档案信息安全风险评估体系的构建与应用

李鑫磊
兴安盟公安局　内蒙古　兴安盟　137400

摘　要：本文探讨了档案信息安全风险评估体系的构建与应用，分析了技术、管理、环境和法律等多方面风险因素。通过构建评估指标体系、选择定性与定量评估方法，设计了完整的评估流程。体系验证与优化确保了评估的科学性和实用性。在应用层面，实施风险评估、制定应对措施、持续监控与改进，以及与公安业务融合，为档案信息安全提供了全面保障。

关键词：档案信息；安全风险评估；体系构建；应用

引言

随着信息技术的飞速发展，档案信息安全面临前所未有的挑战。网络攻击、病毒感染、系统漏洞等技术风险，以及安全管理制度不完善、人员安全意识淡薄等管理风险，都对档案信息安全构成威胁。本文旨在构建一套科学、系统的档案信息安全风险评估体系，为公安局档案信息安全管理提供理论依据和实践指导。

1 档案信息安全风险因素分析

1.1 技术因素

一是网络攻击风险极为突出，黑客凭借精湛技术突破网络防线，入侵档案信息系统后，会肆意窃取、篡改或删除珍贵档案信息，令公安工作陷入极大混乱并造成重大损失，常见的网络攻击手段花样繁多，SQL注入攻击中，攻击者在输入字段插入恶意SQL代码，操控数据库执行非授权命令，以此获取或破坏档案信息；DDoS攻击则通过海量请求拥塞目标服务器，致使档案信息系统瘫痪，无法正常提供服务。二是病毒感染也是一大隐患，计算机病毒传播能力极强，既能借助网络迅速扩散，也能通过移动存储设备传播，一旦档案信息系统被感染，病毒便会如蛀虫般侵蚀系统，导致档案数据损坏或丢失，严重影响其完整性与可用性。三是系统漏洞也为档案信息安全埋下潜在威胁，档案信息系统运行时不可避免地存在操作系统漏洞、数据库漏洞等，给攻击者提供可乘之机，使其能绕过安全防护机制，获取系统控制权并对档案信息进行恶意操作。

1.2 管理因素

（1）安全管理制度不完善是常见问题，档案信息安全管理方面制度漏洞多且执行不到位，像用户权限管理混乱，不同级别人员访问权限界定不明，易使敏感信息被不当获取；数据备份不及时问题突出，档案信息系统若遭攻击或出故障，数据丢失后难恢复，严重影响公安工作正常开展。（2）人员安全意识淡薄也是重要风险，部分工作人员对档案信息安全重要性认识不足，日常工作中易违规操作，如随意将存储档案信息的设备连到不安全网络、在不安全环境下处理档案信息，还存在泄露密码行为，让档案信息面临非法访问风险，增加其安全不确定性。（3）应急响应机制不健全不容忽视，发生档案信息安全事件时，若缺乏该机制，就无法及时控制事态，事件初期不能快速判断性质和危害程度，错过最佳处理时机，处理过程中各部门还可能缺乏协调配合，难以形成应对合力减少损失[1]。

1.3 环境因素

自然灾害具有不可预测性和强大的破坏力，一旦发生，极有可能对档案信息系统设备造成严重的物理损坏。地震的强烈震动可能使存储设备掉落、损坏，洪水可能淹没机房，导致设备进水报废，火灾则会直接烧毁设备和存储介质，这些设备一旦损坏，存储其中的档案数据就可能面临丢失的风险，而档案数据往往具有极高的价值和不可再生性，其丢失会给公安局的工作带来极大的负面影响。电力故障也是影响档案信息安全的重要因素。档案信息系统的正常运行高度依赖稳定的电力供应，如果电力供应中断或不稳定，系统可能无法正常工作。

1.4 法律因素

目前，我国在档案信息安全方面的法律法规存在短板，对一些侵权行为的界定不清晰、处罚标准不细化，实际操作中难以准确判断侵犯档案信息安全行为的性质和严重程度，无法给予恰当惩处，这种法律模糊性带来潜在隐患，不法分子可能利用法律漏洞从事危害活动，而相关部门因缺乏明确法律依据打击此类行为时困难重重。同时合规风险也是公安局档案信息管理需高度关注的问题，公安局在档案信息管理工作中必须严格遵守相关法律法规和行业标准，但实际操作中，若因对相关法

律法规理解不足、管理疏忽等未遵守规定，就可能面临法律诉讼和监管处罚，法律诉讼耗费大量时间和精力且可能影响公安局声誉，监管处罚如罚款、业务限制等会严重影响正常工作。

2 档案信息安全风险评估体系的构建

2.1 评估指标体系

技术指标聚焦档案信息系统技术防护能力，其中网络攻击防护能力考量防火墙、入侵监测系统等安全设备的配置、性能以及应对网络攻击的手段；病毒防范能力通过杀毒软件更新频率、病毒库完整性以及系统对病毒的实时监测和清除能力来考察；系统漏洞修复情况关注操作系统、数据库等是否存在已知漏洞以及修复的及时性，以此防止攻击者利用漏洞入侵。管理指标考察公安局档案信息管理水平和规范程度，涵盖安全管理制度的完善程度，像用户权限管理、数据备份恢复等制度是否健全；人员安全培训情况体现工作人员对档案信息安全重要性的认识和操作技能水平；应急响应机制有效性衡量发生安全事件时能否迅速有效采取措施减少损失。环境指标关注外部环境影响，自然灾害防护能力评估机房等设施抵御自然灾害的能力，电力保障水平考察电力供应的稳定性、可靠性以及不间断电源等设备配备情况，防止电力故障导致数据丢失。法律指标则涉及法律法规遵守情况和合规风险管理水平，避免违法违规带来不良后果。

2.2 评估方法选择

定性评估方法侧重于对档案信息安全风险进行描述性和分析性评估，邀请信息安全领域专家对公安局档案信息系统的安全状况全面评估，专家凭借丰富经验和专业知识，细致审查系统各环节，判断可能存在的风险因素，并依据经验和判断确定风险等级；问卷调查是向相关人员发放问卷，收集其对档案信息安全风险的看法和意见，进而对风险进行定性描述。此方法能充分发挥专家主观能动性和经验优势，但评估结果可能受专家个人经验和主观因素影响。定量评估方法运用数学模型和统计方法，对档案信息安全风险进行量化分析，如采用层次分析法（AHP），通过构建层次结构模型、比较判断矩阵等步骤确定各评估指标权重，明确不同指标在风险评估中的重要性，再结合模糊综合评价法，综合考虑各指标实际情况，计算风险综合得分，使评估结果更客观、准确，能为决策提供更精确的风险量化信息和更科学的依据。

2.3 评估流程设计

第一，准备阶段是评估的基础，需明确评估目标，清晰界定评估所涵盖的范围，精准选择评估方法，同时组建一支专业能力强、经验丰富的评估团队，成员可包括信息安全专家、档案管理人员等，此外全面收集与档案信息安全相关的资料，如系统架构、管理制度等，为后续工作提供充分依据。第二，识别阶段聚焦于对档案信息安全面临的风险因素进行全面排查，从技术、管理、环境和法律等多个维度进行分析，准确确定评估指标，为后续评估工作搭建清晰的框架。第三，评估阶段运用选定的评估方法，如定性评估的专家评估法、问卷调查法，或定量评估的层次分析法、模糊综合评价法等，对档案信息安全风险进行量化或定性评估，精确计算风险得分，以直观呈现风险状况。第四，报告阶段根据评估结果撰写详细的评估报告，报告内容应涵盖评估过程、风险状况、得分情况等，同时针对评估中发现的问题，提出切实可行的风险应对措施和建议，为公安局改进档案信息安全管理工作提供有力指导[2]。

2.4 体系验证与优化

构建档案信息安全风险评估体系后，验证与优化环节至关重要，可选取部分公安局开展试点应用工作，让评估体系在实际场景中运行，全面收集来自不同层面的反馈意见，如一线档案管理人员操作过程中发现的问题、信息安全技术人员对评估指标合理性的看法，以及公安局管理层对评估结果实用性的评价等。基于这些反馈意见，需对评估指标和方法进行细致调整与完善，若某些评估指标在实际评估中难以准确获取数据或不能有效反映风险状况，就需对其进行修改或替换；若定性评估方法受主观因素影响较大，或定量评估方法的数学模型不够精准，就需优化评估流程或改进数学模型。通过不断调整和完善，使评估体系更加贴合实际需求，确保评估结果能真实、客观地反映档案信息安全风险状况，进而提高评估体系的科学性和实用性。

3 档案信息安全风险评估体系的应用

3.1 风险评估实施

实地调研能直观了解网络拓扑结构、安全设备部署等实际情况；系统日志分析可获取安全设备运行记录、人员操作记录等信息，为评估提供客观依据；问卷调查能收集工作人员对档案信息安全的看法和经验，从不同角度丰富数据来源。风险计算依据评估指标体系和方法，对收集到的数据进行处理和分析，运用定性或定量评估方法确定各风险因素的风险得分，再综合考虑各因素权重，计算出综合风险等级，以量化方式呈现档案信息安全风险状况。结果分析则是对评估结果的深入挖掘，通过剖析风险得分和综合风险等级，找出档案信息

安全的主要风险点和薄弱环节，为制定针对性的风险应对措施提供有力依据。

3.2 风险应对措施制定

（1）技术层面，要强化网络安全防护，部署防火墙、入侵检测系统等安全设备，构建坚固的网络安全防线；定期进行病毒查杀和系统漏洞修复，防止病毒入侵和系统被攻击；采用数据加密技术，对档案信息进行加密处理，保障其在传输和存储过程中的安全性。（2）管理层面，完善安全管理制度，清晰明确各部门和人员的安全职责，确保安全管理工作有章可循；加强人员安全培训，通过定期培训和考核，提高工作人员的安全意识和操作技能；建立健全应急响应机制，制定详细的应急预案并定期组织演练，提升应对突发安全事件的能力。（3）环境层面，加强机房建设和管理，采取防火、防水、防雷等措施，为档案信息系统提供安全可靠的运行环境；配备不间断电源（UPS），保障电力供应稳定，避免因电力故障导致数据丢失。（4）法律层面，加强对相关法律法规的学习和宣传，确保公安局档案信息管理工作严格符合法律要求；建立合规风险管理体系，定期进行合规检查和评估，及时发现和解决合规风险，保障档案信息安全管理工作合法合规。

3.3 持续监控与改进

建立有效的监控机制对档案信息安全至关重要，可借助安全信息和事件管理系统（SIEM）等技术手段，对档案信息系统展开全面、细致的监控，保证任何潜在的安全威胁都能被迅速察觉。同时，定期评估与复审不可或缺，要定期对档案信息安全风险评估体系进行评估和复审，紧密结合公安局业务发展和技术变化的实际情况，及时调整评估指标和方法，以此确保评估体系始终具备有效性和适应性，能准确反映档案信息安全面临的新情况、新问题。基于监控和评估结果，应稳步推进持续改进工作，不断优化风险应对措施，针对新发现的风险因素和安全事件制定更科学、有效的应对策略，还要从制度、技术、人员等多个层面持续改进档案信息安全管理工作，提高档案信息安全保障水平，形成动态、闭环的管理体系，确保档案信息随时都能得到可靠的安全保障，为公安局的各项工作提供坚实支撑。

3.4 与公安业务的融合

在支撑警务决策、促进信息共享和提升执法公信力方面，档案信息安全风险评估发挥着重要作用，在警务决策中，评估结果可作为关键参考，在制定重大警务行动方案时，充分考虑档案信息安全风险并采取相应防范措施，能有效规避潜在风险，保障警务行动顺利推进，防止因档案信息泄露等问题影响行动效果。在促进信息共享上，基于档案信息安全保障，可推动公安局内部各部门间的信息共享与协同工作，通过搭建安全的信息共享平台，实现档案信息的快速传递与高效利用，让各部门及时获取所需信息，提高公安工作整体效率，使各项警务工作更加协同、有序[3]。在提升执法公信力方面，可靠的档案信息安全保障是确保执法过程公正、透明的重要基础，公众对档案信息安全充满信任会增强对公安工作的认可，进而提升公安局的执法公信力。

结语

综上所述，档案信息安全风险评估体系的构建和应用，为公安局提供了一套全面、科学的风险管理工具。通过精准识别风险、有效评估风险，制定针对性应对措施，并持续监控与改进，确保了档案信息安全，同时评估体系与公安业务深度融合，为警务决策、信息共享和执法公信力提升提供了有力支撑，为公安工作高质量发展和社会长治久安奠定了坚实基础。

参考文献

[1]董旭冉,叶尔丰.数字化时代档案信息安全风险评估与防控体系构建[J].山西档案,2024(11):153-155.

[2]柴晶晶.数字档案馆建设中的信息安全风险评估与控制体系探讨[J].畅谈,2023(9):229-231.

[3]邓紊.事业单位档案保密风险评估、防控策略与“三合一”制度的融合实践[J].办公室业务,2025(6):134-136.