档案数据化过程中的安全风险与治理策略

陈晨[1] 侯燕军[2] 刘知[3]

1 湖北省汉江河道管理局后勤服务中心，湖北省潜江市，433100；

2 湖北省汉江河道管理局，湖北省潜江市，433100；

3 湖北省汉江河道管理局仙桃东荆河管理分局，湖北省潜江市，433100；

摘要：随着信息技术的飞速发展，档案数据化已成为档案管理领域的必然趋势。在档案数据化过程中，安全风险问题日益凸显，对档案的真实性、完整性和可用性构成了严重威胁。本文深入探讨了档案数据化过程中存在的数据泄露、篡改和丢失等安全风险现状，从技术、管理和人员层面分析了这些风险产生的成因。阐述了档案数据化安全风险治理对档案管理、社会稳定和国家信息安全的重要性。针对性地提出了技术防范、管理优化和人员培训等一系列治理策略，旨在为档案数据化的安全发展提供有益的参考和借鉴。

关键词：档案数据化；安全风险；治理策略

DOI：10.64216/3080-1486.25.12.099

引言

在当今数字化时代，信息技术的广泛应用深刻改变了档案管理的方式，档案数据化成为了档案事业发展的重要方向。档案数据化不仅提高了档案管理的效率和便捷性，还为档案信息的共享和利用提供了更广阔的空间。档案数据化在带来诸多便利的同时，也面临着前所未有的安全挑战。数据泄露、篡改和丢失等安全事件时有发生，给档案管理部门、社会和国家带来了严重的损失。深入研究档案数据化过程中的安全风险，并制定有效的治理策略，具有重要的现实意义。

1 档案数据化安全风险现状

1.1 数据泄露风险现状

在档案数据化过程中，数据泄露是最为常见且危害极大的安全风险之一。随着档案数据的数字化存储和传输，大量敏感信息以电子形式存在，这使得数据泄露的途径更加多样化。网络攻击是导致数据泄露的主要原因之一。黑客通过各种手段，如网络扫描、漏洞利用等，入侵档案管理系统，获取并窃取其中的敏感数据。例如，一些不法分子利用档案管理系统中存在的安全漏洞，绕过系统的身份验证和访问控制机制，非法获取档案数据并出售给第三方，给档案所有者带来了巨大的损失。

内部人员的违规操作也是数据泄露的重要风险因素。部分档案管理人员由于安全意识淡薄或受到利益诱惑，可能会将档案数据泄露给外部人员。一些档案管理部门在人员管理方面存在漏洞，对员工的权限设置不合理，导致员工可以随意访问和下载敏感档案数据，增加了数据泄露的风险。移动存储设备的使用也增加了数据泄露的可能性。员工在工作过程中，可能会将档案数据拷贝到移动硬盘、U 盘等存储设备中，一旦这些设备丢失或被盗，就可能导致档案数据的泄露[1]。

1.2 数据篡改风险现状

数据篡改是指对档案数据进行非法修改，以达到某种不正当目的的行为。在档案数据化过程中，数据篡改风险同样不容忽视。由于档案数据的数字化存储和处理，使得数据的修改变得更加容易和隐蔽。黑客可以通过攻击档案管理系统，修改其中的档案数据，破坏档案的真实性和完整性。例如，在企业的档案管理系统中，黑客可能会篡改员工的人事档案，为自己或他人谋取不正当利益。

内部人员的误操作或恶意篡改也是数据篡改的重要原因。档案管理人员在进行数据录入、修改等操作时，如果没有严格按照操作规程进行，可能会导致数据的错误修改。一些心怀不满的内部人员可能会故意篡改档案数据，以达到报复或其他目的。系统软件的漏洞也可能被利用来篡改档案数据。

1.3 数据丢失风险现状

数据丢失是档案数据化过程中面临的又一重要安全风险。自然灾害、硬件故障、软件故障等都可能导致档案数据的丢失。地震、火灾、水灾等自然灾害可能会破坏档案数据存储设备，导致数据无法恢复。例如，在一些地区，由于地震发生，档案管理部门的服务器和存储设备受到严重损坏，大量档案数据丢失，给档案管理工作带来了巨大的困难。

硬件故障也是数据丢失的常见原因之一。硬盘老化、损坏，服务器故障等都可能导致档案数据的丢失。一些档案管理部门由于资金有限，使用的存储设备老化严重，

没有及时进行更新和维护，增加了数据丢失的风险。软件故障也可能导致数据丢失。档案管理系统在运行过程中，可能会出现程序崩溃、数据损坏等问题，导致档案数据无法正常访问或丢失。人为因素也可能导致数据丢失[2]。档案管理人员在进行数据备份、迁移等操作时，如果操作不当，可能会导致数据丢失。

2 档案数据化安全风险成因分析

2.1 技术层面成因

从技术层面来看，档案数据化安全风险的产生主要与网络安全技术、数据存储技术和加密技术等方面的不足有关。网络安全技术的不完善是导致数据泄露和篡改的重要原因之一。目前，一些档案管理系统的网络防护能力较弱，无法有效抵御黑客的攻击。防火墙配置不合理，入侵检测系统的灵敏度较低，无法及时发现和阻止网络攻击行为。

数据存储技术的落后也增加了数据丢失的风险。一些档案管理部门仍然采用传统的磁带、磁盘等存储方式，这些存储设备的可靠性较低，容易受到物理损坏和数据老化的影响。数据存储的冗余度不足，一旦存储设备出现故障，就可能导致数据丢失。加密技术的应用不够广泛也是一个问题。部分档案管理系统没有对敏感档案数据进行加密处理，使得数据在传输和存储过程中容易被窃取和篡改。

2.2 管理层面成因

管理层面的问题也是档案数据化安全风险产生的重要原因。档案管理部门在安全管理制度方面存在漏洞，缺乏完善的安全管理体系。一些档案管理部门没有制定明确的安全管理规章制度，对档案数据的访问、存储、传输等环节没有严格的规定和约束。在人员管理方面，对员工的安全培训和教育不足，导致员工的安全意识淡薄，无法正确识别和防范安全风险。

档案管理部门在安全审计和监督方面存在不足。缺乏有效的安全审计机制，无法及时发现和纠正员工的违规操作行为。对档案管理系统的安全状况缺乏定期的评估和检查，不能及时发现和解决系统中存在的安全隐患。档案管理部门在应急管理方面也存在问题。没有制定完善的应急预案，在发生安全事件时，无法及时采取有效的应对措施，导致损失扩大。

2.3 人员层面成因

人员层面的因素对档案数据化安全风险的影响也不可忽视。部分档案管理人员的专业素质和技能水平较低，无法胜任档案数据化管理工作[3]。一些档案管理人员缺乏对信息技术和网络安全知识的了解，在操作档案管理系统时容易出现错误，增加了安全风险。档案管理人员的安全意识淡薄，对档案数据的安全重要性认识不足。在工作过程中，不遵守安全规定，随意泄露档案数据，给档案安全带来了严重威胁。

档案管理部门在人员招聘和选拔方面存在问题。在招聘档案管理人员时，没有对其安全意识和专业技能进行严格的考核和评估，导致一些不具备相应能力的人员进入档案管理岗位。在人员激励和约束机制方面也存在不足，对员工的违规行为缺乏有效的惩罚措施，对员工的安全工作缺乏足够的激励，影响了员工的工作积极性和责任感。

3 档案数据化安全风险治理的重要性

3.1 对档案管理的重要性

档案数据化安全风险治理对档案管理具有至关重要的意义。确保档案数据的安全是档案管理的基本要求。档案是历史的真实记录，具有重要的历史价值和参考价值。如果档案数据在数据化过程中出现泄露、篡改或丢失等安全问题，将严重影响档案的真实性和完整性，降低档案的利用价值。加强档案数据化安全风险治理，能够保障档案数据的安全，维护档案的历史价值和权威性。

档案数据化安全风险治理有助于提高档案管理的效率和质量。通过采取有效的安全治理策略，可以减少安全事件的发生，避免因安全问题导致的档案管理系统故障和数据丢失，保证档案管理工作的正常进行。安全治理策略的实施可以优化档案管理流程，提高档案管理人员的工作效率，提升档案管理的整体质量[4]。

3.2 对社会稳定的重要性

档案数据涉及到社会各个领域的信息，如个人隐私、企业商业秘密、政府机密等。档案数据的安全与社会稳定密切相关。如果档案数据泄露，可能会导致个人隐私被侵犯，引发社会公众的恐慌和不满。一些涉及个人敏感信息的档案数据泄露，可能会导致个人受到骚扰、诈骗等侵害，影响个人的正常生活。

企业档案数据的泄露可能会导致企业的商业秘密被竞争对手获取，给企业带来巨大的经济损失，甚至可能导致企业破产。这不仅会影响企业的发展，还会导致大量员工失业，对社会稳定造成不利影响。政府档案数据的安全关系到国家的政治稳定和社会秩序。政府的一些机密档案数据如果泄露，可能会被别有用心的人利用，制造社会混乱，破坏国家的安全和稳定。加强档案数据化安全风险治理，对于维护社会稳定具有重要的作用。

3.3 对国家信息安全的重要性

档案数据是国家信息资源的重要组成部分，档案数据化安全风险治理对国家信息安全具有重要的战略意义。随着信息技术的发展，国家之间的信息竞争日益激

烈，档案数据成为了国家重要的战略资源。如果档案数据在数据化过程中出现安全问题，可能会导致国家重要信息的泄露，给国家的安全和利益带来严重威胁[5]。

一些涉及国家军事、外交、科技等领域的档案数据，一旦泄露，可能会被敌对势力利用，对国家的安全和发展造成重大影响。加强档案数据化安全风险治理，能够保障国家档案数据的安全，维护国家的信息主权和安全利益。良好的档案数据化安全管理体系也有助于提高国家在国际信息领域的竞争力，促进国家信息产业的健康发展。

4 档案数据化安全风险治理策略

4.1 技术防范策略

在技术防范方面，首先要加强网络安全防护。档案管理部门应建立完善的网络安全防护体系，包括防火墙、入侵检测系统、加密技术等。防火墙可以有效阻止外部网络的非法访问，防止黑客的攻击。入侵检测系统可以实时监测网络中的异常行为，及时发现并报警。同时，采用加密技术对档案数据进行加密处理，确保数据在传输和存储过程中的安全性。例如，在档案数据的传输过程中，可以采用 SSL/TLS 加密协议，对数据进行加密传输，防止数据被窃取和篡改。

加强数据备份和恢复技术的应用。档案管理部门应定期对档案数据进行备份，并采用异地备份的方式，确保在发生自然灾害、硬件故障等情况时，能够及时恢复数据。可以采用磁带库、磁盘阵列等存储设备进行数据备份，同时建立数据恢复测试机制，定期对备份数据进行恢复测试，确保备份数据的可用性。

4.2 管理优化策略

在管理优化方面，档案管理部门应建立完善的安全管理制度。制定明确的安全管理规章制度，对档案数据的访问、存储、传输等环节进行严格的规定和约束。例如，建立用户身份认证和授权机制，对不同用户的权限进行合理设置，确保只有授权用户才能访问和操作档案数据。建立安全审计制度，对用户的操作行为进行实时监控和审计，及时发现和纠正违规操作行为。

加强人员管理。在人员招聘和选拔过程中，要对其安全意识和专业技能进行严格的考核和评估，确保招聘到具备相应能力的人员。加强对员工的安全培训和教育，提高员工的安全意识和专业技能。定期组织安全培训课程和演练，让员工了解档案数据化安全的重要性，掌握安全操作技能和应急处理方法。

4.3 人员培训策略

人员培训是档案数据化安全风险治理的重要环节。档案管理部门应制定系统的人员培训计划，对不同岗位的员工进行有针对性的培训。对于档案管理人员，应加强信息技术和网络安全知识的培训，提高其操作档案管理系统的能力和安全意识。培训内容可以包括档案管理系统的操作使用、网络安全基础知识、数据加密技术等。

对于档案管理部门的管理人员，应加强安全管理知识的培训，提高其安全管理水平。培训内容可以包括安全管理制度的制定和执行、安全风险评估和应对等。要注重培训的效果评估，通过考试、实际操作等方式对员工的培训效果进行评估，及时发现培训中存在的问题并进行改进。

5 结论

档案数据化是档案管理领域的发展趋势，但在数据化过程中面临着诸多安全风险。为了保障档案数据的安全，必须深入分析安全风险的成因，充分认识档案数据化安全风险治理的重要性，并采取有效的技术防范、管理优化和人员培训等治理策略。只有这样，才能确保档案数据化的安全发展，为档案管理事业和社会的稳定发展提供有力保障。

参考文献

[1]孙胜利,祁天娇.赋能数字文化产业发展：敦煌档案数据要素化转型探究[J/OL].档案管理,1-6[2025-10-09].

[2]王伟东.协同治理视域下人事档案数据化的实践路径研究[J].办公室业务,2025,(9):8-10.

[3]孙铭.浅析实现档案数据化的可行路径[J].黑龙江档案,2024,(4):211-213.

[4]李青.浅析档案管理数据化内涵、困境与对策[J].参花(上),2023,(10):110-112.

[5]金波,杨鹏,宋飞.档案数据化与数据档案化:档案数据内涵的双维透视[J].图书情报工作,2023,67(12):3-14.

作者简介：陈晨，出生年月：1990 年 7 月，性别：女，民族：汉族，籍贯：湖北武汉，学历：本科，职称（现职称）：助理馆员，研究方向：档案管理。

侯燕军，出生年月：1986 年 7 月，性别：女，民族：汉族，籍贯：湖北武汉，学历：本科，职称（现职称）：助理馆员，研究方向：档案管理。

刘知，出生年月：1990 年 2 月，性别：女，民族：汉族，籍贯：湖北武汉，学历：本科，职称（现职称）：助理馆员，研究方向：档案管理。