信息安全管理促进企业数字技术创新研究

李述卫
（南京领行科技股份有限公司，江苏 南京 211100）

摘要：随着数字经济的蓬勃发展，企业纷纷投入大量资源进行数字技术创新，以期在激烈的市场竞争中占据有利地位。然而，数字技术创新过程中面临的信息安全问题不仅威胁了企业的核心资产，还可能阻碍技术创新进程。因此，如何通过有效的信息安全管理促进企业数字技术创新成为当前亟待解决的问题。基于此，本文首先对信息安全管理进行了概述，明确了信息安全管理的重要性。接着，分析了信息安全管理的特征和信息安全管理对企业数字技术创新的作用机制，通过对企业数字技术创新过程中的信息安全风险探究，提出了几点建设性的建议，旨在促进企业的健康发展。

关键词：信息安全管理；企业；数字技术创新

一、信息安全管理促进企业数字技术创新理论分析

（一）信息安全管理的概述

信息安全管理是一种系统的方法，旨在保护企业的信息资产免受各种威胁，确保信息的可用性、完整性和保密性。随着信息技术的快速发展，企业对信息安全的依赖日益增加，信息安全成为企业可持续发展的重要保障。对此，信息安全管理不仅涵盖了技术层面的防护措施，如防火墙、入侵检测系统、数据加密等，还涉及管理层面的策略、流程和标准。通过制定并实施一系列信息安全政策，企业能够有效识别、评估和控制潜在的风险，从而减少信息泄露、数据损坏和业务中断的可能性，保障企业的稳定运行。

（二）信息安全管理的特征

信息安全管理的特征主要体现在其系统性、持续性、技术性和人文性等方面。系统性是指信息安全管理体系是一个涵盖企业所有部门和业务流程的全面系统，需要从整体上考虑信息资产的安全问题，确保信息的完整性、可用性和保密性。持续性则强调信息安全管理工作是一个持续改进、不断优化的过程。随着信息技术的快速发展和信息安全威胁的日益复杂，企业必须不断更新其安全策略和技术手段，以应对新的挑战。技术性是指信息安全管理工作需要依赖先进的技术手段，包括防火墙、入侵检测系统、数据加密技术等，这些技术手段可以有效防止外部攻击和内部泄露，保护企业信息资产的安全。人文性则强调信息安全管理工作不仅仅是技术问题，更是一个管理问题，它需要关注人的因素，提高员工的信息安全意识，建立良好的信息安全文化，确保信息安全政策得到有效执行。

（三）信息安全管理的重难点

首先，企业在实施信息安全管理时，往往需要采取一系列严格的控制措施，如访问控制、数据加密等，虽然能够提高信息的安全性，但同时也可能增加企业的运营成本，降低业务处理效率。因此，如何在保障信息安全和提高业务效率之间找到平衡点，是企业需要重点考虑的问题。其次，随着信息技术的发展，新的安全威胁不断出现，如新型病毒、网络钓鱼、高级持续性威胁等，具有较强的隐蔽性和破坏性，给企业的信息安全带来了极大的风险。因此，企业需要建立一套快速响应机制，及时发现和处理安全事件，减少安全威胁对企业的影响。最后，由于缺乏必要的培训和教育，许多员工的信息安全意识较为薄弱，容易成为安全漏洞。因此，企业需要加强信息安全培训，提高员工的信息安全意识，使他们能够自觉遵守信息安全政策，共同维护企业的信息安全。总而言之，信息安全管理的重难点不仅在于技术层面，更在于管理层面，企业需要整体考虑信息安全问题，建立一套科学、合理、有效的信息安全管理体系。

（四）信息安全管理与企业数字技术创新

1. 信息安全管理对企业数字技术创新作用机制

首先，通过建立健全的信息安全管理体系，企业可以有效防范风险，为技术研发团队提供一个稳定的工作环境，更加专注于数字技术创新本身。其次，良好的信息安全管理实践有助于提升企业内部的信息流通效率。通过实施严格的信息安全政策，企业可以确保对敏感信息的适当保护，同时通过合理的信息权限管理，促进非敏感信息在团队间的快速传递，从而加快项目进度，提高创新效率。再者，在当今高度互联的商业环境中，企业往往需要与其他公司、研究机构等外部实体合作，共同推进技术创新。此外，随着消费者对个人信息保护意识的提高，越来越多的人开始倾向于选择那些能够提供更好数据安全保障的产品和服务。因此，企业通过加强信息安全管理，不仅可以保护自身免受潜在的法律风险，还能够在激烈的市场竞争中脱颖而出，吸引更多的客户，为技术创新成果的商业化应用奠定坚实的基础。

2. 数字技术创新的表现

在技术层面上，数字技术创新主要体现在信息技术的更新换代与深度融合。通过人工智能技术，企业可以实现智能化生产和服务，提高生产效率，降低运营成本；通过区块链技术，企业可以构建更加安全透明的供应链体系，提高供应链管理效率，增强企业竞争力。

在业务层面上，数字技术创新主要体现在企业业务模式的创新和优化。数字技术的应用使得企业可以打破传统业务模式的局限，实现业务流程的数字化转型。例如，通过电子商务平台，企业可以实现线上销售，扩大市场覆盖面，提高销售效率；通过在线支付系统，企业可以提供更加便捷的支付方式，提高客户体验。

在组织层面上，数字技术创新主要体现在企业组织结构的优化和管理方式的创新。企业通过构建更加扁平化的组织结构，能够实现信息的高效流通和资源共享，提高企业的决策效率和执行力。例如，通过企业资源规划（ERP）系统，企业可以实现各部门之间的信息共享，提高协作效率。

二、企业数字技术创新的信息风险探究

（一）企业信息安全管理的最新风险

首先，网络攻击技术的不断进化是企业面临的主要风险之一。黑客利用先进的技术手段，如人工智能和机器学习，开发出更加隐蔽和高效的攻击工具。例如，勒索软件攻击、零日漏洞利用等新型攻击方式，能够绕过现有的安全防御系统，给企业带来严重的经济损失和声誉损害。其次，数据泄露是另一个不容忽视的风险来源。随着企业数字化转型的加速，大量的敏感数据被存储在云端或企业内部网络中，一旦泄露，不仅可能导致客户信息的泄露，还可能暴露企业的核心技术和商业秘密，严重影响企业的竞争力。

再者，供应链攻击成为企业信息安全的新威胁。供应链攻击是指攻击者通过攻击企业的合作伙伴、供应商等第三方，进而渗透到目标企业的网络中。这种攻击方式隐蔽性强，难以被发现，一旦成功，往往能够获取到企业的敏感信息，甚至控制企业的关键系统。随着企业间合作的加深，供应链攻击的风险也在不断增加，企业需要加强对合作伙伴的安全审核，确保供应链的安全性。

（二）信息风险特点

首先，企业数字技术创新的信息风险具有高度的不确定性。在数字技术快速发展的背景下，新的信息安全威胁层出不穷，企业难以准确预测未来的安全风险，这使得企业在制定信息安全策略时面临巨大的未知挑战，企业必须保持高度的警觉性和灵活性，及时调整安全措施，以应对不断变化的威胁环境。

其次，企业数字技术创新的信息风险具有扩散性。在信息化、网络化的企业运营环境中，信息的流动速度极快，一旦发生信息安全事件，其影响范围往往会迅速扩大，不仅波及企业内部的各个部门，还可能对供应链上下游的合作伙伴、客户乃至整个行业造成影响。

再者，企业数字技术创新的信息风险具有隐蔽性和潜伏性。许多信息安全威胁在初期往往难以被发现，如内部人员的不当操作、恶意软件的潜伏等，这些风险可能在一段时间内不会对企业造成直接损害，然而一旦触发，破坏力极大。因此，企业需要建立完善的风险预警机制，通过定期的安全审计、漏洞扫描等手段，及时发现潜在的安全隐患，采取措施加以防范。

最后，企业数字技术创新的信息风险具有连锁反应性。在企业数字化转型过程中，各项业务高度依赖信息系统，一旦某一环节出现安全问题，可能会引发连锁反应，影响整个业务流程的正常运行。例如，数据泄露可能导致客户信任度下降，进而影响企业的市场竞争力。因此，企业在进行数字技术创新时，应充分考虑信息安全因素，建立全面的风险管理体系，确保在面对安全事件时能够迅速响应，减少损失，维护企业的正常运营。

三、信息安全管理促进企业数字技术创新路径研究

（一）建立健全企业信息安全管理体系

首先，企业需要构建一个全面的信息安全政策框架，明确信息安全的目标、标准和程序，为企业的信息安全管理工作提供明确的规范指导。信息安全政策应当覆盖企业运营的所有方面，包括数据管理、网络管理、物理安全、人力资源管理等，确保企业在各个层面上都能有效识别和管理信息安全风险。其次，企业应当清晰信息安全管理组织结构，明确各层级的职责与权限，确保信息安全政策的有效执行。信息安全管理部门应当由具备专业技能和丰富经验的人员组成，负责制定和更新信息安全策略，监督信息安全政策的执行情况，以及对信息安全事件进行响应。同时，企业还应建立跨部门的信息安全协调机制，确保各部门在信息安全管理工作中的协作与配合，形成合力，共同应对信息安全挑战。再者，企业还应定期进行信息安全风险评估，及时发现潜在的安全威胁，采取有效措施加以防范。信息安全风险评估应当覆盖企业的所有业务流程，识别出可能存在的信息安全风险点，评估这些风险对企业的潜在影响，从而制定相应的风险应对策略。此外，企业还应建立信息安全事件报告和处理机制，确保一旦发生信息安全事件，能够迅速响应，减少企业实际损失，尽快恢复业务运营。

（二）强化企业员工信息安全管理意识

员工是企业信息安全的第一道防线，他们的行为直接影响到企业信息系统的安全状况，提高员工的信息安全意识，不仅能够有效预防信息安全事故的发生，还能够促进企业在数字技术领域的创新。

首先，企业应对员工进行信息安全培训，内容涵盖最新的信息安全威胁、法律法规要求、企业内部的信息安全政策等，采用多样化的形式，如在线课程、现场讲座、案例分析，以提高培训的吸引力和实效性。通过培训，员工可以及时了解信息安全领域的最新动态，掌握必要的信息安全知识和技能，提高应对信息安全威胁的能力。其次，企业需要建立一套完善的信息安全激励机制，鼓励员工主动参与到信息安全工作中来。例如，可以设立信息安全优秀个人或团队奖项，对在信息安全方面表现突出的员工给予奖励。同时，对于违反信息安全规定的行为，企业也应有明确的处罚措施，以此来强化员工遵守信息安全规定的意识。通过正向激励与负向惩罚相结合的方式，可以有效提升员工的信息安全责任感。最后，企业应当注重培养员工的创新思维，鼓励他们在日常工作中发现潜在的信息安全问题，探索新的信息安全解决方案。通过激发员工的创造力，不仅可以提高企业的信息安全水平，还能够推动企业在数字技术领域的持续创新。

（三）提高企业信息安全管理智能水平

在当今信息化时代，智能信息安全管理通过运用先进的信息技术手段，可以实现对企业信息资产的全面、动态、智能保护，从而为企业创造一个安全、可靠的信息环境，促进技术创新的持续发展。

首先，利用人工智能技术，可以实现对网络威胁的智能感知与响应。通过机器学习算法，企业能够自动识别和预测潜在的安全威胁，及时采取措施进行防御，减少安全事件的发生。例如，基于深度学习的入侵检测系统，能够通过分析网络流量模式，自动识别异常行为，提前预警，有效防止恶意攻击。其次，大数据分析技术的应用，为信息安全管理提供了新的视角。通过对海量数据的分析，企业可以更准确地了解自身的安全状况，发现潜在的风险点。大数据分析不仅能够帮助企业识别已知威胁，它还能够帮助企业发现未知的威胁，实现对安全风险的预判。例如，通过分析员工的网络访问记录，发现异常的访问模式，及时采取措施，防止数据泄露。再者，云安全服务能够为企业提供全方位的安全保障，包括数据加密、访问控制、安全监控等。企业无需自建安全设施，即可享受到专业的安全服务，降低了信息安全管理的成本，提高了效率。此外，云平台的弹性特性，使得企业能够根据业务需求，灵活调整安全资源配置，确保在不同业务场景下，都能获得最佳的安全保护。

四、结束语

综上所述，本文通过理论分析和实证研究，揭示了信息安全管理在促进企业数字技术创新中的重要作用，为企业在数字时代实现可持续发展提供了参考和借鉴。未来研究可进一步探索不同类型企业在信息安全管理方面的差异性及其对数字技术创新的影响，为更多企业提供个性化的信息安全管理方案。

参考文献：

[1] 彭雪晴 . 数字金融推动企业数字化转型 [J]. 大众投资指南，2024（16）：54-56.

[2] 张云，尹艺霏 . 数字化转型、公司治理模式与企业全要素生产率 [J]. 郑州大学学报（哲学社会科学版），2023，56（5）：53-58.

[3] 谢康，胡杨颂，刘意，罗婷予 . 数据要素驱动企业高质量数字化转型——索菲亚智能制造纵向案例研究 [J]. 管理评论，2023（2）：328-339.

[4] 韩冬梅，马圣楠，刘建梅 . 数字化与企业内部控制质量 [J]. 中国审计评论，2023（2）：79-110.

[5] 黄勃，李海彤，刘俊歧，雷敬华 . 数字技术创新与中国企业高质量发展——来自企业数字专利的证据 [J]. 经济研究，2023（4）：97-115.