外网环境下数据泄露风险评估与防控研究

乔 敏
零八一电子集团有限公司，四川 成都 611700

[摘要]在公司数字化进程不断推进和居家工作方式逐渐流行的过程中，企业外部网络安全漏洞问题也变得越来越突出。本文对在外联网中发生的数据丢失的风险进行了全面的研究，主要有来自互联网上恶意攻击、员工不合规操作、外包供应商风险问题还有信息技术的发展所带来的潜在威胁等问题，在此基础上以 GB/T45577-2025《数据安全技术数据安全风险评估方法》标准为基础，建立由资产识别、威胁分析、脆弱性评估以及风险量化的四层结构的数据泄露风险评估模型，形成了多层级的评估指标体系。对所发现的风险项，从技术手段保障、管理体系保障、教育培训保障及应急处置四个方面进行全方面的管控机制的设计；最后以分阶段开展、实时监控审核、常态复审更新、成效考核为四方面来说明防控措施执行方式及长效机制建设。

[关键词]外网环境；数据泄露；风险评估
DOI：10.33142/sca.v9i4.19585　　中图分类号：TP309　　文献标识码：A

Research on Risk Assessment and Prevention of Data Leakage in External Network Environment

QIAO Min
Lingbayi Electronics Group Co., Ltd., Chengdu, Sichuan, 611700, China

Abstract: With the continuous advancement of digitalization in companies and the gradual popularity of working from home, the issue of external network security vulnerabilities in enterprises has become increasingly prominent. This paper conducts a comprehensive study on the risk of data loss in the extranet, which mainly includes malicious attacks on the Internet, employee noncompliance operations, outsourcing supplier risks and potential threats caused by the development of information technology. On this basis, based on the standard GB/T45577-2025 Data Security Technology Data Security Risk Assessment Method, a four tiered data leakage risk assessment model is established, which consists of asset identification, threat analysis, vulnerability assessment and risk quantification, and forms a multi-level evaluation index system. Design a comprehensive control mechanism for the identified risk items from four aspects: technical means, management system, education and training, and emergency response; Finally, the implementation of prevention and control measures and the construction of long-term mechanisms will be explained in four aspects: phased implementation, real-time monitoring and review, regular review and update, and effectiveness assessment.

Keywords: external network environment; data leakage; risk assessment

在数智化时代下，数据成为企业最重要的战略资源之一，在此环境下，外网环境的开放性使得数据面临史无前例的数据泄露隐患，而据 Verizon 发布的《2025 年数据泄露调查报告》显示全球有 67%的数据泄露来自外部攻击，内鬼+合作伙伴一共占到 34%左右；系统入侵已经成为造成数据泄露的第一大原因；勒索软件的数据泄露占到了总数据泄露的 44%；使用尚未修补过的漏洞进行入侵攻击增长了 34%，发现了凭证滥用占比 22%，网络钓鱼占到了 16%。在该背景下，《GB/T45577-2025 数据安全技术数据安全风险评估方法》，首次制定出全国性的数据安全风险评估通用性方法，同时将“合规+实战”相结合。同时，在 2026 年 1 月 1 日，《中华人民共和国网络安全法》更新并实行，也将“大数据泄露”作为新增加的违法行为。对互联网中的数据泄露的风险进行分析以及采取防御策略的研究有着非常重要的理论与实际作用。

1 外网环境下数据泄露的主要风险来源分析

在互联网环境中数据泄漏的风险因素可以总结为外部网络安全威胁，内部员工行为，外包商链路风险以及新兴技术带来的风险四大方面。外部网络安全威胁是最主要的数据泄漏威胁源，Verizon 研究显示，通过未修补漏洞

进行攻击的行为增长了 34%左右，其中边缘设备及虚拟专用网络成为攻击对象的比例达到 22%，相比去年增加了近 8 倍之多。CheckPoint《2025 年网络安全报告》表明，偷窃信息黑客软件猛增了 58%，对 BYOD 设备进行企业访问凭据盗窃，边缘设备漏洞成为入侵公司内部网络的踏脚石。内部员工行为也是一个很重要的原因。Verizon 报告显示，内部人士及合作伙伴占到了数据泄露总量的 34%，并且员工使用未经许可的人工智能程序——“隐秘 AI”的行为越来越普遍了，在 14%的员工中，他们会定期通过公司的设备进入生成式人工智能体系。而第三方面临的风险也在不断被放大，到 2025 年，全球大约有三分之一的数据泄露案件都与第三方供应商或者外部平台有着密切联系。Mandiant 公司分析称，黑客会借助第三方 SaaS 集成功能在云环境下窃取并传输公司信息，能够达到长时间潜伏以及长期攻击的效果。新技术的应用带来新的安全挑战，不容小觑。工作人员上传敏感信息至 GenAI 平台存在泄露公司机密的风险，同时大多数公司缺少有效的 AI 应用管理制度，而且边缘计算、物联网等新型信息技术的应用进一步增加了黑客可利用的安全漏洞，很多终端设备以初始弱密码运行并长时间未更新软件，为外部入侵者提供了方便的盗取信息渠道。

2 外网环境数据泄露风险评估模型构建

2.1 评估指标体系设计

建立完善的评价指标是进行数据泄露风险测评的前提条件，本文基于 GB/T45577-2025，采用“情景＋要素”二元评价框架，在资产、威胁、脆弱性及已有防范措施四个方面建立指标体系，其中资产维度涵盖数据资产分类分级、数据价值评估、数据生命周期阶段以及业务重要性等级等；而根据 GB/T45577-2025 的规定，将数据安全风险界定为数据安全事件发生的概率与之对于国家安全、公共利益或者个人/组织的利益带来的影响程度，增加了“合规损害”这一维度。因此资产管理不仅仅是数据分析商业价值，还包括了法律价值及社会影响的层面。威胁维度包含：外部攻击频率与强度、内部人员威胁等级、第三方供应链威胁等级以及新型威胁，例如 AI 辅助攻击的暴露程度。标准把风险源分为威胁、脆弱性和违规操作三个类别，给威胁辨识提供了一个体系性的思路。脆弱性包含技术脆弱性和管理脆弱性两方面。已有控制措施有效性的维度包括：技术防护措施覆盖率、管理制度执行率、监测审计能力和应急响应成熟度。

2.2 风险评估方法与流程

本文采用了以质与量结合的方式来进行风险评价的方式。在质上用层次分析法来对指标重要度做评判，在量上参考了信息风险因素分析模型以及 CVSS 评分体系，使风险数值化。风险量化模型比如 CVSS，FAIR 等都用于信息安全风险评估领域之中，而 FAIR 的优点就是把威胁由技术层面转到财务层面，变成可以量化的风险。从而能够使得信息安全由“合规列表”转变为公司高层管理者的业务风险管理问题。

FAIR-CAM 架构是在对传统的 FAIR 模型进行扩充的基础上把防护手段同风险挂钩，具有突破传统漏洞管理的风险评定的能力。联合 GB/T45577-2025 附录 D 中提供的关于数据安全风险量化的分析及评价方式，在这基础上本文把风险值确定为：风险值＝资产价值*威胁出现的概率*脆弱性被利用的可能性/控制力度。

风险评估开展过程符合国家标准的要求的五环节闭合模式。评估准备阶段确定评估内容、目的及所需资源，定义需要评估的对象即需评估的外网系统的边界、数据资产的范畴以及评估时间；风险辨识阶段利用资产扫描得出数据资产列表，分析威胁源及威胁作用方式，使用扫描工具如漏洞扫描器和渗透测试工具查找系统的缺陷点；风险分析阶段对辨识所得风险进行定性和定量分析并分别采用层次分析法和 FAIR 模型获得相应的风险值；风险判定阶段按照风险值大小将风险分为三级高危、中危、低危风险，制定解决顺序表；风险评估结果编制阶段形成风险清单、等级划分、处置意见等内容的评估报告用以支持防控决策。

3 外网环境下数据泄露防控体系设计

3.1 技术防护措施

技术防护是防护体系的基础，在边界防护方面，传统的 VPN 早已无法满足外网环境下对企业安全的防护需求，零信任网络访问完全打破了传统的 VPN“进了内部网就安全了”的理念，转变为“绝不放肆、持续检测”的基于身份的安全访问方式。ZTNA 结合 DLP 可以强化访问控制、守护机密信息，在企业被入侵情况下还可以保持运行，腾讯 iOA 等零信任安全管理系统利用了端点 DLP、实时的信任判断以及 EDR 联防联控的方式能够大幅度减少远程办公的数据泄漏隐患约 60%。

对于数据的安全方面而言，SASE DLP 防数据泄露方案对分散部署的数据进行实时监控，自动化的控制策略以及加密的隧道通道来保障对分布部署的数据环境中的敏感信息进行全面的安全保护。自动化的 DLP 引擎基于 NLP、OCR 等手段可以做到精确匹配，误报率小于 0.5%。同时还有数据加密、数据去敏化、数字指纹技术等一系列组合起来就形成了一个完整的数据安全传输与使用流程。

在监控告警方面，在部署以用户实体行为进行异常行为判断预警系统的基础上，通过机器学习算法给每个员工创建出一个正常的活动基准模型并对每个员工的登录时间和地点、访问频次等进行持续跟踪来达到自动发现异常行为的目的。

3.2 管理机制建设

管理制度是防护系统的基础支撑。从制度规范的角度出发：建立大数据安全管理制度、数据分类分级制度、权限管理方法、第三方安全管理要求及数据安全风险处置预案。《国家网络安全事件报告管理办法》自 2025 年 11 月 1 日起实施，《管理办法》要求关键信息基础设施保护者应在发生“重大”以上的网络安全事件时在一小时内上报。公司应当把这一项法定责任写入公司的管理体系之中。

从组织保障上看，在组织保障上，要设立决策层、管理层、执行层三级数据安全管理组织结构，界定各自职权；数据安全事件应急工作要实行统一指挥、分级应对的原则，履行数据使用者的数据安全责任。外包服务安全管理方面，要树立“零信任供应链”的观念，把第三方服务商纳入长期监管范畴之内，严控身份认证及访问权限，压缩凭证有效时限。

3.3 人员安全意识培养

人员作为信息安全保护最活跃也是最弱的一环，安全教育宣传要面向全体职工，对领导层、技术员以及普通职员进行不同层次的安全宣教培训；培训的内容有信息安全法律规章、安全使用规则、防范钓鱼邮件、保密管理及移动终端安全等；研究结果表明公司的安全教育普及率高低以及员工的安全知识掌握程度会影响着该单位发生信息泄漏的次数多少；同时还需要建立健全对于违规行为的处罚制度，树立“每个人都是一道防线”的安全理念。

3.4 应急响应与恢复机制

应急响应及恢复是整个防护体系的关键环节之一。参考 NIST 等相关成熟框架制定涵盖预防、监测、分析、控制、消除、恢复、回顾等七个步骤在内的应急响应策略，在检测环节中由 SOC 进行全天候（7*24h）不间断监视，在阻止环节中针对不同事件采用隔离或断开网络等措施以阻止扩散。应急演练是对应急体系的一种验证和完善方式，2025 年“数安铸盾”演习显示，“实战+复盘”的演习形式可以使公司的应急能力得到很大提升，“快速止血-准确定位-风险防控-应急联动-复盘总结”。

4 防控策略实施与持续优化

4.1 分层部署与集成应用

防控措施需要做到分层设置，构建多层次防线系统。最内层是网关层面防御，在此安装使用 ZTNA、下一代防火墙以及入侵检测/防御系统；零信任框架的建立不能一步到位，要采取“分期分阶段、按需实施、逐步推进”的方式来落地实施，先做好远程访问、第三方访问等风险比较高的部分；中间层是对数据的安全保护，在此可以部署数据防泄漏系统、数据加解密以及敏感信息管理系统，对外敏感数据进行标识及监管；最外层是对终端的安全处理，在这里可以部署终端 DLP 客户端、终端检测和响应系统以及杀毒组件，以达到对企业员工使用的个人计算机设备统一管控的目的。第四层是监测审计层，在此层布置了用户实体行为分析、安全信息及事件管理系统以及安全运营中心，构建起全天候态势感知的能力，不同层次之间应当利用开放接口的方式进行整合，研究发现，部署安全编排自动化与响应平台可以将安全事件的平均响应时间从数小时内降至分钟级，大大提高了联防联控的速度，同时在集成使用上需要建立一个统一的安全策略管理系统，做到策略的一站式集中制定下发及审核，防止出现多个安全平台相互割裂的情况出现。

4.2 监测与审计机制

形成常态化监测及审计体系是保证防护措施顺利进行的基础，在监测方面，通过安全信息与事件管理系统对安全日志进行统一采集、整合以及及时报警；部署自动化的响应编排平台可以做到对安全事件的分钟级处理。在审计方面，建立固定的审计流程，即：日常审计、专项审计、年度总审计，合规审计自动化可以实现对 80%的合规检测任务自动执行，从而大大提高了审计速度。

4.3 风险动态再评估

风险是不断变化的，防控方案也需要随风险的变化而不断地改进，企业可以实行双周安全快报制度，利用自动化软件制作安全现状报告书，方便高层领导了解情况做出相应的决定。并且每年做一次全面的安全检测，让第三方进行全方位的安全渗透测试等。还要依照 GB/T45577-2025 的要求，对于重要的数据的使用者需要每年度对自己的网络数据处理行为进行风险评估，并且要向相关管理部门提交风险评估书。

4.4 防控效果评价与改进

构建安全保障成效衡量指标系统，在技术和管理及人员三个方面加以定量分析。技术方面有漏洞修补率、入侵阻断率、信息泄密事件频率、平均查杀速度、平均处置速度等；在管理方面有政策标准覆盖情况、合规审查合格比率、外包安全测评符合度等；人员层面有培训参训情况、欺骗式电子邮件模拟测试成功率等。把安全投入同风险削减收益联系起来，使网络安全成为企业发展的“催化剂”，

达到安全与事业互相促进的效果。

5 结束语

外网环境下的信息泄露风险已经成为了数字化背景下企业所面临的重大难题之一。文章通过分析引起风险的因素，依托 GB/T45577-2025 标准模型制定出全面的风险测评方案，并分别从技术保护、管理制度、人才培养以及应急预案四个方面制定了综合性防控策略，在传统以边界防护为主的安全布局下再加入以上这些措施就可以形成一个完整的外网环境下信息泄露风险治理方案。传统的依靠在边界的防范的传统安全结构无法抵御越来越多出现的网络攻击手段。建立基于数据为中心的主动防御模式，零信任的安全框架，持续化动态的风险检测和控制机制可以更好地解决这种情况下数据泄露的风险问题。未来的生成式人工智能、量子计算等先进技术将会使信息泄露风险越来越多样化与复杂化。于是，机构要不断跟踪新出现的威胁态势，不断丰富完善风险分析的方法，提升风险防范的技术措施，加强管理体系建设，在不断发展变化的安全形势中做好数据安全的持续防护工作。

[参考文献]

[1]王伟洁,周千荷.国外数据安全保护的最新进展、特点及启示[J].科技中国,2021(7):34-36.

[2]邵晶晶,韩晓峰.国内外数据安全治理现状综述[J].信息安全研究,2021,7(10):922-932.

[3]齐继国,李凌航,李论,等.人工智能管理学研究综述——基于中英文文献的比较分析[J].管理学研究,2025,10(4):19-48.

[4]龙军,邓茜尹,陈云飞,等.基于图卷积的无监督跨模态哈希检索算法[J].计算机工程与设计,2024,45(8):2393-2399.

作者简介：乔敏（1980—），毕业于电子科技大学计算机科学与技术专业，现就职于零八一电子集团有限公司。