 DOI: https://doi.org/10.12345/daglyqyfzyj.v3i7.30319

A brief discussion on the dilemma of data leakage and prevention ideas between government and enterprise —— An investigation into the protection of commercial secrets and national secrets in the Internet environment

Yifan Zhang Lijun Zhou Yuxin Zhan

Hubei Institute of Aerospace Chemical Technology, Xiangyang, Hubei, 441003, China

Abstract

In the face of the systemic risks associated with the integration of big data information on the Internet, this paper analyzes the risk and harm of three typical types of government and enterprise protection data needs: organizational structure and personnel information, work plans and activity schemes, and notification documents and project materials. To address these risks, a three-dimensional breakthrough framework of 'structure-person-measures' is proposed. The paper also provides several operational solutions for system construction and cost-effectiveness analysis, offering a reusable methodological paradigm for preventing and controlling Internet data leaks.

Keywords

Internet data leakage; data leakage prevention; systematic advancement; demand orientation; practical path

浅谈政企数据泄露困境与防治思路——互联网环境下商密与国密保护探究

张一帆 周力军 詹雨欣

湖北航天化学技术研究所，中国·湖北 襄阳 441003

摘 要

面对当下互联网大数据信息统合的系统性风险，本文对三类典型政企防护数据需求：组织架构与人员信息、工作计划与活动方案、通知文件与项目材料进行泄露风险分析和危害解析。针对风险，提出“结构—人—措施”的三维突破框架。并提供了几种体系建设的操作方案和成本效果分析，为互联网数据泄露防治提供可复用的方法论范式。

关键词

互联网数据泄露；数据泄露防治；系统化推进；需求导向；实践路径

1 引言

在国家安全战略与《数据安全法》双重驱动下，数据已成为政企核心资产。据 IBM《2024 年数据泄露成本报告》显示，全球单次数据泄露事件平均损失达 435 万美元，较 2020 年增长 32%。在数字化转型加速的背景下，政企机构面临的数据泄露风险呈现跨域化、APT 化、供应链化新特征，互联网数据泄露的防治已成为政企难以回避的问题。传统粗放式以边界防护为核心手段信息管理体系已难以应对当前云环境、移动办公等新型场景。建立整体化、精细化的信息管理目标，建立一套立体、多维度的信息保护体系将成为政企工作的迫切需求。

2 互联网数据泄露的典型场景

近年来，互联网带来的信息泄露时有发生，主要来自组织架构与人员信息、工作计划与活动方案、通知文件与项目材料等三个层次。反映出，风险源自决策层、组织层、基层三个维度，是一种普遍存在影响范围广的风险。

2.1 组织架构与人员信息泄露

现象分析：近年来，境外组织和商业组织存在以根据泄露的组织架构图、会议参会名单、项目人员名单深度分析的手段，攻击者可利用图数据库技术（如 Neo4j）构建关联网络，结合企业官网、招标平台、工商登记等多源数据拼凑完整架构图（如利用天眼查、企查查等商业数据平台）。政企人员进行定向的网络攻击（包括暴力破解邮箱、邮件钓鱼

【作者简介】张一帆（1994–），男，中国湖北襄阳人，本科，政工师，从事保密管理与保密技术防护研究。

等）、通信骚扰和线上攀拉。如“某科技公司因未配置 API 访问控制，导致大量公民个人信息被境外 IP 窃取，网信办依据《数据安全法》处以警告及罚款。”[1]

组织架构上主要风险在于组织架构有着广泛的对外展示需求，且关联性强，可以从企业展示、商务痕迹、政府登记等多个途径获取和校对，对于定向窃密来说是一张易于获取的路线图，提供窃密目标和窃密路线。人员信息泄密主要风险在于人员可能主动展示特定人员或项目组成员名单，人员的岗位、职务、邮件地址、领域成果，核心目标容易遭到社会工程攻击，包括破解互联网邮箱和网盘、线上定向诱骗策反、线下搭讪骚扰等。从国家秘密的角度上来讲，组织架构还包含了政企反窃密的核心部门，可能会被有意绕开，部分人员的岗位、领域成果可能本身就涉及国家秘密，泄密会造成恶劣影响。从商业秘密角度上来讲，组织架构会反映公司的战略意图，结合其他人员和计划信息，很容易分析出公司工作重心，核心成员会被计划性窃密、策反。

2.2 工作计划与活动方案泄露

现象分析：政企在政务云平台、公开招标平台、服务网盘等渠道将项目具体时间节点和参数、产品关键工艺流程完全公开。竞争对手通过收集倒推，在商业竞争和对口谈判中占据优势。如 2022 年某市智慧城市项目招标前，竞争对手通过政府官网公示的《项目推进会方案》中“参会企业名单 + 时间节点”，倒推技术路线与预算分配，最终以低于成本价 5% 中标。

工作计划与活动方案本身泄密影响有限，其危险性主要在于其会被线上反复传播，可能在互联网平台中公开，窃密者可以通过个别公开的计划和方案去特定组织者倒查，进一步搜集线上公开的信息进行大数据分析，危害在于通过其中人员名单来推测业务项目组成员，通过时间节点、管理要求、重要来宾来推断资源分布、企业产能、项目进展等。从国家秘密的角度上来讲，工作计划的项目名称、背景、上下游节点和要求都可能涉及国家秘密，泄密可能会造成恶劣影响。从商业秘密角度上来讲，计划和方案会被倒推生产研发能力，关键参数，会直接影响政企的行业竞争力，关键人物被骚扰拉拢策反更是会直接影响企业利益。

2.3 通知文件与项目材料泄露

现象分析：通过国家保密局公开案例和近年来频发的影视、游戏情报泄露可见。通知文件与项目材料泄露风险长期存在，末端存在单点失效现象。泄露后，组织找回、消除影响会消耗人力物力，影响企业形象，严重的可能面临行政和法律纠纷。新的数据共享条例中也做了明确要求，“政务数据共享应建立分类分级管理制度，对涉及国家安全、公共安全的敏感数据实行加密传输与存储，共享方需签订安全协议并接受定期审计。”[2]

通知文件在传达学习至末端容易出现学习形式不受控的情况，通过互联网传输和展示，而项目在展示和汇报过程中会通过邮箱、网盘、微信等渠道不加保护地传递，并在客户方进一步扩散。通知文件可以直接反映企业战略决策和工作重心，而项目材料不仅有本项目详细内容，也可能包含政企核心展示介绍材料，项目上下游背景，业务链全貌，模块成本等相关信息。从国家秘密上讲，政企存在大量的涉及国家利益通知文件要求限制传播范围，有着明确且复杂的管理要求，泄露将导致严重的后果可能涉及法律责任追究。从商业秘密上讲，这类文件泄露频率高涉及范围广，容易形成大数据富集效应，导致在竞标等行业竞争情景下处于劣势。

3 互联网数据泄露的防治措施

3.1 建立精细防护上层框架

组织架构与人员信息的泄密源自管理的粗犷，应当从系统设计和制度建设上解决。组织架构的信息保护主要手段有精简扁平化组织架构图，使用错位部门名称来避免信息拼图，对部门对外名称进行审查，避免体现具体项目和业务信息，强化人员意识避免公开部门名称串联信息。对人员信息的保护手段主要为最小化管理和分级控制，最小化即只提供必要信息，避免整个政企使用同一套台账同一套表头，根据部门或项目实际业务需求精细化表头，建立管理制度，明确管理要求，仅限定对外公布人员信息的部门。

另一方面，对人员信息的保护体现在建立分级保护的管理体系。需要保护、需要核心保护、管理人员、技术人员等因素建立加权保护网络。以竞业协议，建立核心项目组，建立脱密期等手段，对人员形成有效控制。以统一代号，提供介绍模板，代理沟通联络的方式，为需要保护的人员的对应需求提供体系保护。必要时也可以寻求法律保护，“个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律规定：……（三）采取相应的加密、去标识化等安全技术措施”[3]

3.2 构建责任制压实主体责任

工作计划与活动方案的泄密主要源自源头行为管理不严格、协作混乱，应当从人员行为控制上解决。可以通过建立责任制，设立联络员来解决。可以以签订责任书、责任令的形式委任专人进行核心信息的碎片化隔离和元数据管控。以部门、班组为单位设立联络员协调计划发布和进度报告汇总，可以提高项目管理效率，避免沟通失误。也可以根据是否涉及国家秘密和商业秘密对计划和方案进行拆分、脱密，进一步降低风险。

在实践中，可以通过以下几个抓手来落实。一是应急处理预案和建立责任追究制度，通过制度框架和业绩考核保障设计落地；二是线下审批和电子 OA 分级访问授权，根据零信任原则规划信息防护路径，构建管理围栏；三是适当的内部监管和演练，通过定期的自查总结和入侵式内部演练，保持责任体系的有效性。

3.3 采取管理加技术多维防护

通知文件与项目材料的泄密主要在于信息管理框架的缺失，缺乏对信息本身的保护措施。一方面需要建立信息审查机制，对传达输出的信息进行评估分级，另一方面需要对信息本身进行保护。信息审查可以通过集中审查或部门自行审查，其作用是判断信息需要保护的措施并标注，可以根据是否涉及国家秘密，是否涉及商业秘密进行标注。信息保护常见的手段有限制传播范围、对内容进行修改遮蔽、增加物理锁和设置文档密码、盖专用印戳加电子水印，可以根据核心利益保护需求应用。

信息审查体系的构建存在 4 个知悉维度，即定员、内部、公开、公布。定员是指信息仅在确认的人员之间知悉，内部是指仅在公司内部或者部门内部知悉，公开即不限制传播，公布即上传至互联网供人随意查阅。信息审查即让信息的业务主管人结合泄露后造成的风险隐患和业务需求确定信息的知悉维度。

4 综合治理体系建设

4.1 设立内部管理机构

可以根据需要设立信息保护的管理机构，如果涉及保护国家秘密，还需要根据国家行政管理机构发布的资质审查评分标准设立组织机构。需要通过制定管理责任书、发文任命、建立制度体系框架、设立相应的考核及奖惩机制为管理提供基础。

以实践来讲建立内部管理机构治理对于互联网泄密治理的效果显著，通过分析状态，动态反馈制定的管理措施。相对的成本较高，不仅限于专兼职管理人员人力成本，重点在于决策层领导班子需要听取汇报、参与管理，避免管理浮于形式。

管理机构的主要职责在于制定具体的保护措施，修订完善制度，监督组织实施保护措施。涉及国家秘密保护体系的情况，还包含人员日常教育和离退职人员的脱密管理，如果政企有内部线上办公系统，管理机构还应该监督信息系统的管理和运行。

4.2 组建内部局域网

可以通过组建内部局域网的方式，控制信息边界。如果涉及国家秘密应当根据国家信息系统分级保护标准建设，并通过国家行政管理部门审查。参考国家建设标准 GB/T 22239-2019：三级以上系统应实现安全审计功能，审计范围覆盖所有用户，记录重要用户行为、系统异常事件；审计记录保留时间不少于 6 个月。[4] 局域网需要通过防火墙或其他安全产品对外部访问和向外传输进行控制审计，对用户进行身份鉴别，达到信息审查的目标。

建立内部局域网的成本会因为系统开发需求较大的浮动，但是发挥成效在于监督和推动职能部门落实管理设计路线，依照分级责任制做到长效管理。

内部局域网的作用在于提供一个相对稳定的线上办公环境，从传播手段上限制传播范围。也可以根据人员保护等级、岗位职责、项目配置多个维度，建立多层的内部局域网。同时需要注意的是，在建立多层局域网时，需要重点控制同时授权访问多个网络的用户，此类用户的数据泄露会导致短板效应，使整个内部局域网失效。

4.3 配置电子锁

电子锁可以通过直接在电子文档上以压缩文件、数据文件自带的功能设置，也可以通过光盘等只读介质实现，根据具体需要也可以采购专用的反复制反烧录软件进行处理。对电子锁的配置，应当制定相应的流程，留存记录，建立密码簿，避免电子锁滥用，电子文档使用效率降低。

电子锁的人力成本和资产成本都相对可控，人力成本主要在于使用的教育和违规行为的监督。但是作用更偏向防止负面影响扩散，难以独立达到本质安全。

电子锁的作用在于限制电子信息在互联网上的二次传播，防止信息在互联网的病毒式扩散。需要进一步控制可以采取身份鉴证的电子锁，对长期合作对象提供电子签名解锁的方案，对短期合作伙伴可以提供限制使用次数的密钥。需要注意的是，除了需要严格控制的硬性电子锁，还可以使用加印可视和非可视电子水印、反文档识别噪点的非硬性电子锁。

5 结语

信息革命大数据时代下，信息保护直接关系政企发展环境与核心利益，实现健康长效发展和增长的重要保障。本文通过解构互联网泄密场景，揭示信息失控的深层根源，针对症结从实际出发，提出“结构—人—措施”靶向的突破路径和实践经验，及对应管理体系模型。

参考文献

[1] 奇安信威胁情报中心.2023中国政企机构数据安全风险研究报告[R].2024.

[2] 全国信息安全标准化技术委员会.GB/T22239-2019信息安全技术网络安全等级保护基本要求[S].2019.

[3] 《中华人民共和国个人信息保护法》[S].北京：法律出版社.2021.

[4] 国家互联网信息办公室.网络数据安全管理条例（征求意见稿）[Z].2021-11.