the three-part test and clarifies why governance evidence is structurally relevant across jurisdictions, because "reasonable steps" is not peripheral but definitional for protectability.

A second major literature stream connects trade secret protection to contemporary digital risk drivers. Cloud collaboration, shared workspaces, and multi-platform workflows increase the number of legitimate access points and normalize micro-disclosures, making secrecy failures more likely to arise as by-products of ordinary work rather than intentional theft. The attached chapter captures this dynamic by emphasizing that leakage mechanisms often follow routine practices such as link-based sharing, external guest access, personal device storage, and fragmented retention

behavior, thereby shifting the governance focus toward designing safe pathways for necessary sharing (Shakhatreh, 2024).

This aligns with broader cybersecurity governance scholarship that highlights the need for organizational oversight, role clarity, and repeatable control performance under complex digital environments.

NIST CSF 2.0 is particularly relevant for the trade secret literature because it elevates "Govern" as a core function and emphasizes accountability, policy, and risk management roles. This focus mirrors the evidentiary questions in trade secret disputes, where decision makers assess whether the claimant's protective posture was supervised and consistently executed (NIST, 2024). ENISA's threat landscape reporting provides further context by documenting persistent cybercrime dynamics and the operational significance of data-related threats that interact with confidentiality and business continuity expectations (ENISA, 2024).

A third stream links governance to remedy feasibility and emphasizes that time-to-action and documentation quality shape outcomes. When confidentiality governance is evidence-ready, organizations can pursue legal remedies while minimizing additional disclosure, because they can precisely define the secret, demonstrate disciplined protection, and reconstruct access and dissemination patterns through logs and records. This is consistent with the chapter's argument that enforceability is strengthened when controls produce durable proof artifacts across the lifecycle (Shakhatreh, 2024).

Empirical sources reinforce the scale and cost environment that motivates this shift toward evidence-oriented governance. IBM's Cost of a Data Breach Report 2024 estimates the global average breach cost at USD 4.88 million, which illustrates that confidentiality failures can create material economic exposure even before litigation and reputational dynamics are fully accounted for (IBM Security & Ponemon Institute, 2024). Verizon's 2025 DBIR further contextualizes organizational exposure by reporting analysis of 22,052 incidents and 12,195 confirmed breaches, underscoring the frequency environment in which credential compromise and misuse can undermine controlled accessibility (Verizon, 2025).

Table 2 synthesizes the principal literature themes and clarifies how each theme contributes to an evidence-ready trade secret governance model.

Table 2 shows that the strongest consensus across sources is procedural: trade secret protection is sustained when legal criteria are translated into lifecycle controls that simultaneously reduce leakage probability and generate reproducible evidence for enforcement.

Table 2. Synthesis of literature streams and their implications for trade secret governance

Literature stream	Core claim	Governance implication
Legal doctrine on protectability	Reasonable steps is a constitutive element of protectability	Design proportionate controls and retain proof artifacts
Practical guidance on reasonable steps	Controls must be concrete, contextual, and documentable	Policies, access discipline, training, contracts, monitoring
Flow-based corporate governance	Secrecy is stabilized through lifecycle continuity and aligned roles	Map controls to creation, sharing, third parties, retention, incidents
Cybersecurity governance integration	Accountability and repeatable outcomes support defensibility	Integrate IAM, logging, governance oversight, audits
Empirical cost and frequency context	Breaches are frequent and economically material	Justifies investment in evidence readiness and control rigor

Sources: *(WTO, 1994; EU Directive 2016/943; WIPO, 2019; Shakhatreh, 2024; NIST, 2024; ENISA, 2024; IBM, 2024; Verizon, 2025)*

Aims. The aim of this article is to develop an evidence-ready model for trade secret protection in corporate information flows by: translating legal criteria into lifecycle controls and proof artifacts; specifying a role-responsibility structure for distributed confidentiality governance, and linking these design choices to measurable indicators and remedy readiness under current digital risk conditions.

Methodology. This article uses a qualitative, synthesis-based design with three components. First, it applies doctrinal analysis of core legal sources governing undisclosed information, focusing on the operational meaning of secrecy, value, and reasonable steps under TRIPS and the EU Trade Secrets Directive (World Trade Organization, 1994; European Parliament & Council, 2016). Second, it conducts a structured literature review of practitioner and institutional guidance on "reasonable steps" and confidentiality governance, including WIPO materials and governance frameworks (World Intellectual Property Organization, 2019; National Institute of Standards and Technology, 2024). Third, it uses analytical mapping to transform legal elements into operational controls, evidence artifacts, and indicator sets, then contextualizes the model with recent empirical cybersecurity statistics from breach-cost and incident-pattern reporting.

Results. The core result is that trade secret defensibility increases when confidentiality controls and proof artifacts are produced continuously across the information lifecycle rather than added after an incident. This continuity logic is explicit in the attached chapter's lifecycle framing and governance outputs across creation, internal use, collaboration, third-party transfer, retention, and incident response.

Table 3 provides a compact lifecycle-to-evidence map that organizations can use to design controls that are simultaneously preventive and evidentiary.

Table 3. Evidence-Ready Public Records Management: Information Security and Long-Term Digital Preservation in State Governance

Lifecycle stage	Typical disclosure risk	Minimum control objective	Evidence artifact (examples)
Creation and capture	Unmarked drafts, uncontrolled copies	Classify and anchor custody early	Classification record; ownership attribution; version history
Internal use and refinement	Excess privilege and lateral visibility	Enforce least privilege and logging	Access matrix; audit logs; access review records
Collaboration and sharing	Link oversharing, guest access	Use approved sharing pathways	Approved zones; link expiry rules; sharing registers
Third-party transfer	Scope creep and retention by vendors	Control boundary by contract and access	NDA and use limits; transfer logs; audit rights evidence
Retention and disposal	Data sprawl and long exposure windows	Minimize and dispose securely	Retention schedule; deletion attestations; repository inventory
Incident response	Evidence loss and uncontrolled disclosure	Preserve proof and limit diffusion	Legal hold records; sealed evidence pack; incident timeline

Source: systematized by the author

The table 3 operationalizes "reasonable steps" as lifecycle continuity: each stage must both reduce leakage probability and generate reproducible proof that secrecy was actively maintained.

A second result is that secrecy governance is inherently multi-actor. Enforceability depends on consistent behavior across executive accountability, legal routing, security operations, business ownership, procurement, and end users, because inconsistencies become exploitable weaknesses in protectability narratives.

Table 4 summarizes a role-responsibility model that links functions to both control contribution and evidence contribution.

Table 4. EU Data Governance and AI Ethics in Higher Education: A Responsible Digitalisation Framework for Compliance and Capability

Role	Governance responsibility	Control contribution	Evidence contribution
Executive management	Risk appetite and accountability	Mandate, resourcing, oversight	Policy approvals; oversight minutes
Legal and IP	Legal routing and enforcement readiness	Templates, escalation pathways	Chain of title; legal hold documentation
Information security	Control design and monitoring	IAM, logging, DLP, incident response	Audit trails; incident records
Business owners	Asset definition and value rationale	Crown-jewel identification, tiering	Trade secret register entries; valuation notes
Procurement/vendor mgmt	Third-party boundary control	NDA, audit rights, offboarding controls	Vendor access reviews; audit reports
Employees/contractors	Confidentiality compliance	Correct channel use, handling discipline	Training attestations; acknowledgements

Source: systematized by the author

Distributed responsibility is not a managerial preference; it is an evidentiary necessity because "reasonable steps" must be shown through

consistent organizational practice, not isolated technical controls.

A third result is that remedy effectiveness depends on whether the organization can act quickly without widening disclosure. EU trade secret law supports confidentiality-preserving litigation measures, but this advantage materializes only if a claimant can define the secret precisely, show governance discipline, and preserve chain-of-custody evidence.

Table 5 outlines a minimal evidence readiness pack that supports fast, confidentiality-preserving escalation.

Table 5. Rebalancing Welfare for Better Living: How State Social Policy Shapes Quality of Life Outcomes

Evidence component	What it contains	Why it matters for enforceability
Secret definition file	Scope statement, components, exclusions	Prevents failure due to vagueness
Secrecy governance record	Policies, classification rules, access matrices	Demonstrates sustained "reasonable steps"
Access and activity logs	Authentication and file activity history	Supports attribution and timeline reconstruction
Dissemination trail	Sharing registers, link history, watermark IDs	Reconstructs diffusion and breach scope
Third-party duty documents	NDAs, use limits, audit rights, offboarding	Establishes contractual and duty-based breaches
Incident record and legal hold	Timeline, containment, preserved images/snapshots	Reduces spoliation risk and supports urgent measures

Source: systematized by the author

Evidence readiness converts confidentiality governance into litigation feasibility by enabling targeted claims supported by structured artifacts rather than broad, risk-amplifying disclosures.

A fourth result is that the economic and operational pressures that motivate evidence-ready governance can be supported by current statistics. IBM's 2024 Cost of a Data Breach report estimates the global average breach cost at USD 4.88 million, highlighting material business exposure when confidential information control environments fail. Verizon's 2025 DBIR reporting indicates that compromised credentials remain a major initial access vector, and additional analysis tied to the 2025 dataset reports credential-stuffing activity as a substantial share of authentication attempts in observed environments. ENISA's 2024 threat landscape further underscores the persistence of ransomware and data-related threats as core risk categories that interact with confidentiality and availability in modern organizations.

Table 6 summarizes selected empirical signals and explains their governance meaning for trade secret protection.

Table 6. Trade Secret Protection in Corporate Information Flows: From "Reasonable Steps" to Evidence-Ready Digital Governance

Empirical signal	Reported statistic	Governance implication for trade secrets
Average cost of data breach	USD 4.88 million (global average, 2024)	Raises the value of preventing diffusion and documenting diligence
Credential misuse in breaches	Compromised credentials as a major initial access vector in the 2025 DBIR dataset	Supports prioritizing IAM, MFA, and least privilege as protectability controls
Prime threat categories	Availability attacks and ransomware emphasized among key threats	Reinforces the need for incident-time legal hold and evidence preservation

Source: systematized by the author

These statistics do not measure trade secret loss directly, but they justify governance investments by demonstrating the frequency and cost environment in which confidentiality failures occur.

Discussion. The results support a coherent interpretation of trade secret protection as a governance-and-proof problem. Under TRIPS and the EU Trade Secrets Directive, "reasonable steps" is evaluated contextually, meaning that controls must be proportionate to value and risk and must be demonstrable through records. The lifecycle mapping shows why isolated measures underperform: a single weak stage, such as permissive external sharing, can undermine the practical secrecy boundary even if creation-stage controls are strong. The role-responsibility model clarifies that legal enforceability is shaped by operational behavior, because courts and counterparties assess whether secrecy handling was consistent, intentional, and supervised.

Integrating cybersecurity governance frameworks strengthens this approach by offering a structured language for accountability, monitoring, and continuous improvement. NIST CSF 2.0's emphasis on governance aligns with the need to demonstrate oversight and risk management as part of reasonable steps, particularly for third-party and multi-platform environments. ISO/IEC 27001 can serve as an institutional backbone for evidence-oriented confidentiality controls, while trade secret-specific documentation narrows the gap between general security management and legal protectability narratives.

A practical implication is that organizations should design "safe pathways" for necessary sharing. If business processes force employees into ad hoc exchanges, micro-disclosures become normalized and may later appear as permissive handling that weakens protectability. The evidence readiness pack addresses the remedy side of the problem by reducing response time and enabling confidentiality-preserving escalation that EU law explicitly supports.

Limitations should be stated clearly. The framework is conceptual and must be adapted to sectoral constraints, jurisdiction-specific evidentiary practices, and organizational maturity. The empirical statistics used here

describe breach environments rather than trade-secret-specific loss, so future validation should use incident datasets where trade secret claims, evidence artifacts, and remedy outcomes can be jointly analyzed.

Conclusions. Trade secret protection in corporate information flows is most robust when it is treated as an evidence-ready control environment rather than as a legal label applied after harm occurs. The article demonstrates that "reasonable steps" becomes operationally meaningful when translated into lifecycle continuity, distributed responsibility, and proof artifacts that can be reproduced under dispute conditions. This approach aligns with the legal structure of TRIPS and the EU Trade Secrets Directive, while benefiting from governance frameworks that emphasize accountability and continuous monitoring. Empirical breach-cost and incident-pattern reporting provides a realistic justification for investing in confidentiality governance, because the cost and frequency environment makes reactive protection economically fragile.

Funding. The authors declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The authors declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this article are solely those of the author's and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. European Parliament & Council. (2016). Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng
2. European Union Agency for Cybersecurity. (2024). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
3. IBM Security, & Ponemon Institute. (2024). Cost of a Data Breach Report 2024. https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf
4. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems: Requirements. https://www.iso.org/standard/27001
5. International Organization for Standardization. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection: Information security controls. https://www.iso.org/standard/75652.html
6. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
7. Shakhatreh, H. (2024). Comparison of Commercial Dispute Resolution Mechanisms in Jordan and the Middle East. *Public Administration and Law Review*, (2(18), 51–66. https://doi.org/10.36690/2674-5216-2024-2-51-66

8. Shakhatreh, H. J. M. (2023). Development of E-Commerce within the Framework of Compliance with Financial Law. *Financial and Credit Activity Problems of Theory and Practice*, *4*(51), 429–439. https://doi.org/10.55643/fcaptp.4.51.2023.4123
9. Shakhatreh, H., & Ababneh, E. M. (2023). The main ways of leaking commercial secrets and measures to protect them. *Economics, Finance and Management Review*, (2), 76–82. https://doi.org/10.36690/2674-5208-2023-2-76-82
10. Shakhatreh, H.J.M. (2025). Intellectual Property Protection in Corporate Information Flows: Trade Secrets, Digital Risks, and Remedies. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions.* 208 p. (pp. 27-43). Scientific Center of Innovative Research. https://doi.org/10.36690/IPP-27-43
11. Verizon. (2025). 2025 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
12. Verizon. (2025). Additional 2025 DBIR research on credential stuffing. https://www.verizon.com/business/resources/articles/credential-stuffing-attacks-2025-dbir-research/
13. World Intellectual Property Organization. (2019). Protecting trade secrets: How organizations can meet the challenge of taking "reasonable steps". https://www.wipo.int/en/web/wipo-magazine/articles/protecting-trade-secrets-how-organizations-can-meet-the-challenge-of-taking-reasonable-steps-41043
14. World Trade Organization. (1994). Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), Article 39: Protection of undisclosed information. https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm