国有企业信息化建设中的安全问题与对策

刘皓然
济南热力集团有限公司　山东　济南　250014

摘　要：互联网技术在不断发展，国有企业的网络安全成为了必须重视的问题，国有企业要想利用互联网提升企业经济发展的速度，就要避免因网络安全问题带来的经济损失。本文主要分析了国有企业网络建设过程中，我国网络安全管理目前的状况，同时对可能会产生的影响因素进行深入研究，找到提升网络安全管理水平的有效策略和防护措施，这对我国经济发展建设有着非常重要的作用。

关键词：国有企业；信息化建设；网络安全管理

引言：国有企业是国家经济发展的重要支柱，信息化建设对于国有企业的发展至关重要。然而，在信息化建设过程中，安全问题成为了一个不容忽视的问题。论文将从国有企业信息化建设中的安全问题入手，探讨相应的对策。

1 国有企业信息化建设的概念和特点

1.1 概念

国有企业信息化建设是指利用信息技术手段，对企业的生产、经营、管理等各个方面进行数字化、智能化改造，以提高企业的竞争力和效率的过程[1]。信息化建设是现代化企业的必经之路，也是国有企业转型升级的重要途径。

1.2 特点

1.2.1 统一规划，分步实施

信息化建设是一项系统性、复杂性、长期性的工程，需要在全局规划下进行。国有企业需要根据自身的发展战略和实际情况，制定详细的信息化建设规划，明确目标和阶段性目标，并制定具体的实施计划和方案。在统一规划下，分步实施，逐步推进信息化建设。

1.2.2 注重实际应用

信息化建设的目的是为了提高企业的运营效率和管理水平，提升企业的竞争力和创新能力。因此，信息化建设必须注重实际应用，以解决实际问题和提高企业的业务能力。企业需要从自身业务和管理流程出发，开展信息化建设，提高信息化应用的水平和效果。

1.2.3 技术先进，兼顾安全

信息化建设需要采用先进的技术手段，以提高工作效率和管理水平。同时，企业也需要注意信息安全问题，保障企业的数据和资产安全。因此，在信息化建设中，需要注重技术选型和安全防范措施，确保信息化建设的质量和可持续性。

1.2.4 团队建设，注重人才培养

信息化建设需要一支专业化、高素质的人才队伍来支持[2]。国有企业需要重视团队建设，注重人才培养和吸引，打造一支具有创新精神和实践能力的信息化人才队伍。同时，企业还需要关注信息化技术的更新换代，及时更新知识和技能，以适应信息化建设的需求和挑战。

1.2.5 管理创新，与业务深度融合

信息化建设是对传统业务流程的数字化改造，需要与业务深度融合，实现业务流程的在线化和智能化。因此，在信息化建设中，需要注重管理创新，探索新的管理模式和方法，以提高企业的管理效率和水平。同时，也需要关注数据驱动的管理方式，通过数据分析和挖掘，实现对业务的精细化管理和优化。

2 国有企业信息化建设的意义

伴随着信息技术的不断建设，国有企业在生产经营、市场营销与信息化建设之间有非常紧密的关系，便捷与风险并存。在信息化系统开发的过程中，因其本身存在安全漏洞，所以使一些非法分子获得机会，也使其安全受到了威胁。信息安全建设首先可以保证个人信息不会出现泄露的情况。对于国企来讲，人力资源管理中信息资料属于非常重要的部分，通过这一方式能够保证这些资料不被泄露，使国有企业的人力资源信息得到保障。其次是能够提高国有企业科技信息共享的有效性。当前国有企业通过搭建共享平台实现信息共享，而通过这一方式能够加强网络系统的安全性，使国有企业的利益不受不良因素的影响。

2.1 提高运营效率和管理水平

信息化技术的应用可以实现企业各个环节的数字化管理，减少中间环节，提高信息传递速度和准确性，提高决策效率和管理水平。比如，利用信息化技术可以实现生产计划的智能化管理，减少生产过程中的浪费和损

失；可以实现物流管理的自动化，提高物流效率和准确性；可以实现财务管理的数字化，减少人工操作误差，提高数据准确性和可靠性。

2.2 提升企业的创新能力和市场适应能力

信息化技术的应用可以促进企业的创新，提高研发能力和技术水平，更好地满足市场需求。比如，利用信息化技术可以实现产品设计的协同和仿真，提高产品设计的效率和质量；可以实现市场调研的自动化，提高市场调研的准确性和全面性；可以实现营销手段的多样化，提高营销效率和精准度。

2.3 提高企业的社会责任感和公共形象

信息化技术的应用可以更好地履行社会责任，提高公共形象，为社会做出更大的贡献[3]。比如，利用信息化技术可以实现环境监测的自动化，提高环境监测的准确性和全面性；可以实现公共服务的在线化，提高公共服务的质量和便捷性；可以实现社会安全防控的智能化，提高社会安全防控的精准度和效率。

2.4 促进企业数字化转型

信息化建设可以促进企业数字化转型，实现业务流程的在线化和智能化。比如，利用信息化技术可以实现供应链的在线化和智能化，提高供应链的响应速度和准确性；可以实现客户关系管理的数字化，提高客户关系管理的质量和效果；可以实现生产制造的智能化，提高生产制造的效率和质量。

3 国有企业信息化建设中的安全问题

3.1 网络安全问题

网络安全问题是国有企业信息化建设中面临的一个重要问题。随着企业信息化程度的不断提高，企业的数据和资产越来越多地集中在网络上，同时也面临着更多的网络安全威胁。

一方面，黑客攻击是企业网络安全面临的最大威胁之一。黑客可以通过各种手段入侵企业的网络系统，窃取企业的机密信息，破坏企业的正常运营，甚至导致企业的数据和资产受到严重损失。另一方面，病毒传播也是企业网络安全面临的一个重要问题。病毒可以通过网络传播到企业的计算机系统中，导致计算机系统崩溃，损害企业的数据和资产。此外，企业在数据传输和存储过程中也存在着安全风险。数据泄露可以通过网络传输导致企业的数据被窃取，影响企业的声誉和形象。

3.2 信息安全管理问题

信息安全管理问题是国有企业信息化建设中必须重视的一个问题。由于缺乏完善的信息安全管理制度和流程，以及缺乏足够的信息安全人员和定期的信息安全测试，很容易导致信息安全问题的发生。

缺乏完善的信息安全管理制度和流程。很多企业在信息安全管理方面存在缺陷，没有建立完善的信息安全管理制度和流程，导致信息安全管理工作不规范、不统一，难以实现全面、系统、规范的管理。这样一来，即使发生了信息安全问题，也难以快速、准确地定位和解决问题。

缺乏足够的信息安全人员。企业在信息安全管理方面的人力资源配备不足，缺乏专业的信息安全人员，无法有效地开展信息安全管理工作。这样一来，即使企业建立了完善的信息安全管理制度和流程，也难以保障其落实和执行。

缺乏定期的信息安全测试。企业没有定期对其信息系统进行全面的测试和评估，不能及时发现和解决潜在的安全问题[4]。这样一来，一旦发生信息安全问题，将会给企业带来不可估量的损失。

3.3 内部人员欺诈问题

内部人员欺诈是国有企业信息化建设中一个越来越突出的问题。随着信息技术的发展和应用，内部人员欺诈的手段也在不断升级和翻新。比如，利用网络漏洞进行攻击、利用内部人员的身份进行诈骗、利用信息化手段进行传销等。这些欺诈行为不仅会给企业带来经济损失，还会影响企业的声誉和形象，给企业带来极大的损失和负面影响。

内部人员欺诈的发生，往往是因为企业内部人员对于信息安全的重视不够、内部管理混乱、员工素质参差不齐等原因所致。因此，加强信息安全管理成为了防范内部人员欺诈的重要措施。

4 对策分析

为了解决上述安全问题，需要从以下几个方面入手：

4.1 加强技术防范措施

国有企业信息化建设中，网络安全问题一直是一个重要的话题。为了保障企业信息的安全，需要采取一系列的技术防范措施。

首先，需要加强网络安全技术研究和应用。网络安全技术包括防火墙、入侵检测系统、反病毒系统、访问控制系统等多种手段，能够识别和处理各种网络安全威胁，从而保障企业网络的安全性。

其次，需要对员工进行网络安全培训。网络安全不仅仅是技术问题，还需要全员参与。企业应该对员工进行网络安全培训，提高员工的网络安全意识和技能，让员工了解网络安全的重要性和必要性，从而形成全员参与的网络安全文化。

第三，需要建立完善的网络安全管理制度。企业应

该建立完善的网络安全管理制度，包括网络安全保障措施、网络安全监控和应急响应机制等内容，确保网络安全问题能够得到及时发现、及时处置。

第四，需要加强信息安全监测和预警。企业应该建立信息安全监测和预警机制，实时监测和分析企业网络安全状况，及时发现和解决网络安全问题[5]。同时，还需要针对不同等级的网络安全事件制定相应的应急预案，确保在发生网络安全事件时能够迅速采取有效措施进行处置。

4.2 加强信息安全管理

随着信息化建设的深入推进，信息安全问题逐渐成为了企业必须面对的重要问题。国有企业需要加强信息安全管理，确保企业信息化建设过程中各类资产和数据的安全性。

首先，需要建立完善的信息安全管理制度和流程。信息安全管理制度应该包括信息安全管理的目标、职责、流程、标准等内容，确保信息安全管理工作能够得到全面、系统、规范的管理。同时，还需要建立信息安全管理的监督和评估机制，定期对信息安全管理工作进行检查和评估，及时发现和解决存在的问题。

其次，需要加强信息安全人员的培训和管理。信息安全人员是保障企业信息安全的关键，需要企业加强信息安全人员的培训和管理工作，提高信息安全人员的专业水平和职业道德。企业可以引进和培养信息安全人才，同时也需要对现有的信息安全人员进行定期的培训和考核，确保他们能够跟上技术的发展和企业的需求。

第三，需要加强信息安全技术的应用和管理。信息安全技术是保障企业信息安全的重要手段，需要加强信息安全技术的应用和管理工作。企业应该根据不同的安全威胁和风险等级，采取不同的技术手段和防范措施，确保企业信息系统的安全性。同时，还需要对新技术和新应用进行评估和测试，确保其安全性和可靠性。

第四，需要加强信息安全教育和宣传。信息安全教育和宣传是提高企业员工信息安全意识和技能的重要途径，需要企业加强信息安全教育和宣传工作，提高员工的信息安全意识和风险意识，让员工了解网络安全的重要性和必要性，从而形成全员参与的信息安全文化。

4.3 加强内部人员管理

国有企业信息化建设中，内部人员欺诈是一个比较常见的问题[6]。内部人员欺诈不仅会给企业带来经济损失，还会影响到企业的声誉和形象，因此必须加强内部人员管理，防范和杜绝内部人员欺诈的发生。

首先，需要建立完善的员工管理制度。企业应该明确员工的权责和操作规范，建立完善的员工档案，记录员工的职务、工作经历、培训情况、违规行为等信息，以便于进行管理和监督。同时，还应该加强对员工的培训和教育，提高员工的信息安全意识和能力，让员工了解企业的信息安全政策和规定，自觉遵守信息安全规范。

其次，需要加强对员工的监督和审查。企业应该建立监督机制，对员工的行为进行监督和审查，及时发现和纠正员工的不当行为。对于发现的不当行为，应该严格按照制度和流程进行处理，涉及到违法犯罪的行为应该及时向公安机关报案，追究其法律责任。

第三，需要加强对员工的背景调查和审核。企业在招聘员工时，应该对应聘者进行背景调查和审核，了解其教育背景、工作经历、职业资格等信息，确保其符合招聘要求和企业信息安全管理的需要。同时，在员工入职后，也应该定期对其进行背景调查和审核，及时发现和解决员工在职期间存在的问题和风险。

第四，需要加强对员工的道德教育和引导。企业应该加强对员工的道德教育和引导，提高员工的道德素质和职业操守，让员工能够自觉遵守企业的信息安全规定和政策，避免因为个人原因造成企业信息安全问题的发生。

结语

国有企业信息化建设中的安全问题是一个复杂而又普遍存在的问题。要解决这些问题，需要从技术防范、信息安全管理、内部人员管理等多个方面入手。只有采取全面、综合性的措施，才能真正提高企业信息化建设的安全水平。

参考文献

[1]何玉谶，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（2）：109-110.

[2]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.

[3]沈素忠.大数据背景下A公司管理信息集成化的实践研究[D].桂林：桂林理工大学，2020.

[4]丘涛.智慧工地建设的数据信息协同管理研究[D].广州：华南理工大学，2019.

[5]姜鹤.基于企业信息化建设的网络安全管理问题研究[J].企业改革与管理，2020（15）：76-78.

[6]兰洋，黄天，梅飞.国有企业信息化建设中的网络安全问题探究[J].现代工业经济和信息化，2019，9（12）：78-79.