

Study on risk assessment and prevention strategy of electronic file storage security

Yun Zhou

Chifeng Ningcheng County Public Resource Trading Center, Chifeng, Inner Mongolia, 024200, China

Abstract

With the advent of the information age, electronic archives have become an indispensable part of modern society, widely used in governments, enterprises, and various institutions. However, the storage and management of electronic archives pose numerous security risks. How to ensure the security of electronic archives and prevent potential threats has become an urgent issue that needs to be addressed. This paper evaluates the risks associated with the storage security of electronic archives, discusses the main threats and risk factors currently faced, and proposes corresponding preventive strategies. The study shows that by strengthening technical protection measures, optimizing management processes, and enhancing personnel safety awareness, among other means, it is possible to effectively reduce the security risks of electronic archives, providing a guarantee for their long-term stable storage.

Keywords

electronic archives; storage security; risk assessment; prevention and control strategies; information security

电子档案存储安全风险评估与防控策略研究

周云

赤峰市宁城县公共资源交易中心, 中国·内蒙古 赤峰 024200

摘要

随着信息化时代的到来,电子档案已成为现代社会中不可或缺的一部分,广泛应用于政府、企业及各类机构。然而,电子档案的存储和管理带来了不少安全风险,如何保障电子档案的安全性,防范潜在的安全威胁,已成为当前亟待解决的问题。本文通过对电子档案存储安全风险评估,探讨了当前电子档案存储安全面临的主要威胁和风险因素,并提出了相应的防控策略。研究表明,针对电子档案存储的安全风险,可以通过强化技术防护措施、优化管理流程、提高人员安全意识等多方面的手段,有效减少电子档案的安全隐患,为电子档案的长期稳定存储提供保障。

关键词

电子档案; 存储安全; 风险评估; 防控策略; 信息安全

1 引言

随着信息技术的飞速发展,电子档案在各个领域的应用愈加广泛,成为现代社会不可或缺的重要组成部分。尤其是在政府机关、企事业单位、教育科研等各个领域,电子档案的存储与管理是日常工作中不可或缺的环节。然而,电子档案的存储面临诸多安全风险,尤其是数据泄露、篡改、丢失等安全问题,已成为当前社会面临的重要挑战。因此,研究电子档案存储安全风险评估与防控策略,不仅对提升信息安全具有重要意义,也为各类组织的电子档案管理提供了理论依据和实践指导。

目前,尽管许多国家和地区都在加强电子档案的管理和安全保护,制定了相关的政策法规,但由于技术手段不断

变化,安全防护的难度也在加大。电子档案的安全问题,除了外部攻击的威胁外,还有系统漏洞、管理不到位、人为疏忽等内因^[1]。为了有效预防和应对这些安全问题,必须深入分析电子档案存储的安全风险,建立健全的防控机制。

本文的研究目标是,通过分析电子档案存储中可能存在的安全风险,提出相应的防控策略,为提高电子档案的安全性提供理论支持。文章结构如下:第一部分分析电子档案存储的安全风险因素;第二部分探讨当前常见的安全防控措施;第三部分提出针对电子档案存储的安全防控策略;最后,给出结论。

2 电子档案存储安全风险评估

2.1 技术风险

技术风险是电子档案存储过程中最为常见的风险之一。随着信息技术的不断发展,各种新技术层出不穷,虽然这些新技术提升了档案存储的效率和便捷性,但也带来了不少新

【作者简介】周云(1975-),男,中国内蒙古赤峰人,本科,经济师,从事档案管理研究。

的安全隐患。

硬件故障：电子档案存储依赖于各种硬件设备，如服务器、存储设备等。若硬件出现故障，将导致电子档案无法访问，甚至可能造成数据丢失或损坏。

系统漏洞：电子档案存储系统通常包含多个软件系统，若其中某一部分存在漏洞，黑客可以利用这些漏洞对系统进行攻击，获取或篡改存储的数据。

恶意软件：恶意软件（如病毒、木马等）是电子档案存储中常见的安全威胁之一。这些恶意软件能够感染存储系统，导致档案数据丢失、泄露或被篡改。

2.2 人为风险

除了技术风险，人为因素同样在电子档案存储安全中占据重要地位。由于大多数电子档案管理系统都是由人来操作和维护的，因此人为操作失误和故意破坏等因素都可能引发安全问题^[2]。

操作失误：操作人员的疏忽或不当操作可能导致档案数据的丢失或损坏。例如，误删除、覆盖文件，或操作错误导致数据不一致。

权限管理不当：在电子档案的管理过程中，若权限分配不合理，可能会导致敏感信息泄露或未经授权的人员访问档案数据。

内部人员泄密：某些内部员工可能会由于个人原因或恶意行为，故意泄露电子档案中的敏感信息，给组织造成重大损失。

2.3 外部风险

外部风险主要指的是来自黑客攻击、自然灾害等外部因素对电子档案存储安全的威胁。

黑客攻击：随着网络攻击手段的不断升级，黑客通过网络入侵电子档案存储系统，窃取、篡改或删除档案数据的情况时有发生。黑客攻击不仅会造成数据的丢失或泄露，还可能对整个存储系统的可靠性和稳定性产生严重影响。

自然灾害：如火灾、地震、水灾等自然灾害也可能对存储设施造成严重破坏，进而导致电子档案数据的丢失。

3 电子档案存储安全防控措施

3.1 强化技术防护

备份机制：为了防止数据丢失或损坏，定期备份电子档案数据是一个有效的防护措施。通过定期备份，可以确保在发生故障或攻击时，可以恢复丢失的档案数据。

加密技术：对电子档案进行加密处理是防止数据泄露的有效手段。通过加密，只有具备相应权限的人才能访问和读取档案数据，从而减少数据泄露的风险。

防火墙与入侵检测系统：安装防火墙和入侵检测系统可以有效防止黑客攻击和恶意软件入侵，对存储系统进行实时监控，及时发现并阻止潜在的安全威胁。

3.2 优化管理流程

权限控制：对电子档案的访问权限进行严格控制，确

保只有经过授权的人员才能访问敏感信息。实施最小权限原则，避免不必要的权限滥用。

安全审计：建立安全审计机制，记录所有访问和操作档案的行为。通过定期审查审计日志，及时发现异常操作，并采取相应措施进行处理。

人员培训：定期对电子档案管理人员进行安全培训，提高其安全意识和应对突发事件的能力。通过提高员工的安全意识，减少人为失误和内部泄密的风险。

4 电子档案存储安全风险防控策略

4.1 多层次防护策略

为了有效应对电子档案存储中的各种安全风险，必须采用多层次的防护策略。这种策略不仅仅依赖于单一的技术防护，而是通过技术与管理的结合，形成从多个方面共同保障档案存储安全的防护体系。

物理层防护：物理安全是确保电子档案存储系统正常运行的基础。确保存储设备所在的物理环境安全，可以有效避免火灾、水灾等自然灾害对存储设施造成破坏。为此，需要通过对数据存储设备的硬件设施进行定期检查，确保设备处于良好工作状态。同时，存储设备应放置在专门的机房中，机房需符合消防标准并配置温湿度控制系统，避免由于设备过热或潮湿引发故障^[3]。为了进一步增强物理防护，还应设置门禁系统，限制未授权人员进入存储设备区域。除了自然灾害的预防，物理防护还需要加强设备的防盗措施，确保存储设施免受盗窃或人为破坏。

网络层防护：在网络层防护方面，必须通过多重网络安全技术确保电子档案存储系统的安全性。首先，安装防火墙和入侵检测系统（IDS）是必不可少的，这些技术可以帮助防止黑客通过网络攻击存储系统，避免恶意软件的侵入。防火墙能够有效控制外部网络流量，防止未经授权的访问，而入侵检测系统则能够及时检测并响应入侵行为，减少潜在风险。此外，对于存储系统的网络进行隔离管理，也能减少不同系统之间的安全漏洞传播风险。数据在传输过程中需要进行加密，以防止在网络中途遭受截获或篡改。通过部署虚拟专用网络（VPN）等技术手段，可以确保敏感档案在传输过程中的保密性与完整性。

应用层防护：在应用层，电子档案存储系统的安全性同样需要充分保障。加密技术是保障数据安全的重要手段。无论是在存储数据时，还是在数据交换过程中，都需要通过加密算法保护档案数据的机密性。例如，使用 AES（高级加密标准）等强加密算法对存储数据进行加密，可以有效防止数据被未经授权的人员读取。备份同样是关键的安全措施，定期备份可以确保在数据丢失或遭受攻击时能及时恢复系统。除此之外，还应加强应用软件的安全性，避免因软件漏洞导致的数据泄露或损坏。为此，系统应进行定期的软件更新和漏洞扫描，及时修补存在的安全漏洞。此外，用户身份验证和访问控制措施也应得当，确保只有经过授权的用户

才能访问和操作存储数据。

4.2 风险评估与应急响应

建立完善的电子档案存储安全风险评估机制是提高档案存储安全性的关键一步。通过定期对存储系统的安全性进行评估,能够及时发现潜在的风险并采取有效措施进行化解。风险评估是一个系统化的过程,不仅仅依赖于技术手段,还需要结合管理层的定期审查,以确保所有潜在的安全威胁都能得到充分的关注和处理。

定期安全评估:定期的风险评估可以帮助组织及时识别存储系统中的潜在风险,包括硬件故障、软件漏洞、网络攻击等。评估过程应包含对现有安全防护措施的检查,评估其有效性,并在此基础上提出改进建议。例如,在硬件方面,需要对设备的老化情况进行检查,确保设备能够继续稳定运行;在软件方面,需要检查系统的补丁更新情况,确保没有已知漏洞未修补。在进行评估时,还应充分考虑外部环境的变化,例如网络安全形势的变化、自然灾害的影响等因素。这一评估应由专门的安全团队来完成,并结合自动化工具对系统的弱点进行扫描,确保评估覆盖全面、深入。

应急响应机制:一旦发生安全事件,能够迅速启动应急响应机制是防控风险的关键。应急响应机制应明确各类安全事件的应对措施,包括黑客攻击、数据泄露、系统崩溃等常见情况。应急响应机制需要明确各方责任、制定应急处理流程、并进行定期的应急演练,确保在安全事件发生时,相关人员能够迅速、有效地采取措施,最大程度减少损失。应急响应计划应包括事件检测、报告、分析、响应、恢复等阶段,并确保各阶段的顺利衔接。对于数据泄露或篡改的事件,应及时启动数据恢复流程,并通过法律途径追责,防止事件进一步扩大^[4]。应急响应机制的建立不仅能减少事故发生后的影响,也能提升系统的韧性和恢复能力。

5 电子档案存储安全的未来发展趋势

随着信息技术的不断发展,电子档案存储面临的安全威胁日益复杂。除了传统的黑客攻击、硬件故障等问题外,随着新兴技术的不断发展,电子档案存储的安全防控体系也需要适应这些新挑战。未来,电子档案存储的安全防控将朝着智能化、分布式和区块链化等方向发展。

智能化防控:随着人工智能技术的不断成熟,智能化防控将成为电子档案存储安全的一个重要趋势。通过引入人工智能技术,可以实现对存储系统的实时监控与自动化风险识别。人工智能能够通过大数据分析技术,挖掘存储系统中的潜在风险,提前发现异常行为或潜在的安全漏洞,及时发出警报。此外,人工智能还可以根据系统的运行情况,

智能化调整存储系统的安全策略。例如,基于用户行为分析(UBA)技术,可以通过监控用户的访问模式,及时发现是否有异常的访问行为,从而减少内部人员的恶意行为。人工智能的应用可以大幅提升安全防护效率和准确性。

分布式存储:随着云计算和大数据技术的发展,分布式存储逐渐成为一种新兴的存储方式。与传统的集中式存储方式相比,分布式存储通过将数据分散存储在多个地点,从而有效降低单点故障的风险。对于电子档案存储而言,采用分布式存储能够确保数据在遭遇系统故障、自然灾害等情况下仍然能够保持完整和可用。

区块链技术:区块链技术以其去中心化、不可篡改和透明的特点,为电子档案的安全提供了强有力的保障。区块链能够通过将电子档案的数据进行加密并存储在多个节点上,确保数据的完整性和不可篡改性。电子档案一旦上链,就无法被任何一方单方面修改或删除,从而大大增强了档案的可信度。此外,区块链技术还能提供高度透明的审计功能,使得每一笔操作都能够追溯,增加数据的可信性和安全性^[5]。在未来,区块链技术有望成为电子档案存储系统的重要组成部分,为档案管理带来新的突破。

6 结语

电子档案存储的安全性是信息化时代信息保护的重要组成部分,直接关系到各类组织的运营安全和数据完整性。通过本文对电子档案存储安全风险评估与防控策略的分析,提出了针对技术、管理和人员培训等多个层面的防控措施。随着科技的不断进步,新的技术和手段必将不断涌现,电子档案存储的安全防控将变得更加智能化和多元化。只有与时俱进,不断完善安全防控体系,才能有效应对日益复杂的安全挑战,保障电子档案的安全与完整。未来,我们应继续关注新技术的应用和发展,及时调整防控策略,确保电子档案存储系统始终保持高度的安全性。

参考文献

- [1] 张美芳,马丹宁.声像档案数字化抢救中存储与长期保存策略的研究[J].数字与缩微影像,2007(01):26-29.
- [2] 黄昌瑛.电子档案信息安全保障策略研究[D].福建师范大学,2007.
- [3] 田淑华.电子档案信息安全管理研究[D].中北大学,2009.
- [4] 李玉虎,黄丽华,张美芳,等.全国档案科技发展的研究报告[C]//中国档案学会.回顾与展望——中国档案事业发展研究报告.中国档案学会档案保护技术委员会,2010:249-280.
- [5] 中国机电兵船工业档案学会2010年学术论文评审结果[J].机电兵船档案,2010(06):4-11.