Challenges and strategies for trade secret security protection in the new digital economy era

3 June 2025

The better the question. The better the answer.
The better the world works.

Shape the future
with confidence
聚信心 塑未来

Challenges and strategies for trade secret security protection in the new digital economy era

3 June 2025

I. Policy updates: Interpretation of the 2025 *“Regulations on the Protection of Trade Secrets (Exposure Draft)”*

1. Background and significance

On 25 April 2025, the State Administration for Market Regulation released the *“Regulations on the Protection of Trade Secrets (Exposure Draft)”* to address new challenges in trade secret protection in the digital economy era. The draft introduces a dedicated chapter on “trade secret protection system construction”, providing detailed guidance on definition, infringement identification, enforcement procedures and legal liabilities, offering clearer compliance directions for enterprises.

2. Key highlights

- Expanded definition: Clarifies the boundaries of technical and operational information and specifies exceptions for “voluntary customer choice”.
- Enhanced enforcement: Targets new infringement methods like “electronic intrusion” and grants market regulators authority to seize evidence and impose coercive measures.
- Collaborative mechanism: Promotes cross-departmental and cross-regional cooperation.

Business operator

Fulfill primary responsibility | Strengthen self-protection

- Encrypt and store confidential information
- Develop confidentiality training plans for employees
- Establish an encryption and storage mechanism for confidential information

Market regulator

Organization and coordination | Supervision and administration | Service and guidance | Collaborative protection mechanism

- Carry out special training on trade secret protection
- Set up service sites
- Collaborate with judicial authorities to investigate and handle infringement cases

Industry organization

Industry self-regulation | Dispute coordination | Formulation of industry norms

- Issue industry protection compliance guidelines
- Mediate infringement disputes between enterprises
- Organize exchanges of protection experience within the industry

Local government

Coordinated leadership | Capacity building

- Establish special protection funds
- Incorporate protection work into regional development plans
- Build communication platforms between the government and enterprises

Social supervision

Infringement reporting | Confidentiality safeguard

- Set up a dedicated hotline for reporting infringement
- Establish a reporting reward system
- Severely punish malicious reports that disrupt order

II. Characteristics and limitations of traditional trade secret management

1. Typical features of traditional trade secret management

- Static confidentiality measure: Relies heavily on non-disclosure agreements and physical isolation, focusing on direct control over trade secret carriers but lacking dynamic updates.
- Post-incident remediation: Prioritizes legal actions after leaks occur, such as administrative complaints or civil lawsuits, with insufficient preemptive risk assessment or monitoring.
- Limited technical safeguard: Uses basic encryption and access control, failing to address digital scenarios like cloud data or AI tools.
- Contract-dependent personnel management: Emphasizes pre-employment screening, exit audits and training, relying on employee compliance rather than proactive controls.

2. Limitations of traditional management in the digital era

- Ineffective against new leakage scenario: Cloud computing and AI enable infringements like unauthorized server access or malware, making traditional physical theft prevention obsolete.
- Outdated technical defense: Static encryption cannot counter AI-powered hacking, such as reverse engineering of product keys.
- Inefficient evidence collection: The “access + substantial similarity” principle struggles in digital environments where cloud leaks leave minimal traces.
- Lack of industry collaboration: Relies on isolated corporate defenses without cross-departmental (e.g. market regulation, public security and courts) coordination.

III. Challenges and strategies for trade secret management in the new landscape

Typical risks

Type I

Internal AI tool risks: Uncontrolled permissions of AI or cyber attacks may lead to data leakage

Type II

External AI tool risks: Employees using third-party AI tools could upload sensitive data

Type III

Data training risks: Unauthorized data collection or training with confidential data may lead to Infringement

Type IV

Permission control: Traditional permission management cannot meet the fine-grained access requirements of AI scenarios

Type V

Security protection: Static encryption is difficult to cope with AI-driven dynamic attacks

Management measures

System improvement

- Establish a tiered management system and clarify departmental responsibilities
- Standardize the Use of AI Tools

Technical safeguard

- Data encryption, access control and anonymization
- Algorithm Models: Vulnerability detection, security enhancement and integrity protection

Employee empowerment

- Employee screening and regular training
- Case warnings to enhance employees’ confidentiality sensitivity

Ecological synergy

- Blockchain technology application and secure data sharing
- Promote industry standards formulation, experience sharing and training

Amid digital transformation and AI adoption, enterprises face more complex risks in trade secret management. While AI optimizes workflows, it also introduces new protection challenges.

1. Risks from AI-related activities

- Internal AI tool risks: Poorly secured internal AI tools (e.g. data analytics, automation) may leak trade secrets.
- External AI tool risks: Employees using third-party AI tools with weak privacy policies could inadvertently upload sensitive data.
- Data training risks: Non-compliant data collection for AI training may violate others' trade secrets, embedding them into algorithms.

2. Trade secret management strategies

- Strengthen policies: Define departmental responsibilities, restrict external AI tools with approval logs and enforce least-privilege access for internal AI.
- Enhance technical safeguards: Invest in data encryption, access control, anonymization and regular AI model vulnerability checks.
- Raise awareness: Conduct rigorous employee screening, regular training on AI-specific risks and legal consequences.
- Leverage industry collaboration: Develop secure data-sharing standards and best practices through cross-industry partnerships.

IV. EY approach to trade secret management

1 Risk assessment and management

- Comprehensive assessment:
  Identify risks from employees, partners, competitors and emerging technologies etc.
- Vulnerability checks:
  Identify the vulnerability in the entire chain of data storage, transmission and usage
- Customized strategy:
  Design differentiated control measures based on risk levels (such as tiered protection and dynamic monitoring)

2 System development and improvement

- Top-level design:
  Formulate a confidentiality policy framework and clarify the definition, scope and tier standards of trade secrets
- Process control:
  Execute non-disclosure agreements with employees and suppliers
  Set up access control system
  Implement classified and tiered management
- Compliance adaptation:
  Conduct regular compliance audits and dynamically optimize relevant corporate institutional documents based on regulatory standards

3 Technology application and safeguards

- Basic protection:
  Encryption technology (two-way encryption for data storage/transmission)
  Access control (biometric identification, dynamic token two-factor authentication)
  Data leakage prevention (DLP)
- Intelligent monitoring:
  AI algorithm analysis of abnormal data flow (e.g., frequent external transmission/unauthorized access)
  Blockchain evidence storage

4 Training and awareness enhancement

- Tiered training:
  Confidentiality systems and legal liabilities training for new employees
  Specialized training for core positions
  Trade secret compliance course for management
- Cultural penetration:
  Establishment of industry leakage case database
  Confidentiality culture month activities
  Internal leakage reporting mechanism

- Risk assessment and management: We assist enterprises in conducting comprehensive trade secret risk assessments to identify threats and vulnerabilities, encompassing risks from employees, partners, competitors and emerging technologies. Leveraging assessment results, we craft trade secret risk management strategies to help enterprises effectively manage and mitigate risks.
- System development and improvement: We support enterprises in establishing robust trade secret protection systems and processes. This includes formulating confidentiality policies, executing non-disclosure agreements with employees and suppliers, implementing classified and tiered management of trade secrets and setting up access control and permission management systems. Moreover, we assist in reviewing and optimizing existing confidentiality systems to ensure legal compliance and alignment with actual business conditions.
- Technology application and safeguards: We continuously monitor and research the latest technological developments to provide advanced technical support and solutions for trade secret protection. In terms of information security technology, we recommend and assist enterprises in deploying encryption technologies, access control technologies and data leak prevention technologies to enhance the confidentiality and security of trade secrets.
- Training and awareness enhancement: We prioritize employee training and education on trade secret protection. Through training courses, workshops and case studies, we enhance employees' awareness of confidentiality and legal responsibilities, ensuring they grasp the significance of trade secrets and the legal ramifications of leaks. We aid enterprises in fostering a culture of confidentiality, creating a strong protective environment where safeguarding trade secrets becomes a natural practice for employees.

Conclusion

The integration of digital economy and AI demands proactive trade secret governance. Enterprises must build three core capabilities:

- AI-powered defense: Shift from isolated safeguards to ecosystem-wide “predict-block-trace” systems.
- Dynamic strategy adaptation: Link protection mechanisms to business operations for real-time risk alerts.
- Value-driven transformation: Make trade secret management a competitive advantage for innovation.

By recognizing the criticality of trade secrets and addressing emerging challenges, businesses can strengthen protection frameworks to sustain competitiveness and growth.

For more information, please contact us:

Kelvin Gao

Managing Partner
Greater China Cybersecurity Services
Ernst & Young (China) Advisory Limited
kelvin.gao@cn.ey.com

Winson Woo

Partner
Greater China Cybersecurity Services
Ernst & Young (China) Advisory Limited
winson.woo@cn.ey.com

Nelson Chan

Partner
Greater China Cybersecurity Services
Ernst & Young (China) Advisory Limited
nelson.chan@hk.ey.com

Wendy Xia

Partner
Greater China Cybersecurity Services
Ernst & Young (China) Advisory Limited
wendy.xia@cn.ey.com

Yang Zhou

Partner
Greater China Cybersecurity Services
Ernst & Young (China) Advisory Limited
yang.zhou@cn.ey.com

Alice Bao

Partner
Greater China Cybersecurity Services
Ernst & Young (China) Advisory Limited
alice.hx.bao@cn.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients, nor does it own or control any member firm or act as the headquarters of any member firm. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

APAC no. 03023473
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com/china

Follow us on WeChat
Scan the QR code and stay up-to-date with the latest EY news.