数据安全视角下企业保密管理机制与实践路径探讨

宣俊
中核第七研究设计院有限公司，山西 太原 030012
DOI: 10.61369/TACS.2026020006

摘　　要： 在数字技术迅猛发展的大背景下，数据安全日益成为企业管理的一大焦点。从数据安全视角出发，构建保密管理机制，不仅影响企业核心利益，还关系到其可持续发展。本文以科研设计单位作为例，分析当下这类企业在保密管理中存在的主要挑战，并阐述如何构建管理机制，在此基础上提出了具体的实践路径，以期能够为同类企业提供有益参考和借鉴。

关 键 词： 数据安全；企业保密管理机制；实践路径

Discussion on Enterprise Confidentiality Management Mechanism and Practical Paths from the Perspective of Data Security

Xuan Jun
China Nuclear No.7 Research and Design Institute Co., Ltd., Taiyuan, Shanxi 030012

Abstract: Against the backdrop of the rapid development of digital technologies, data security has increasingly become a key focus of enterprise management. From the perspective of data security, constructing a confidentiality management mechanism not only affects the core interests of enterprises, but also is related to their sustainable development. Taking scientific research and design institutions as an example, this paper analyzes the main challenges existing in the confidentiality management of such enterprises at present, elaborates on how to construct the management mechanism, and puts forward specific practical paths on this basis, aiming to provide useful reference for similar enterprises.

Keywords: data security; enterprise confidentiality management mechanism; practical paths

当下，数字化转型让企业发展具有了新动能，但也带来了数据安全方面的风险。保密管理早已超越了传统的纸质文件管理和控制，而是扩展到了诸多环节，如信息系统、业务流程等等，导致安全威胁日益剧增，且复杂多变，需要企业及时转变理念，调整策略，并基于数据安全角度对保密管理工作进行重新审视[1]。本文聚焦科研设计单位工作实际，分析保密管理机制和实践路径，以期提高企业保密工作成效。

一、数据安全视角下企业保密管理面临的主要挑战

（一）内部人员行为带来的数据泄露风险

数据安全防护离不开内部人员，其作为首道防线，面临的管控难度也是最大的。分析工作实际，发现内部人员泄露数据主要包括以下几种情况。第一，无意之失，部分员工未形成保密意识，对于敏感文件的保密意识不强，在日常工作中使用微信、qq等即时工具进行传输，或把工作数据上传到公共云存储，由此导致信息泄露[2]。第二，违规操作，部分员工为了工作便利，未严格遵循企业制定的安全管控制度，用自己的私人邮箱接收工作邮件、借助个人移动硬盘拷贝涉密资料，导致数据超出了有效监管范围[3]。

（二）外部网络攻击手段日益智能化

当前，外部网络攻击呈现出一些新的特征，如组织化、智能化等。如果属于高级持续性威胁攻击，则具有目标明确、潜伏周期长等特点，攻击者为了窃取核心数据，往往会对特定单位进行长期渗透[4]。而勒索病毒的持续演变，也会影响单位正常业务，给其带来直接经济损失。当下，钓鱼邮件的不断翻新，导致其迷惑性越来越强，攻击者的诱导，使得员工点击恶意链接或提供敏感信息。值得注意的是，伴随着人工智能技术的出现和广泛应用，攻击者又有了新的攻击手段，即借助 AI 生成高度仿真的钓鱼邮件、视频等进行精准攻击。科研设计单位由于其独特的定位，使得它承担的任务具有较强的特殊性，所拥有的科研成果、技术资料都具有较高的价值，容易被外部攻击[5]。

（三）新技术应用带来信息边界模糊化

当下，新一代信息技术的出现和广泛应用正在改变信息系统形态。在普及云计算之后，企业数据已经突破了本地服务器限制，而是分布在云端多个节点，如何进行数据主权与管控责任划

分已成为一大难题[6]。大数据技术的广泛应用，让数据在诸多环节如采集、分析等环节中频繁流转，不断延长的数据生命周期和增加的接触人员，增加了泄露风险。在移动办公这一场景下，员工对工作事物的处理主要依赖个人设备，但设备安全性存在较大差异，面临的网络环境也较为复杂，不利于企业统一管控。此外，技术的叠加应用也模糊了信息边界，急需更新传统的防护理念[7]。

二、构建全方位多层次的保密管理机制

（一）健全数据分类分级管理制度

保密管理离不开数据分类分级，且其属于一项基础工作。在实际工作中，科研设计单位应基于数据敏感程度和泄露后有可能造成的危害程度对数据进行分级，在此基础上制定管理要求。首先，建立科学的数据分类标准，基于业务领域对数据进行划分，将其分为科研数据、经营信息等类别，在此基础上，明确主管部门与管控责任。其次，重视数据定级管理[8]。科研设计单位核心数据包含核心技术资料、重大科研成果等，通过严格管控，限定知悉范围。在工作中，任何接触与操作都应经过审核，并全程保留痕迹，以便后续追溯。针对重点数据应进行重点防护，不断规范使用流程、增强授权管理，建立审批备案制度[9]。针对一般数据，则要在注重安全保障的同时，不断提高其便利使用程度，并通过减少管控环节，提高工作效率[10]。再次，构建动态调整机制。基于数据价值变化与应用场景的优化，应定期组织评估，并及时调整管理策略。最后，在业务流程中融入分类分级要求，并在各个环节如数据产生、使用等环节采取科学的管控措施，以便更好地落地落实。

（二）完善人员管理与技术防护体系

保密工作的顺利实施需要做好人员管理，其属于该项工作的关键环节，而技术防护则提供了重要支撑，二者之间应打好配合。人员管理方面，应对涉密人员的全生命周期进行有效管理[11]。在招聘环节，应对人员的背景进行严格审查，从源头入手，把好入口。入职环节，则要签订保密承诺书，让涉密人员明确自身的职责和应承担的义务。在岗期间，可定期培组织保密教育相关培训，从岗位特点出发设计培训内容。针对核心涉密人员，应组织专门的培训与考核，保障其持证上岗[12]。此外，还应建立日常监督机制，由部门负责人主要负责，定期和涉密人员谈话。离岗环节，在进行交接管理的同时，做好脱密期管理，并及时收回相关权限与设备，并签订离岗保密承诺书。技术防护方面，应做好技术防护部署工作。针对终端安全层面，采取终端安全管理，不断规范移动存储设备使用，合理管控 USB 接口，告别违规拷贝。此外，还应部署数据防泄漏系统，以监测、阻断敏感数据外发行为[13]。网络安全层面，采取网络分区管理，将核心系统和办公网络进行逻辑隔离，以降低可能存在的横向渗透风险。此外，还应部署入侵检测与防御系统，以便及时发现、阻断攻击行为[14]。

（三）建立全流程数据安全监测机制

对数据安全的监测不应只停留在某个环节，而是要贯穿到整个过程。为此，企业在建立安全监测机制时，应覆盖数据的全生命周期，从而在可管可控的同时，兼顾可追溯。一建立日志审计系统，全面记录操作行为如数据访问、拷贝等，并对日志开展分析审计，通过检查、分析，了解其是否存在异常的行为、违规操作。如果是核心数据与重要系统，则要进行实时审计，一旦发现问题，立即警告。二部署用户行为分析工具，构建用户行为基线模型，基于计算学习算法对偏离基线的非正常行为进行识别。三对数据进行流转监测，这里指的是监测数据的内部流 + 外部发送，从而对敏感数据进行识别，察觉其是否存在异常流动。在具体工作中，可设置数据外发审批流程，审批所有向外发送敏感数据的相关行为，且审批过程应留痕备查。如果属于高风险行为如，批量导出和频繁下载等，则要安排二次审批、多人审批[15]。

三、推进保密管理实践的具体路径

（一）加强保密文化建设，提升全员安全意识

企业保密工作的有效开展，需要将保密文化作为软实力。在实际工作中，科研设计单位应注重保密文化建设，并将其融入企业文化建设的全过程中，让保密要求进驻全体员工脑海，并成为其自觉行为。第一，领导应做做好带头示范，由单位负责人牵头，主抓保密工作，通过带头示范，营造良好的保密氛围。第二，不断丰富宣教形式，借助内部网站、工作群等载体，科普保密知识，发布风险提示。此外，还可组织保密知识竞赛、案例警示等丰富的活动，提高宣传教育的吸引力。第三，从岗位特点出发，结合不同群体进行差异化培训，不断提高保密教育的精准性、有效性。总之，保密文化建设不应急于一时，而是要持之以恒，以便让保密意识真正进驻员工的脑海和心田，并能转化为他们的日常行为。

（二）强化技术防护能力，筑牢数据安全屏障

技术手段为保密管理提供了重要支撑。为此，企业应基于数据安全需求，不断加强技术防护能力建设。第一，完善网络边界防护，积极部署下一代防火墙、入侵检测系统，从而将外部攻击隔绝在外。对网络进行分区管理，将核心系统和办公网络进行逻辑隔离，避免横向渗透风险。第二，重视数据加密保护，针对重要数据，可从存储、传输环节入手，采用高强度的加密措施。当移动设备丢失或被盗的时候，加密技术能够避免数据被非法获取。此外，还应重视邮件加密，为敏感信息的传输安全提供保障。第三，建设数据备份恢复体系，对重要数据进行定期备份，且将备份数据和生产系统进行物理隔离。针对勒索病毒等风险，应建立离线备份机制，以便遭到攻击后能快速恢复业务。在此过程中，应做好技术防护的与时俱进工作，基于威胁变化对策略与工具进行及时更新。

（三）完善监督检查机制，推动责任有效落实

保密管理制度是否执行到位和监督检查息息相关。科研设计单位应建立常态化监督检查机制，以充分落实保密责任。第一，进行定期检查，基于年度计划组织全面检查，并不断提高覆盖范围，使其延伸到制度执行、人员管理等诸多方面，以便及时发现

其中的薄弱环节。第二，开展专项抽查，对于重点部门、关键环节等进行不定期抽查，检验防护措施的实用性。

四、结语

总之，数据安全视角下的企业保密管理属于一项复杂的系统工程，不仅要注重理念更新，还要兼顾机制完善与实践深化。科研设计单位应基于自身工作实际，把握挑战，构建全方位管理机制，落实实施路径，从而在提升保密工作水平的同时，确保核心数据资产安全，并为其高质量发展奠定扎实根基。

参考文献

[1] 黄颂凯 . 人工智能技术在企业保密管理中的应用及风险防 控研究 [J]. 中国企业经营管理知识仓库，2025，23（01）：39- 41.

[2] 裴洋 ." 杨三角 " 理论在企业保密管理体系架构中的应用 [J]. 现代班组，2025（02）：87-88.

[3] 黄颂凯 . 从老办法到新体系：企业保密管理数字化转型的进 阶之路 [J]. 中国商人，2025（14）：246-247.

[4] 翁非 . 电网企业档案应急服务信息化支撑能力提升研究与实践 [J]. 海峡科学 ,2023(09):67-71.

[5] 刘岳婷，刘玉成 . 大数据时代的企业信息化管理策略 [J]. 现代企业文化，2023（35）：21-24.

[6] 向英 , 韩玄 . 电力行业人工智能技术应用的网络安全风险分析 [J]. 信息安全与通信保密 ,2023(10):67-74.

[7] 李显康 . 人工智能技术应用于基建档案管理的可行性探索 [J]. 中文科技期刊数据库（全文版）工程技术 ,2023.

[8] 刘鹏程 , 张玉臣 , 汪永伟 , 等 . 人工智能背景下保密管理专 业 的 实 践 教 学 建 设 思 考 [J]. 计算机教育 ,2024(6):172-177.

[9] 杨利娜 . 浅析数字经济时代，陕煤物资集团档案信息化转型策略研究 [J]. 兰台内外 ,2023(14):13-15.

[10] 邵雨 . 基于 CiteSpace 的我国企业档案数字化发展历程与趋势分析 [J]. 黑龙江档案 ,2023(02):17-19.

[11] 高瑞琴 . 新形势下企业档案管理信息化建设探究 [J]. 兰台内外 ,2022(28):4-6.

[12] 刘岩 . 大数据时代背景下科研档案信息化建设的若干思考 [J]. 黑龙江档案 ,2021(04):306-307.

[13] 田璐 . 大数据时代背景下高校档案信息化建设探究 [J]. 兰台内外 ,2021(18):37-38.

[14] 刘卫红 . 企业档案管理信息化建设的问题及创新路径探寻 [J]. 企业科技与发展 ,2021(07):177-179.

[15] 梁荃 . 大数据背景下企业档案工作应对探索 [J]. 山东档案 ,2020(02):43-44.

