 DOI: https://doi.org/10.12349/iser.v6i9.7442

Research on network information security management in enterprise informatization construction

Lei Yang

Inner Mongolia Civil Aviation Airport Group Co., Ltd. Hohhot Branch, Hohhot, Inner Mongolia, 010000, China

Abstract

With the accelerated digital transformation and widespread adoption of information technology, enterprise informatization has become a critical pathway to enhance competitiveness. However, the escalating cybersecurity threats have made information security management a major challenge that enterprises must confront. Starting from the practical needs of enterprise informatization, this study provides an in-depth analysis of the importance of network information security management. It systematically explores six key security management strategies: technical protection, institutional norms, personnel training, risk control, technological innovation, and supply chain management. The research reveals that establishing a multi-layered and comprehensive security protection system forms the foundation for ensuring enterprise information security. Moreover, the organic integration of technical measures and management practices is crucial for enhancing security effectiveness.

Keywords

enterprise informatization; network security; information security management

企业信息化建设中的网络信息安全管理研究

杨蕾

内蒙古自治区民航机场集团有限责任公司呼和浩特分公司，中国 · 内蒙古 呼和浩特 010000

摘　要

随着数字化转型进程的加速推进和信息技术的广泛应用，企业信息化建设已成为提升竞争力的关键途径，然而网络安全威胁的日益严峻使得信息安全管理成为企业必须面对的重大挑战，本研究从企业信息化建设的实际需求出发，深入分析了网络信息安全管理的重要性，系统探讨了包括技术防护、制度规范、人员培养、风险管控、技术创新和供应链管理在内的六大安全管理策略，研究发现，构建多层次、立体化的安全防护体系是保障企业信息安全的基础，而将技术手段与管理措施有机结合则是提升安全防护效能的关键。

关键词

企业信息化；网络安全；信息安全管理

1 引言

在全球数字经济蓬勃发展的背景下，企业信息化建设已经从可选项转变为必选项，成为企业保持市场竞争优势的重要支撑，但与此同时，网络攻击手段的不断升级、数据泄露事件的频繁发生，以及各类安全威胁的层出不穷，使得网络信息安全问题日益凸显，成为制约企业信息化健康发展的关键因素，如何在推进信息化建设的同时确保网络信息安全，已经成为企业管理者必须深入思考和着力解决的核心问题，基于此，本文将从企业信息化建设的现实需求出发，全面剖析网络信息安全管理的重要性，并提出切实可行的管理策略，以期为企业构建安全可靠的信息化环境提供理论指导和实践参考。

【作者简介】杨蕾（1987–），女，中国甘肃隆德人，本科，工程师，从事网络信息安全研究。

2 企业信息化建设中的网络信息安全管理重要性

2.1 确保核心业务数据安全，防范机密信息泄露风险

企业在信息化建设过程中产生和积累的海量数据已成为其最宝贵的资产之一，这些数据涵盖了客户资料、财务信息、研发成果、战略规划等核心商业机密，一旦发生泄露将给企业带来难以估量的损失，网络信息安全管理的首要任务便是为这些关键数据筑起坚固的防护屏障，防止内部人员的恶意窃取和外部黑客的非法入侵 [1]。在当今复杂多变的网络环境中，数据泄露的途径日趋多样化，既包括传统的网络攻击手段，也涉及社会工程学等新型威胁方式，因此企业必须建立全方位的数据安全防护机制，从数据的产生、传输、存储到使用的各个环节实施严格管控，确保核心业务数据始终

处于安全可控的状态之下。

2.2 维护系统运行稳定性，保障企业运营连续性

信息系统的稳定运行是企业正常开展各项业务活动的基础保障，而网络安全事件往往会导致系统崩溃、服务中断等严重后果，直接影响企业的生产经营活动。勒索软件攻击、分布式拒绝服务攻击等恶意行为可能使企业的核心业务系统陷入瘫痪，造成订单处理延误、生产线停工、客户服务中断等一系列连锁反应，进而导致经济损失和声誉受损，强化网络信息安全管理能够有效预防和抵御各类网络攻击，确保企业信息系统的高可用性和业务连续性。此外，完善的安全管理体系还能够帮助企业建立快速响应和灾难恢复机制，即使在遭受攻击的情况下也能够迅速恢复系统运行，将损失降至最低，从而为企业的稳健发展提供坚实保障。

2.3 满足合规监管要求，规避法律责任和经济损失

随着各国对数据安全和隐私保护的重视程度不断提升，相关法律法规日趋严格和完善，对企业的网络信息安全管理提出了更高要求，欧盟《通用数据保护条例》、中国《网络安全法》《数据安全法》等法规的实施，明确规定了企业在数据收集、处理、存储等方面的合规义务，违反相关规定将面临巨额罚款和法律制裁 [2]。企业必须建立符合监管要求的安全管理体系，确保在数据处理的全生命周期中严格遵守相关法律法规，这不仅是企业履行社会责任的体现，更是避免法律风险和经济损失的必要举措。同时，良好的安全合规管理还能够提升企业的市场信誉和客户信任度，为企业赢得更广阔的发展空间和更多的商业机会，成为企业核心竞争力的重要组成部分。

3 企业信息化建设中的网络信息安全管理策略

3.1 构建多层次技术防护体系，实现纵深安全防御机制

企业应当采用纵深防御的理念构建多层次的技术防护体系，形成从网络边界到核心数据的立体防护架构，在网络边界层面部署高性能防火墙、入侵检测系统和入侵防御系统，实时监控和阻断外部威胁，在网络内部实施网络分段和访问控制，将不同安全级别的系统和数据进行隔离，防止威胁的横向扩散，针对终端设备部署终端安全管理平台，统一管理防病毒软件、主机防火墙和设备准入控制，确保每一个接入点的安全性。

在应用层面实施 Web 应用防火墙、数据库审计系统等专业防护措施，对应用程序的输入输出进行严格检查，防范 SQL 注入、跨站脚本等常见攻击，同时部署数据防泄露系统，对敏感数据的流转进行全程监控和管控，防止内部数据的非授权外传，在数据层面采用加密技术对重要数据进行加密存储和传输，确保即使数据被窃取也无法被解读利用。

3.2 建立完善制度规范体系，强化安全管理标准化程度

制度建设是网络信息安全管理的基础工作，企业需要建立涵盖组织架构、岗位职责、操作流程、应急预案等各个方面的完整制度体系，首先明确安全管理的组织架构和责任分工，设立专门的信息安全管理部门或安全管理委员会，明确各级管理人员和技术人员的安全职责，建立自上而下的安全责任体系，确保安全管理工作有人抓、有人管、有人负责 [3]。

制定详细的安全操作规程和管理流程，包括账号管理、权限分配、数据备份、系统维护、安全审计等各项日常工作的标准化操作程序，每一项操作都应有明确的执行步骤、审批流程和记录要求，避免因操作不当造成的安全隐患，建立安全事件分级分类标准和应急响应预案，明确不同级别安全事件的处置流程和责任人，确保在安全事件发生时能够快速、有序地进行处置。

3.3 加强人员安全意识培养，提升全员网络安全防护能力

人是网络安全防护体系中最关键也是最薄弱的环节，企业必须高度重视员工安全意识的培养和安全技能的提升，建立分层分类的安全培训体系，针对不同岗位、不同层级的人员制定差异化的培训方案，对于普通员工重点培训基础安全知识、安全操作规范和常见威胁识别方法，对于技术人员则加强专业安全技能和最新攻防技术的培训，对于管理人员着重培养安全管理理念和决策能力。

创新培训方式方法，采用案例分析、模拟演练、在线学习等多种形式开展培训活动，特别是通过真实案例的剖析让员工深刻认识到安全威胁的严重性和防护的必要性，定期组织钓鱼邮件测试、社会工程学演练等实战化训练，检验员工的安全意识水平和应对能力，对于测试中暴露出的问题进行针对性的强化培训，营造浓厚的安全文化氛围，通过安全知识竞赛、安全主题活动、安全标语宣传等方式，让安全意识深入人心，成为企业文化的重要组成部分。

3.4 实施动态风险评估管控，建立预警响应处置联动机制

风险管理是网络信息安全管理的核心环节，企业需要建立动态的风险评估和管控机制，持续识别、评估和应对各类安全风险，构建全面的资产台账和风险清单，对企业的信息资产进行分类分级管理，明确各类资产的重要程度和面临的主要威胁 [4]，采用定性和定量相结合的方法进行风险评估，综合考虑威胁发生的可能性和影响程度，确定风险等级和优先处置顺序。

部署安全态势感知平台，整合各类安全设备和系统的日志信息，运用大数据分析和人工智能技术进行威胁检测和行为分析，实现对安全风险的实时监测和预警，建立分级分类的预警机制，根据威胁的严重程度和紧急程度采取不同的响应措施，对于高危威胁立即启动应急响应流程，对于中低风险制定整改计划并限期完成，构建安全运营中心，配备专业的安全分析人员进行 7×24 小时的安全监控和事件处置。

建立与外部安全机构的合作机制，及时获取最新的威胁情报和漏洞信息，提前做好防范准备，定期开展渗透测试、

漏洞扫描等主动安全检测活动，发现系统和应用中存在的安全隐患并及时修复，建立安全事件的复盘机制，对已发生的安全事件进行深入分析，总结经验教训，优化防护策略和响应流程，形成持续改进的闭环管理模式，确保安全防护能力不断提升。

3.5 推进安全技术创新应用，提升智能化防护检测水平

面对日益复杂和智能化的网络威胁，企业必须积极拥抱新技术，推动安全防护手段的创新升级，将人工智能和机器学习技术应用于安全领域，建立基于 AI 的威胁检测和响应系统，通过对海量安全数据的深度学习和模式识别，实现对未知威胁和零日攻击的有效检测，利用机器学习算法建立用户和实体行为基线，对异常行为进行智能识别和预警，大幅提升安全检测的准确性和及时性。

探索区块链技术在数据安全和身份认证方面的应用，利用区块链的不可篡改性和去中心化特性，建立可信的数据共享和身份验证机制，特别是在供应链安全管理和多方数据协作场景中，区块链技术能够提供更加安全可靠的解决方案，推进零信任安全架构的建设，摒弃传统的边界防护理念，对所有用户、设备和应用进行持续验证和动态授权，实现更加精细化和智能化的访问控制 [5]。

部署安全编排自动化和响应平台，将安全事件的检测、分析、响应和处置流程进行自动化编排，大幅缩短安全事件的响应时间，提升处置效率，探索量子加密、同态加密等前沿加密技术的应用，为未来的数据安全防护做好技术储备，建立安全技术创新实验室或与高校、科研机构合作，持续跟踪和研究最新的安全技术发展趋势，确保企业的安全防护能力始终保持在行业前列。

3.6 完善第三方合作管理，确保供应链安全可控性

在企业信息化建设过程中，第三方合作伙伴的参与不可避免，包括软件供应商、系统集成商、云服务提供商、外包服务商等，这些第三方往往需要接触企业的敏感信息和关键系统，因此加强第三方安全管理至关重要，建立严格的供应商准入机制，在选择合作伙伴时将安全能力作为重要评估指标，要求供应商提供安全资质证明、安全管理体系文档和过往安全事件记录，对于关键供应商进行现场安全审计，确保其具备足够的安全保障能力。

在合同签订阶段明确双方的安全责任和义务，包括数据保护要求、安全事件通报机制、违约责任条款等，要求供应商签署保密协议和安全承诺书，对于需要访问企业系统或数据的第三方人员，实施与内部员工同等严格的身份认证和权限管理，建立专门的第三方访问通道和监控机制，对其操作行为进行全程记录和审计，定期评估第三方的安全状况，通过安全检查、渗透测试等方式验证其安全措施的有效性。

建立供应链安全风险评估机制，识别供应链各环节可能存在的安全隐患，特别关注关键组件和服务的安全性，对于发现的风险制定相应的缓解措施，建立多供应商策略，避免对单一供应商的过度依赖，降低供应链中断的风险，加强与供应商的安全协同，建立安全信息共享机制，及时通报安全威胁和漏洞信息，共同提升整个供应链的安全防护水平，在供应商退出时做好安全收尾工作，确保企业数据和访问权限的完全回收，防止安全风险的延续。

4 结语

企业信息化建设中的网络信息安全管理是一项系统性、持续性的工作，需要企业从战略高度充分认识其重要性，在未来的发展中，企业应当持续关注网络安全技术的演进趋势，不断优化和完善安全管理体系，将安全理念融入企业文化和业务流程的方方面面，只有这样才能在享受信息化带来的效率提升和竞争优势的同时，确保企业的信息资产安全和业务的持续稳定发展，为企业的数字化转型和长远发展奠定坚实基础。

参考文献

[1] 吴琴. 国有企业信息化建设中的网络安全管理探讨[J].科技创新导报,2021,18(24):134-136.

[2] 王秀斌. 企业信息化建设中的网络安全管理问题分析[J].中国管理信息化,2021,24(06):103-104.

[3] 汤荣秀. 企业信息化建设中的网络信息安全[J].信息与电脑(理论版),2020,32(23):230-232.

[4] 刘忠海,刘永胜,于海,等. 对企业信息化建设中的网络安全管理问题探讨[J].数码世界,2020,(11):258-259.

[5] 何玉譞,姚沪兰. 论企业信息化建设中网络安全管理[J].通讯世界,2020,27(02):109-110.