 DOI: https://doi.org/10.12345/daglyqyfzyj.v3i6.28337

Research on the construction of risk prevention and control mechanism of state-owned enterprises

Chaoyu Huo

Sinopec Northwest Branch, Urumqi, Xinjiang, 830011, China

Abstract

With the advancement of information process, the digital transformation of state-owned enterprises (state-owned enterprises) in the field of archives management is gradually accelerating. As an important knowledge wealth and operational data of enterprises, archival information plays an important role in the development of enterprises. However, with the gradual development of archival information to electronic and network, the problem of information security is becoming increasingly serious. The leakage, tampering, loss of file information and other problems seriously affect the normal operation and development of enterprises, and may even bring incalculable losses. How to effectively prevent and control the risk of archival information security while ensuring the convenient flow of information has become an important issue facing the current state-owned enterprises. By analyzing the current situation and characteristics of the archival information security risk of state-owned enterprises, this paper discusses the construction path of the information security risk prevention and control mechanism. Research shows that state-owned enterprises need to strengthen system construction, enhance technical protection ability, and strengthen personnel safety awareness. Through the construction of a perfect information security risk prevention and control mechanism, it can effectively prevent and resolve the file information security risks, ensure the stability and sustainable development of enterprise operation, and provide a solid guarantee for the digital transformation and modern management of state-owned enterprises.

Keywords

state-owned enterprises; archival information; security risk; prevention and control mechanism; digital transformation

国企档案信息安全风险防控机制构建研究

霍超宇

中国石化西北分公司，中国·新疆 乌鲁木齐 830011

摘　要

随着信息化进程的推进，国有企业（国企）在档案管理领域的数字化转型逐渐加快。档案信息作为企业重要的知识财富和运营数据，在企业发展中扮演着重要角色。然而，随着档案信息逐渐向电子化、网络化发展，信息安全问题也日益严重。档案信息的泄露、篡改、丢失等问题，严重影响企业的正常运营和发展，甚至可能带来不可估量的损失。如何在确保信息便捷流转的同时有效防控档案信息安全风险，已成为当前国企面临的重要课题。本文通过分析国企档案信息安全风险的现状与特点，探讨信息安全风险防控机制的构建路径。研究表明，国企需要在加强制度建设、提升技术防护能力、加强人员安全意识等方面进行综合治理。通过构建完善的信息安全风险防控机制，能够有效防范和化解档案信息安全风险，保障企业运营的稳定与可持续发展，为国企的数字化转型和现代化管理提供坚实保障。

关键词

国有企业；档案信息；安全风险；防控机制；数字化转型

1 引言

随着信息化进程的不断推进，企业管理、运营和档案管理的方式逐渐向数字化、网络化转型，档案信息的管理方式也在发生深刻变革。在这一过程中，档案信息的安全问题愈发突出，尤其在国有企业中，档案信息不仅涉及企业内部机密，还关系到国家经济安全和社会稳定。档案信息的泄露、篡改、丢失等问题将给企业带来不可估量的损失，甚至可能危及国家安全。随着信息技术的不断创新，越来越多的档案信息以数字化方式存储与传输，这对信息安全提出了更高的要求。

然而，在信息化快速发展的背景下，许多国企在信息安全管理方面仍然存在不足，未能建立健全的信息安全防控机制。信息技术的飞速发展带来的是信息安全形势的不断变化，传统的安全管理手段已经无法满足新形势下对档案信息的保护需求。国企在技术防护、人员培训、制度建设等方面的薄弱，导致档案信息安全面临诸多风险。

因此，国有企业亟须构建一套适应信息化要求、涵盖

【作者简介】霍超宇（1987–），男，中国陕西渭南人，本科，馆员，从事档案管理研究。

技术、管理、制度、人员等多方面的档案信息安全风险防控机制。本文将探讨如何在信息化背景下，通过加强制度建设、技术防护和人员教育等方面，建立起全面的信息安全防控体系，确保国企档案信息的安全，并为企业的长期稳定发展提供有力支持。

2 国企档案信息安全的现状与挑战

2.1 国企档案信息安全管理现状

随着信息化程度的不断提升，国企档案管理逐渐实现了电子化和网络化，带来了更高效的管理方式。然而，当前国企在档案信息管理上仍面临不少问题。首先，部分国企的信息化建设起步较晚，档案管理依然主要依靠纸质档案和传统的管理方式进行，导致信息安全问题较为突出。在这些企业中，档案信息的保护措施不足，容易受到各种威胁。其次，尽管一些企业在数字化方面取得了进展，信息系统的安全防护措施和技术手段仍存在差距。例如，某些企业的档案信息管理系统未能实现数据加密、访问控制等基本的安全防护手段，使得档案信息容易受到黑客攻击、病毒入侵等安全威胁。此外，国企档案管理人员的安全意识普遍较低，部分人员对信息安全问题缺乏足够的重视，且在技术操作和管理方面存在不足，这进一步加大了安全隐患。

2.2 档案信息安全面临的主要风险

在信息化进程中，国企档案信息安全面临的风险日益严峻。首先，信息泄露风险是最为严重的安全隐患之一。档案信息一旦被非法获取，可能导致企业的核心机密、业务流程、客户数据被外部人员掌握，严重影响企业的经济利益和声誉，甚至会威胁到国家安全。其次，信息篡改风险日益突出，尤其是在网络环境中，黑客通过恶意攻击手段篡改档案内容，可能影响企业的决策判断，导致不必要的经济损失。此外，档案信息的丢失风险也不可忽视。无论是由于系统故障、技术问题，还是人为疏忽，档案信息在存储和传输过程中丢失的情况时有发生，极大地影响了企业日常业务的正常开展，甚至可能影响决策的准确性。最后，技术风险也是国企面临的重要挑战，随着信息技术的不断发展，新型攻击方式和技术漏洞不断出现，现有的防护措施往往无法及时应对这些新兴威胁，进一步加剧了信息安全的复杂性。

2.3 安全防控面临的挑战

在面对日益严峻的档案信息安全问题时，国企的安全防控工作仍然面临诸多挑战。首先，技术防护能力不足是企业安全防控的主要瓶颈。尽管一些企业在信息化建设方面投入了大量资源，但多数企业的信息系统仍处于建设初期，技术防护措施尚不完善。尤其是在数据加密、身份验证和访问控制等关键领域，许多企业的技术手段还远远落后，无法有效防御各种网络安全攻击。其次，制度建设不完善也是一个亟待解决的问题。当前，国企的档案信息安全管理制度还不够健全，缺乏针对性的安全管理规范和应急响应机制。这使得当出现安全问题时，企业往往缺乏有效的应对措施，处于被动地应对状态。最后，人员安全意识薄弱也是导致信息安全隐患频发的重要原因。很多企业的管理人员和普通员工对信息安全问题的重视程度不够，缺乏必要的安全意识和操作规范，容易因操作不当或人为疏忽导致安全事件发生。因此，提升人员的安全意识，开展针对性地培训，成为解决这一问题的关键 [1]。

3 国企档案信息安全防控机制的构建

3.1 加强制度建设，制定信息安全管理规范

完善的信息安全制度是保障档案信息安全的基础。国企应根据实际情况，建立和完善档案信息安全管理制度，制定详细的操作流程、权限管理规定、数据保护措施等，以确保档案信息安全管理的规范性。具体来说，可以从以下几个方面入手：首先，建立信息安全责任制，明确各部门、各岗位的安全责任，落实信息安全管理的具体责任，形成多层次、全覆盖的信息安全管理责任体系，确保责任到位，减少安全管理漏洞。其次，加强信息安全政策和规范的制定，依据国家和行业标准，制定企业内部的信息安全管理政策，细化信息安全管理的具体操作规范，确保各项工作有章可循，提升执行力和透明度。最后，建立信息安全应急响应机制，制定应急预案，建立信息安全事件的响应机制，确保在发生安全事件时，能够及时、有效地进行应对，减少损失并快速恢复正常运行。通过这些措施，国企可以为档案信息的安全提供更加坚实的保障 [2]。

3.2 提升技术防护能力，构建多层次的安全防护体系

技术防护是防止信息安全事件发生的关键。国企应积极引入先进的安全技术，构建多层次的档案信息安全防护体系，确保企业信息系统的稳定与安全。具体包括：首先，数据加密与备份，对企业档案信息进行加密处理，确保信息在存储和传输过程中的安全性，避免数据被泄露或篡改。同时，定期进行数据备份，以防数据丢失或损坏，并确保在灾难发生时能够迅速恢复业务。其次，访问控制与身份认证，建立严格的身份认证机制，确保只有授权人员才能访问档案信息。通过多因素认证等技术手段，提高访问控制的安全性，防止非法访问和数据泄露。第三，网络安全防护，部署防火墙、入侵检测系统等设备，加强网络安全防护，确保企业网络环境的安全。同时，定期进行漏洞扫描和系统安全测试，及时发现并修复潜在的安全隐患，降低安全风险。最后，数据审计与监控，建立数据审计和监控机制，对档案信息的存取、使用和传输进行实时监控，确保数据操作的透明性，并及时发现异常行为，避免安全风险的蔓延。通过这些技术手段，企业能够构建起严密的安全防线，确保档案信息的安全 [3]。

3.3 加强人员安全教育，提升安全意识

人员的安全意识和操作规范是信息安全防控的关键。国企应加强对员工的信息安全培训，提高全员的信息安全意

识，并制定操作规范，确保每个员工都能正确应对信息安全问题。具体包括：首先，定期开展安全培训，通过定期的培训和演练，提高员工对信息安全的认识和应对能力。培训内容应涵盖信息安全基本知识、常见安全威胁、操作规范等，确保员工能够在日常工作中遵循安全规范，从而有效降低人为错误带来的风险。其次，加强内部安全文化建设，通过宣传教育和安全文化建设，提高全员的安全意识，营造全员参与信息安全管理的氛围，使信息安全意识成为企业文化的重要组成部分，提升整体的安全防控水平。最后，强化岗位安全管理，根据不同岗位的安全需求，制定个性化的安全操作规范，确保每个岗位的员工都能够按照规定的安全要求进行操作，减少人为失误和安全漏洞的发生。通过加强人员安全教育和提升安全意识，国企可以建立一个强大的安全防控体系，减少因人为因素引发的安全问题 [4]。

4 国企档案信息安全防控机制的实施效果与展望

4.1 实施效果

通过构建完善的档案信息安全风险防控机制，国企在多个方面取得了积极效果。首先，信息安全水平显著提升。企业通过制定详细的制度、加强技术防护措施以及开展定期的人员培训等多方面的举措，成功提升了档案信息管理的安全水平，信息安全事件发生的频率大幅降低。特别是在信息系统的防护、数据加密、备份恢复等方面的技术应用，为企业提供了强有力的安全保障。其次，风险防控能力增强。随着应急响应机制和技术手段的不断完善，企业对各种安全威胁能够进行更迅速、更有效地应对。面对恶意攻击、病毒入侵等安全事件时，能够在最短的时间内进行隔离、修复，降低了企业遭受损失的风险。此外，企业在内部信息流转环节中，采取了多重安全控制措施，通过设定严格的访问权限、加密数据传输、实时监控等手段，有效保障了档案信息的流转安全，使得信息在传递过程中不易被篡改、泄漏或者丢失，从而增强了企业运营的稳定性和信息透明度 [5]。

4.2 未来展望

随着信息化技术的不断发展，国企面临的档案信息安全挑战日益复杂多变。未来，企业在构建档案信息安全防控机制时，应不断加强技术创新，提高防护能力，尤其是在数据加密、网络安全、漏洞修复等关键领域，需要持续关注最新的技术发展趋势，及时应对潜在的安全威胁。同时，国企应密切关注国家在信息安全领域的政策变化，响应国家号召，推动档案信息管理的标准化、规范化，确保符合日益严格的信息安全法律法规。随着大数据、云计算、人工智能等新技术的不断融入，企业的档案信息安全防控机制需要进行相应的优化。例如，通过人工智能技术分析潜在的安全风险、云计算技术保障数据存储与计算的安全等，从而更高效、更精准地进行防控。国企应紧跟科技步伐，不断优化现有的安全防控措施，以应对未来复杂的安全挑战，确保档案信息的安全性和完整性，为企业的可持续发展提供有力保障。

5 结语

随着信息化技术的不断发展，国企在档案信息安全管理方面面临的风险和挑战也在不断增加。为了应对这些挑战，国企需要构建完善的信息安全防控机制，涵盖制度建设、技术防护、人员培训等多个方面。通过提升信息安全水平、增强风险防控能力，国企能够有效保障档案信息的安全，为企业的稳定运行提供保障。未来，随着新技术的不断发展，信息安全防控机制也应不断创新，以适应新的信息安全需求，确保国企在数字化转型过程中能够安全、稳定、可持续地发展，并进一步推动企业的现代化建设。不断优化和完善信息安全管理体系，将成为国企适应未来发展环境的重要保障，助力企业在竞争激烈的市场中立足长远。

参考文献

[1] 李欣.档案赋能安全风险管控的理论阐释与实践样态[J].山西档案,2024,(09):153-155.

[2] 张丁元.信息化视角下干部人事档案管理研究[J].办公室业务,2024,(17):25-27.

[3] 方华,谭必勇.档案数据治理体系构建的价值导向[J].中国档案研究,2024,(01):152-170.

[4] 马丹.融媒体环境下档案信息化管理探究[J].黑龙江档案,2024,(04):133-135.

[5] 宋燕,张宁,王爽.数字化背景下医院档案信息化建设探究[J].黑龙江档案,2024,(04):241-243.