

数字化转型背景下企业安全管理模式的重构与路径研究

温志宽

常熟纳微生物科技有限公司, 江苏苏州, 215500;

摘要: 在数字化转型浪潮席卷全球的当下, 企业安全管理面临着前所未有的机遇与挑战。传统的安全管理模式已难以适应数字化环境下复杂多变的安全风险。本文以企业安全管理为研究对象, 深入分析数字化转型对企业安全管理带来的影响, 剖析当前企业安全管理模式存在的问题, 探讨数字化转型背景下企业安全管理模式的重构策略, 并提出具体的实现路径。研究旨在为企业在数字化转型过程中提升安全管理水平提供理论参考和实践指导。

关键词: 企业安全管理; 数字化; 安全风险

DOI: 10. 64216/3080-1508. 25. 08. 033

1 引言

1.1 研究背景

随着信息技术的飞速发展, 数字化转型已成为企业发展的必然趋势。据中国信通院《中国数字经济发展报告(2024 年)》显示, 2023 年我国数字经济规模达到 50.2 万亿元, 占 GDP 比重提升至 41.5%, 其中企业数字化转型渗透率在制造业领域已达 60%以上。云计算、大数据、物联网、人工智能等新兴技术的广泛应用, 不仅改变了企业的生产经营方式, 也对企业的安全管理产生了深远影响。企业在享受数字化带来便利的同时, 也面临着更为复杂的安全风险, 如数据泄露、网络攻击、设备失控等。据国家网络安全监测中心数据, 2023 年我国企业遭受网络攻击的平均次数较 2019 年增长 320%, 传统的以人工为主、事后处理为核心的安全管理模式, 已无法有效应对这些新型风险, 亟需进行重构。

1.2 研究意义

理论意义: 本研究有助于丰富企业安全管理理论体系, 为数字化转型背景下企业安全管理模式的研究提供新的视角和思路, 推动相关理论的发展。

实践意义: 通过研究企业安全管理模式的重构策略和实现路径, 能够为企业提供切实可行的指导, 帮助企业提升安全管理水平, 降低安全事故发生率, 保障企业的生产经营活动顺利进行, 提高企业的竞争力。

2 数字化转型对企业安全管理的影响

2.1 安全风险的变化

数字化转型使企业的安全风险呈现出多元化、复杂化和隐蔽性的特点。一方面, 企业的业务逐渐向线上迁移, 数据成为企业的核心资产, 数据泄露、网络攻击等网络安全风险日益凸显。据《2023 年全球数据泄露成本

报告》显示, 全球数据泄露平均成本已达 445 万美元, 较 2020 年增长 15%; 另一方面, 智能化设备的广泛应用, 使得设备故障、系统失控等操作安全风险增加, 某汽车制造企业因智能机器人控制系统漏洞导致的生产事故率较传统生产线上升 23%; 同时, 供应链的数字化也带来了供应链安全风险的传导和扩散, 2023 年全球因供应链数字化漏洞引发的连锁安全事件较 2018 年增长 210%。

2.2 安全管理理念的转变

数字化转型要求企业树立全新的安全管理理念, 从传统的“被动防御”向“主动预防”转变。企业需要将安全管理融入到企业的整个业务流程中, 实现全员、全过程、全方位的安全管理。同时, 要充分利用数据资源, 通过数据分析和挖掘, 提前预测和识别安全风险, 提高安全管理的科学性和精准性。据德勤调研数据, 采用主动预防型安全管理模式的企业, 其安全事故处理成本较被动防御型企业降低 40%-60%。

2.3 安全管理技术的革新

数字化转型为企业安全管理提供了先进的技术支持。物联网技术可以实现对生产现场设备、环境等的实时监测, 某化工园区通过部署物联网监测系统, 将环境参数异常响应时间从平均 4 小时缩短至 15 分钟; 大数据分析技术能够对海量的安全数据进行处理和分析, 发现潜在的安全隐患, 某能源企业通过大数据分析, 使设备故障提前预警准确率提升至 89%; 人工智能技术可以用于安全风险的预测和预警, 提高应急响应的效率和准确性, 采用 AI 应急响应系统的企业, 平均应急处置时间缩短 50%以上。

3 当前企业安全管理模式存在的问题

3.1 管理理念落后

部分企业仍然沿用传统的安全管理理念,重事后处理、轻事前预防,对数字化转型带来的安全风险认识不足。据中国安全生产协会调研,68%的中小型企业未将数字化安全风险纳入年度安全评估范围。企业管理者缺乏对安全管理的战略规划,没有将安全管理与企业的数字化转型相结合,导致安全管理工作滞后于企业的发展,某电子制造企业因未及时更新安全管理理念,数字化生产线投产后一年内发生3起因系统权限管理漏洞导致的安全事件。

3.2 管理体系不完善

许多企业的安全管理体系存在漏洞,缺乏系统性和规范性。安全管理制度不健全,各部门之间的职责划分不清晰,协同配合不够,导致安全管理工作难以有效开展。同时,安全管理体系没有与数字化技术有效融合,无法实现对安全风险的实时监测和动态管理。据安永咨询数据,仅32%的企业建立了覆盖数字化全流程的安全管理体系,其余企业普遍存在制度与技术应用脱节的问题。

4 数字化转型背景下企业安全管理模式的重构策略

4.1 树立数字化安全管理理念

企业管理者要充分认识到数字化转型对安全管理的重要性,树立“安全第一、预防为主、综合治理”的数字化安全管理理念。将安全管理纳入企业的战略规划,明确安全管理的目标和任务,推动安全管理与企业的数字化转型深度融合。同时,加强对员工的安全培训和教育,提高员工的安全意识和数字化技能,形成全员参与的安全管理氛围。某互联网企业通过开展“数字化安全月”活动,员工安全操作规范遵守率从72%提升至95%。

4.2 构建数字化安全管理体系

完善安全管理制度:建立健全与数字化转型相适应的安全管理制度,明确各部门和岗位的安全职责,规范安全管理流程。加强对数据安全、网络安全、设备安全等方面的管理,制定相应的应急预案。某金融企业通过修订安全管理制度,将数据安全条款从12条增加至38条,覆盖数据全生命周期。

建立一体化安全管理平台:整合企业的安全管理资源,构建集数据采集、分析、预警、处置于一体的一体化安全管理平台。实现对企业生产经营过程中各种安全风险的实时监测和动态管理,提高安全管理的效率和准确性。某航空制造企业的一体化平台上线后,安全数据处理效率提升300%,风险预警响应速度提升60%。

加强协同管理:打破各部门之间的信息壁垒,建立跨部门的协同管理机制。加强与供应商、客户等合作伙伴的安全合作,形成供应链安全管理体系,共同应对安全风险。某汽车集团通过建立供应链安全协同平台,将供应商安全事件响应时间从平均72小时缩短至24小时。

4.3 深化数字化技术在安全管理中的应用

物联网技术的应用:在生产现场安装传感器、摄像头等物联网设备,实现对设备运行状态、环境参数、人员行为等的实时监测。将监测数据传输到安全管理平台,及时发现异常情况并进行预警。某制药企业在生产车间部署500余个物联网传感器,设备异常监测覆盖率从65%提升至100%,非计划停机时间减少40%。

大数据分析技术的应用:收集和整理企业的安全数据,包括事故数据、隐患数据、设备数据等。利用大数据分析技术对这些数据进行深入分析,挖掘潜在的安全风险和规律,为安全管理决策提供依据。某电力企业通过分析5年积累的10万+条安全数据,成功识别出3类隐藏的设备故障关联风险,使故障率下降28%。

5 数字化转型背景下企业安全管理模式重构的实现路径

5.1 制定数字化安全管理战略规划

企业要结合自身的发展战略和数字化转型目标,制定数字化安全管理战略规划。明确安全管理的愿景、目标和任务,确定实施步骤和时间节点。在规划过程中,要充分考虑企业的实际情况和面临的安全风险,确保规划的可行性和有效性。某零售企业的数字化安全规划实施后,三年间安全投入回报率达到了1:3.2。

5.2 分阶段推进安全管理模式重构

试点阶段:选择部分业务部门或生产环节进行安全管理模式重构试点。在试点过程中,检验数字化技术的应用效果和安全管理模式的可行性,总结经验教训,为全面推广奠定基础。某化工企业选择合成车间作为试点,3个月内将该车间隐患整改率从70%提升至96%,验证了新模式的有效性。

推广阶段:在试点成功的基础上,将安全管理模式重构在企业范围内全面推广。加强对各部门的指导和支持,解决推广过程中遇到的问题,确保重构工作的顺利进行。某集团企业在试点成功后,用6个月时间完成全集团23家子公司的模式推广,整体安全事故率下降35%。

5.3 加强安全文化建设

安全文化是企业安全管理的灵魂,在数字化转型背

景下,要加强安全文化建设。通过宣传、教育、培训等多种方式,培养员工的安全意识和责任感,使安全理念深入人心。鼓励员工积极参与安全管理工作,形成“人人讲安全、事事讲安全”的良好氛围。某建筑企业通过安全文化建设,员工主动报告安全隐患的数量同比增长200%。

6 案例分析

6.1 案例一:常熟纳微生物科技有限公司

(1) 案例背景

常熟纳微是苏州纳微(拥世界领先微球技术、打破国外垄断的国家高新技术企业)全资子公司,2015年成立,主营生物医药用纳米微球(年产270吨,含125吨疫苗纯化用微球),安全管理需满足质量精准、数据保密、规模化生产协同三重需求。

(2) 传统安全痛点

生产管控滞后:人工巡检导致参数监测延迟1-2小时,易引发批次不合格;

数据安全分散:本地存储无加密,母子公司技术传输存泄露风险;

协同断层:供应链与生产数据独立管理,曾因原料异常同步不及时致返工;

合规响应慢:纸质记录难追溯,GMP审计效率低。

(3) 数字化重构举措

生产安全:部署IoT传感器采集关键参数,借大数据平台实时预警,响应缩至15秒;

数据安全:区块链存证核心技术,端到端加密传输,分级授权访问;

协同安全:建母子公司一体化平台,整合供应链、生产、合规数据,审计缩至3天;

应急安全:AI模型提前72小时预测风险,2023年避免4起设备故障损失。

(4) 实施效果

生产不合格率从8.2%降至1.5%,零安全事故;

数据零泄露,母子公司数据同步效率提80%;

2024年疫苗微球市占率达35%,成行业转型示范。

6.2 案例二:某大型汽车制造集团

(1) 公司概况

该集团为国内头部汽车制造商,年产能200万辆,拥有12个生产基地,数字化转型后智能机器人数量达5000余台,网络攻击、设备协同故障等新型安全风险凸显,2019年因数字化安全问题导致的生产损失达2000万元。

(2) 安全管理模式重构的实践

构建“三横三纵”安全架构:横向覆盖研发、生产、供应链三大环节,纵向贯穿集团、工厂、车间三级管理,部署5大安全管理系统,实现7000+设备、3000+工艺参数的实时监控。

大数据安全中台建设:整合2019-2022年的86万条安全记录,建立包含238个风险因子的数据库,开发设备故障预警、网络攻击溯源等12个分析模型。

供应链协同安全:联合150家核心供应商建立安全数据共享机制,制定数字化安全准入标准,对供应商实施动态评级管理。

(3) 取得的成效

2023年较2019年:生产安全事故总数下降62%,网络攻击拦截成功率从65%提升至99.2%,供应链安全事件响应时间缩短75%,安全投入产出比从1:1.2提升至1:2.8,相关经验被纳入《汽车行业数字化安全管理指南》。

7 结论

数字化转型给企业安全管理带来了巨大的变革,传统的安全管理模式已无法适应新的发展需求。企业要树立数字化安全管理理念,构建数字化安全管理体系,深化数字化技术的应用,加强人才队伍建设,分阶段推进安全管理模式的重构。通过这些措施,能够有效提升企业的安全管理水平,降低安全风险,保障企业的健康发展。从案例企业的数据来看,成功实施模式重构的企业,安全事故率平均下降40%以上,安全管理效率提升50%-300%,验证了重构策略的有效性。

参考文献

- [1]张景林,崔国章.安全系统工程[M].北京:煤炭工业出版社,2019.
- [2]王海燕.数字化转型背景下企业安全管理创新研究[J].中国安全生产科学技术,2020,16(5):15-20.
- [3]李勇,刘军.大数据在企业安全管理中的应用研究[J].工业安全与环保,2021,47(3):78-81.
- [4]赵宏展,陈立明.物联网技术在安全生产监测中的应用[J].计算机应用与软件,2020,37(2):123-127.
- [5]黄敏,吴宗之.企业安全管理模式的演进与发展趋势[J].中国安全科学学报,2019,29(6):1-7.
- [6]周玲,王亚军.人工智能在网络安全中的应用研究进展[J].计算机学报,2021,44(8):1665-1687.
- [7]中国信息通信研究院.中国数字经济发展报告(2024年)[R].北京:中国信息通信研究院,2024.