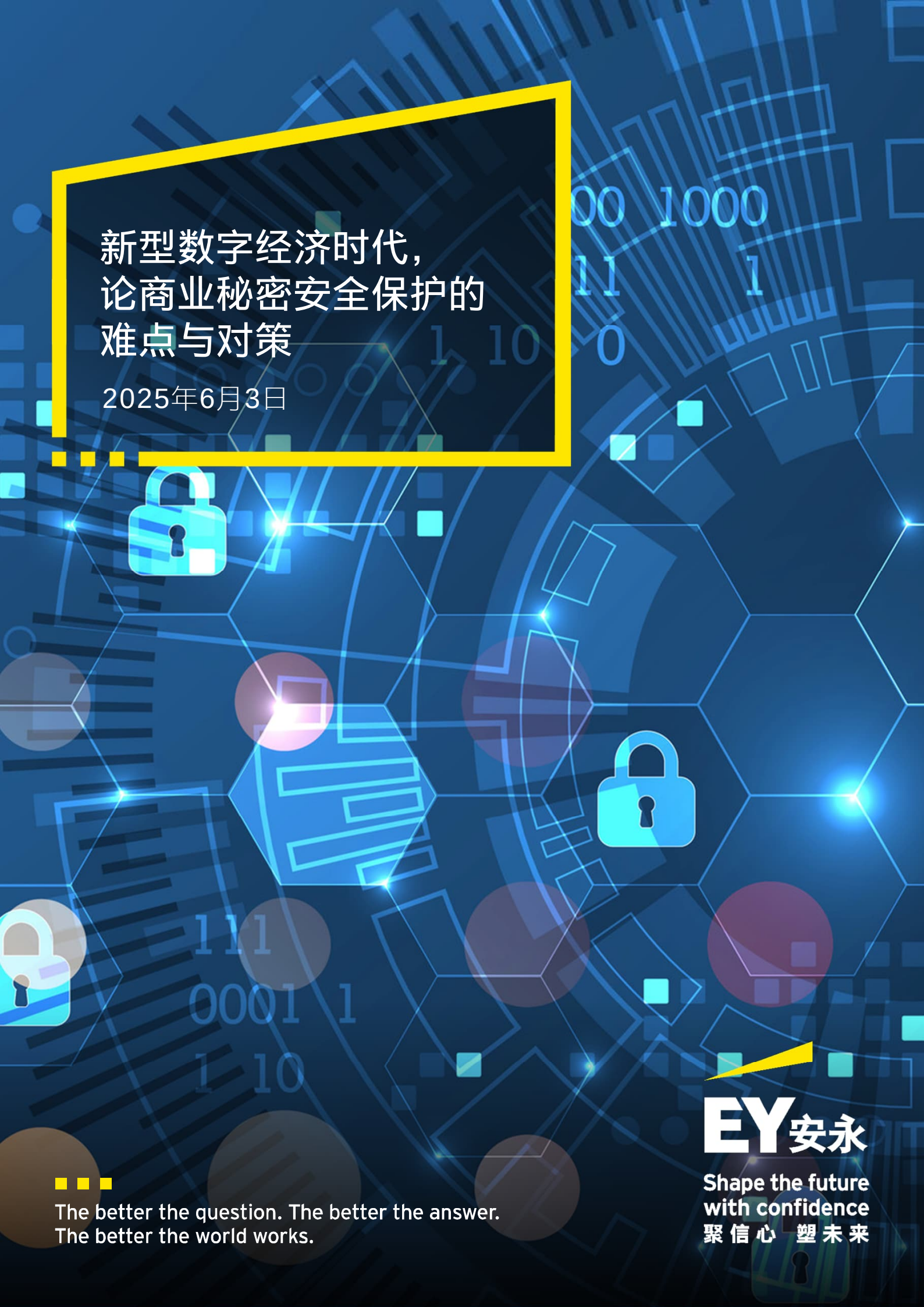
新型数字经济时代，论商业秘密安全保护的难点与对策

2025年6月3日



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

EY安永

Shape the future with confidence

聚信心 塑未来

新型数字经济时代，论商业秘密安全保护的难点与对策

2025年6月3日

一、政策新动态：2025年《商业秘密保护规定（征求意见稿）》解读

1) 背景与意义

2025年4月25日，市场监管总局发布《商业秘密保护规定（征求意见稿）》，旨在应对数字经济时代商业秘密保护的新挑战。征求意见稿首次增设“商业秘密保护体系建设”章节，从界定、侵权认定、执法程序到法律责任全链条细化，为企业提供更清晰的合规指引。

2) 核心亮点

- **定义扩展：**明确技术信息和经营信息的边界，并细化“客户自愿选择”的例外情形。
- **强化执法：**新增对“电子侵入”等新型侵权手段的打击，并赋予市场监管部门查封、扣押等强制措施权限。
- **协同机制：**推动跨部门、跨区域协作。

经营者

主体责任落实

强化自我保护

- 针对涉密信息加密存储
- 制定员工保密培训计划
- 建立针对涉密信息的加密存储机制

市场监管部门

组织协调

监督管理

服务指导

协同保护机制

- 开展商业秘密保护专题培训
- 设立服务站点
- 与司法部门联动查处侵权案件

行业组织

行业自律

纠纷协调

规范制定

- 发布行业保护合规指引
- 调解企业间侵权纠纷
- 组织行业内保护经验交流

地方政府

统筹领导

能力建设

- 设立专项保护资金
- 将保护工作纳入区域发展规划
- 搭建政企沟通平台

社会监督

侵权举报

保密保障

- 开通侵权举报专线
- 建立举报奖励制度
- 严惩恶意举报扰乱秩序行为

二、传统商业秘密管理的特征及局限性

1）传统商业秘密管理的典型特征

- **静态保密措施为主：**传统商业秘密管理多依赖保密协议、物理隔离等静态手段，强调对商业秘密载体的直接控制，但缺乏动态更新机制。
- **事后救济导向：**传统风险应对聚焦于泄密事件发生后的法律追责，主要通过行政投诉、民事诉讼或刑事报案进行维权，缺乏事前风险评估与动态监测。
- **技术防护手段单一：**传统防护手段主要采用基础加密技术和访问控制，对数字化场景（如云端数据、AI工具使用）缺乏针对性防护。
- **人员管理依赖合同约束：**传统人员管理着重对员工的入职审查、离职审计及培训教育。例如，通过背景调查筛选潜在风险人员，在离职时回收涉密设备并要求签署竞业限制协议等，管理多依赖人员自觉性。

2）传统管理在数字化时代的局限性

- **难以应对新型泄密场景：**云计算、AI技术的普及导致侵权行为从物理窃取转向“电子侵入”，未经授权访问企业服务器、植入恶意代码等新型获取商业秘密的手段防不胜防。
- **技术防护滞后于攻击手段：**黑客利用AI算法加速破解加密数据，而传统静态加密技术无法动态适应。例如，通过反向工程破解产品密钥的成本大幅降低。
- **举证与维权效率低下：**传统“接触+实质相同”举证原则在数字环境下适用困难。如云端泄密行为隐蔽性强，企业难以获取电子证据链。
- **行业协同不足：**传统管理依赖企业单点防御，缺乏跨部门（如市场监管、公安、法院）的协作机制。

三、新形势下的商业秘密管理的挑战和策略

典型风险

类型一

企业内部AI工具风险：智能系统权限失控或遭攻击，导致数据泄露

类型二

外部AI工具隐患：员工使用第三方AI工具可能上传核心机密

类型三

数据训练合规风险：非授权数据采集或含密数据训练引发侵权

类型四

权限管控：传统权限管理无法适配AI场景的细粒度访问需求

类型五

安全防护：静态加密难以应对AI驱动的动态攻击

管理手段

制度完善	▪ 建立分级管理制度，明确部门职责 ▪ 规范AI工具使用
技术加固	▪ 数据加密+访问控制+脱敏处理 ▪ 算法模型：漏洞检测+安全加固+完整性保护
人员赋能	▪ 入职审查+定期培训 ▪ 案例警示，提升员工保密敏感度
生态协同	▪ 区块链技术应用，安全数据共享 ▪ 推动行业标准制定，经验共享与培训

在数字化转型与AI技术深度应用的背景下，企业商业秘密管理面临更复杂的风险场景。AI技术在优化业务流程的同时，也带来商业秘密保护的新挑战。

1) AI相关行为引发的风险

- **企业内部AI工具使用风险：**企业部署的智能数据分析、自动化流程等内部AI工具，若缺乏安全防护与权限管理，可能导致商业秘密泄露风险。
- **员工使用外部AI工具风险：**外部通用型AI工具隐私政策与数据安全水平存在差异，员工在工作场景中使用此类工具时，可能将商业秘密数据上传。一旦平台出现安全漏洞或数据使用不当，将造成企业商业秘密扩散。
- **数据收集与训练环节风险：**AI研发过程中，部分企业可能通过非合规方式获取数据，突破其他企业的数据保护措施。同时，使用含商业秘密的数据进行模型训练，可能使算法模型成为侵权载体。

2) 商业秘密管理策略

- **完善管理制度：**健全保护制度，明确部门职责。制定AI工具使用规范，限制外部AI工具，必要时设审批与使用记录；对内部AI工具实施最小权限管理，定期审计。
- **加强技术防护：**加大数据与算法安全投入，用加密技术保护数据存储传输，通过访问控制、数据脱敏、数据屏蔽降低风险，定期检测修复AI算法模型漏洞。
- **提升人员意识：**强化员工入职审查与背景调查，定期开展保密培训，聚焦AI技术新风险，增强员工保密与法律意识。
- **借助行业力量：**人工智能行业探索新技术提升数据共享安全，推动建立统一保护规范，组织经验交流与培训。

四、安永对商业秘密管理的应对思路

1 风险评估与管理

- **全面诊断：**
  识别员工/合作伙伴/竞争对手/新技术等多维度风险
- **漏洞扫描：**
  定位数据存储、传输、使用全链路保密薄弱环节
- **定制策略：**
  基于风险等级设计差异化管控方案（如分级防护、动态监控）

2 制度建设与完善

- **顶层设计：**
  制定保密政策纲领，明确商业秘密定义/范围/分级标准
- **流程管控：**
  签署员工/供应商保密协议
  建立访问控制机制
  实施分类分级管理
- **合规适配：**
  结合法规标准，定期进行合规审计，动态优化企业相关制度文件

3 技术应用与保障

- **基础防护：**
  加密技术（数据存储/传输双向加密）
  访问控制（生物识别+动态令牌双重认证）
  DLP数据泄露防护
- **智能监测：**
  AI 算法分析异常数据流动（如高频外传/非授权访问）
  区块链存证

4 培训与意识提升

- **分层培训：**
  新员工保密制度、法律责任培训
  核心岗位专项培训
  管理层商业秘密合规课
- **文化渗透：**
  行业泄密案例库建设
  保密文化月活动
  内部泄密举报机制

- **风险评估与管理：**协助企业进行全面的商业秘密风险评估，识别企业面临的各种商业秘密威胁和漏洞，包括来自员工、合作伙伴、竞争对手以及新兴技术等方面的风险。根据风险评估的结果，为企业制定商业秘密风险管理策略，帮助企业有效地管理和降低商业秘密风险。
- **制度建设与完善：**帮助企业建立完善的商业秘密保护制度和流程，包括保密政策的制定、员工和供应商保密协议的签署、商业秘密的分类分级管理、访问控制和权限管理等方面的制度建设。同时，还会协助企业对现有的保密制度进行审查和优化，确保其符合法律法规的要求和企业的实际情况。
- **技术应用与保障：**关注和研究最新的技术发展动态，为企业的商业秘密保护工作提供先进的技术支持和解决方案。在信息安全技术方面，推荐和协助企业部署加密技术、访问控制技术、数据泄露防护技术等，以增强企业商业秘密的保密性和安全性。
- **培训与意识提升：**重视对员工的商业秘密保护培训和教育，通过举办培训课程、研讨会、案例分析等方式，提高企业员工的保密意识和法律意识，使员工了解商业秘密的重要性以及泄露商业秘密的法律后果。协助企业开展保密文化建设活动，营造良好的保密氛围，使商业秘密保护成为企业员工的自觉行为。

结语：

数字经济与AI的深度融合，推动商业秘密保护迈入“主动治理”新阶段。企业应紧跟政策动态，构建三大核心能力。

- **智能防御升级：**通过AI实现泄密行为的“预测–阻断–溯源”，将单点防御转化为生态协同。
- **动态策略迭代：**建立与业务联动的保密机制，实现策略的实时校准与风险预警。
- **价值创造转型：**将商业秘密管理体系打造为竞争力内核，驱动创新价值释放。

企业应充分认识到商业秘密的重要性，积极应对新形势下的各种问题，加强商业秘密管理体系建设，不断提升商业秘密保护能力，以增强企业的核心竞争力，助力企业的可持续发展。

如需了解更多信息，欢迎联系我们：

高轶峰

主管合伙人
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
kelvin.gao@cn.ey.com

胡立基

合伙人（华南）
大中华区网络安全与隐私保护咨询服务
安永(中国)企业咨询有限公司
winson.woo@cn.ey.com

陈光华

合伙人（中国香港）
大中华区网络安全与隐私保护咨询服务
安永咨询服务有限公司
nelson.chan@hk.ey.com

夏文婷

合伙人（华中）
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
wendy.xia@cn.ey.com

周旸

合伙人（华中）
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
yang.zhou@cn.ey.com

包红霞

合伙人（华北）
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
alice.hx.bao@cn.ey.com

安永 | 建设更美好的商业世界

安永致力于建设更美好的商业世界，为客户、员工、社会各界及地球创造新价值，同时建立资本市场的信任。

在数据、人工智能及先进科技的赋能下，安永团队帮助客户聚信心以塑未来，并为当下和未来最迫切的问题提供解决方案。

安永团队提供全方位的专业服务，涵盖审计、咨询、税务、战略与交易等领域。凭借我们对行业的深入洞察、全球联通的多学科网络以及多元的业务生态合作伙伴，安永团队能够在150多个国家和地区提供服务。

All in，聚信心，塑未来。

APAC no. 03022961
ED None

ey.com/china

关注安永微信公众号
扫描二维码，获取最新资讯。