石油企业数字化转型中的网络安全保障措施研究

黄锴恒

（中海油信息科技有限公司湛江分公司，广东 湛江 524000）

摘 要 数字化转型战略为石油企业发展带来了核心驱动力，石油企业数字化转型可以实现业务流程优化，提升业务组织能力。在此背景下，石油企业应注意防治网络安全问题，应对可能发生的各种威胁，防止新型网络攻击手段侵害。现有的网络空间具有开放性特征，网络安全威胁类型也极其复杂，石油企业如何在数字化转型过程中建立安全保障措施成为重点问题，这一问题也限制了石油企业的持续发展。为推进石油企业数字化转型，探索网络安全隐患应对措施，形成完善的保障体系。本文以实践发展为背景，针对石油企业数字化转型中网络安全保障措施进行深入研究，并提出相应的完善建议。

关键词 石油企业；数字化转型；网络安全保障

中图分类号：TP393.08 **文献标识码**：A **文章编号**：2097-3365(2024)04-0025-03

信息安全不仅关系到企业的安全，也对国家的安全有间接的影响。石油企业的信息化建设是必然趋势。随着市场竞争逐渐加剧，石油企业发展中出现了不可控因素，作为国有经济不可缺少的重要内容，石油企业需要全面拥抱数字技术，在数字化转型发展中找到强大动力，有效提升组织管理能力。石油企业数字化转型需要将云计算、大数据和人工智能等技术有机地融合，以解决石油企业发展过程中面临的难题[1]。与此同时，将数字化转型工作与相关业务紧密相连，避免安全风险的出现，应对出现的新型挑战。简言之，石油企业安在全生产部署与数字化转型工作中，需要形成标准化网络安全保障规划，解决智能技术应用遇到的问题，为石油企业稳定发展提供保障。

1 石油企业数字化转型现状

在石油企业发展中，面临着市场竞争与科研任务的双重压力。随着石油企业的稳定发展，智能化转型得到了重视，发展方向逐渐拓展至数字盆地、数字建井以及数字油田等领域。在具体业务部署过程中，需要充分考虑现存信息安全风险。为构建多样化数字发展系统，应对系统风险进行充分考虑。通过建设网络信息安全系统，建立风险防控平台。从石油行业整体角度来看，网络安全依然无法得到保障。在石油企业网络转型的初始阶段，虽然部署了防火墙和防病毒系统，也会针对数据问题进行检测。但随着黑客入侵手段更新、升级，仅靠传统设备进行预防，很难保证系统不受入侵。不难看出，石油企业数字化转型工作开展中，网络安全保障应置于首位。随着石油企业发展规划同步更新，全面落实同步使用原则，形成安全保障策略，保证系统处于稳定运行状态[2]。

在物质经济持续发展的背景下，石油行业经济高速增长，逐渐成为国民经济的支柱产业。但是在数字化转型过程中，依然遭遇诸多不确定因素，很难达到预期的工作效果。石油行业需要关注5G技术、互联网技术、大数据技术以及云计算技术等，对生产业务流程进行赋能，提升市场核心竞争力以及业务表现。在网络安全风险预防方面，需要立足于石油企业网络转型的难点，实现精准化安全防护，保证系统处于平衡状态，发挥出基础保障策略的核心意义。总而言之，为提升发展动力，满足可持续发展要求，石油企业依然需要寻找数字化转型的重点。

2 石油企业数字化转型中网络安全存在的问题

2.1 内网存在一定的安全风险

在石油公司的发展中，不仅存在着网络边境的安全保护问题，同样也存在内部网络监控系统不完善的问题，直接导致内部网络的丢失、信息侵犯、间谍和黑客的出现。在信息化时代，随着数字货币的出现，大量犯罪分子企图利用互联网获利。为谋取更大利益，犯罪分子以病毒为手段，突破石油公司的网络安全屏障，损害网络数据。对此，石油公司只有建立健全的监控机制，才能有效地遏制非法侵入。一般情况下，

石油企业受到的病毒入侵主要是恶意软件和u盘病毒，若是系统不慎感染病毒，且并未得到及时升级与更新，则无法解决病毒带来的隐患[3]，甚至部分网络病毒会在系统中扩散，对服务器造成严重负面影响。实践调查可知，在现有的市场环境中，至少有23%的企业曾遭遇恶意软件威胁，导致这一问题出现的主要原因为软硬件漏洞以及员工失职等。

2.2 未有效管控运行维护机制

石油企业为了满足基本业务要求，往往会将发展重点放在业务系统方面。数字化转型的实施，使企业信息系统中网络设备数量剧增。对各个工作部门来讲，必须要了解不同信息系统的运行逻辑及操作方法，还要处理繁多的账号。一旦出现工作失误，则会造成无法挽回的损失。另外，石油企业还涉及职工离职以及岗位变更等情况，由于无法彻底删除、核销离职人员账号，导致账号多人共享的情况普遍存在。从实践角度来看，过多主体使用相同的账号，不仅容易产生安全事故，也容易出现主体核实难的问题。另外，一旦从业人员出现意外操作和违规操作等行为，如误删企业重要的财务数据、经营数据，则无法顺利找回数据，由此造成的经济损失很难挽回。事实上，在日常工作中，由于缺少完善的管控机制，在系统运维管理过程中耗费过多的时间，同时也无法解决黑客攻击带来的影响。

2.3 行业信息化标准体系滞后

在石油行业发展中，数字化转型时间相对较短，信息技术管理标准不健全。一方面，对于部分从业人员来讲，无法清楚认识系统管理的重要性，容易在信息化标准体系建设中造成不可挽回的损失。因此，行业信息化标准体系的建设，需要在系统实践运行中总结经验。另一方面，由于体系建设和云计算大数据融合深度不足、实践工作框架不清晰和适用范围狭窄等问题，导致石油企业信息技术迭代效率及工作标准无法满足需求，削弱了对信息系统的监督与管理能力，无法发挥出数字化转型的引领作用[4]。

2.4 员工网络安全意识较薄弱

石油企业在数字化转型工作开展时，需要将信息技术应用于各个工作环节中，由于新技术、新手段更新速度较快，暴露了从业人员潜在的认知问题，如重建设轻安全等观念，导致网络环境管理体系无法形成标准流程。

为实现安全管理的目标，解决网络安全出现的隐患，需要制定全新的发展模式。但由于石油企业员工相对较多，从业人员安全意识参差不齐，部分员工由于综合素质不足，导致安全管理体系不稳定，常出现数据缺失、系统被盗等问题。例如，使用不安全风险文件、弱口令以及将信息共享网盘等，此类现象均会造成无法挽回的损失。石油企业网络安全处理中，需要了解网络安全的等级，培养高素质网络安全管理人员，避免从业者综合素质不足的情况出现。

3 石油企业数字化转型中的网络安全保障措施

在实现石油工业向数字化过渡过程中，要重点解决的问题就是信息安全。信息网络是开放性结构，在综合运用多种高科技时，必须要针对石油企业的特定业务，对出现的安全问题进行及时处理，保证各项业务稳定开展。在网络空间中数据互相交织，为病毒传播提供了良好媒介，导致网络安全管理难度相对较高，对于石油企业来讲，需要在数字化转型中全面应用网络安全防护机制，具体的工作方案如下。

3.1 严密监测内部网络安全性

在石油企业数字化转型工作中，为了达到网络安全防护的理想目标，需要在网络出口部署安全防护设备，通过入侵检测等技术，将风险降到最低。无论采用任何防风险入侵系统，都需对系统进行定期升级，增加对各类型病毒的防范能力。

首先，在网络安全保障体系应用中，需要以系统正常运行为基础，合理部署应用防火墙，通过脚本检查和过滤等方式，对受到的攻击进行破坏。在外部链接检查工作中，需要配合完善的访问控制策略，对敏感信息和词汇进行过滤，保证网络系统持续运行。

其次，在服务器升级管理过程中，也需逐渐提升安全防护能力，预防外部网络风险的产生[5]。在内部网络环境监控管理时，则需要逐渐加强监控力度，对于安全风险提前预防，达到各项业务开展的基本要求。

最后，在内部服务器管理过程中，需要了解数据实践交互状态，排查潜在的安全威胁，将系统检测技术的作用最大化。在解析网络安全隐患时，需要将恶意攻击置于首位，通过全方位部署，达到理想化预警功能。对石油企业来讲，在开展数字化转型工作时，为规避信息风险问题，需要及时更新检测系统，及时发现系统存在的漏洞，防御高级攻击手段。在提升网络安全监测能力的同时，安全防护能力也会随之提升。

3.2 建立健全完善的运维机制

在运维管理机制建设时，需要关注系统开发运营以及升级现状，及时指出各个工作阶段存在的问题，确定系统具体的覆盖目标，发挥安全管理制度的积极作用，达到稳定运维的理想目的。

第一，在建立健全安全管理制度时，需要通过运维操作和组织管理等方法，形成标准化机房管理体系。在明确各岗位的工作职责的基础上，解决设备管理常见的问题。

第二，提高运营管理系统的应急管理能力，全面检查新上线的服务系统，确保信息终端和服务系统没有问题。一方面，由员工定期展开安全检查，对所有软硬件系统进行统计，及时发现安全风险，将重点放在工作细节上。另一方面，在实践工作中需要对安全设备的日志进行全方位分析，增加数据分析量，达到排除安全隐患的目的，将所有隐患控制在萌芽期，实现网络安全管理的理想目标。运维管理需要遵循的标准如表 1 所示。

表 1 运维管理需要遵循的标准

序号	标准
1	《机房管理》
2	《设备管理》
3	《接入要求》
4	《日常安全管理要求》

3.3 更新行业信息化标准体系

石油企业发展需要提出了一种新的思路，即以政府为导向，以市场为导向，借助网络手段，构建起一条完整的、全产业链的服务链。我们将积极推动国有企业在关键信息基础设施领域率先应用国产密码技术，实现软硬件适配与替代。在信息化标准体系更新中，需要遵循网络安全法，明确信息化发展需要遵循的具体原则。

首先，建立等级保护制度，解决基础设施建设遇到的挑战。在实践工作开展时，信息化标准体系更新应与技术更新同步进行，通过备案和建设整改以及评测等方法，为设备保护提供数据支持，为系统全方位监控提供支持，优化现有的保护机制 [6]。

其次，在石油企业数字化转型过程中，管理人员需要承担安全主体责任，在安全防护系统建设过程中，以满足政策标准为标准，以政策为发展动力，快速完成顶层设计，推动各项业务持续进行。信息管理部门需要分类、分工，明确安全管理工作的核心，为网络安全环境建设提供保障。

3.4 增强员工的网络安全意识

创新是石油企业发展的核心竞争力，在企业数字化转型过程中，需要培养高素质人才，才能达到理想发展目标。

第一，网络空间安全管理，需灵活应对网络环境内各企业间的竞争，避免解决人才短缺等问题。加强石油企业网络环境安全管理，需要以企业实践为基础，解决人才培养薄弱的问题，需要构建专业人才团队，达到可持续发展的理想目标。在解决人才短缺问题时，需要通过聘请对口院校毕业人才的方式，预防网络安全的出现 [7]。

第二，加快企业内部员工培训。企业需要对在职员工进行定期培训，在安全教育和技术指导中，为员工提供交流的机会，对不同类型的员工进行针对性培养，构建高素质人才团队，满足石油企业数字化转型的基本要求。随着石油企业数字化转型的不断深化，石油企业信息化建设已成为必然趋势。在进行数字化改造的过程中，必须要与石油公司的经营活动密切结合，才能有效地防范和应对新的挑战。

4 结论

网络安全是企业数字化转型的关键，石油企业在数字化转型工作开展中，需要具有高度敏锐度，结合行业的现状，落实网络监测体系和相关保障机制、建设高质量人才队伍，为网络安全提供保障。在网络安全标准化流程建设中，需要排查企业网络环境漏洞，关注数据的交互能力，助力石油企业稳定发展，发挥数字化转型战略对石油企业发展的推动作用。

参考文献：

[1] 刘志鹏，赵毅．数字孪生技术在石油化工企业数字化转型中的应用研究 [J]. 石油化工自动化，2022,58(05):1-6.
[2] 杨倩．石油企业人力资源管理守正与创新 [J]. 合作经济与科技，2022(18):93-95.
[3] 闫昆，曹猛，鄢红亮．石油石化企业数字化转型背景下安防工作信息化智能化应用探索与实践 [J]. 中国安全防范技术与应用，2022(Z1):62-68.
[4] 曹光朋．“互联网 + 培训”模式下教育培训融合出版实践与认识：以石油石化行业教育培训融合出版为例 [J]. 新闻研究导刊，2022,13(12):193-195.
[5] 张弢，王雪松，王夏阳，等．石油企业科技管理数字化转型技术体系模型的构建 [J]. 科技创新与应用，2022,12(18):9-14.
[6] 邢悦．企业数字化转型中的组织变革和管理创新：以国际石油公司数字化实践为例 [J]. 中国石油企业，2022(05):54-58,127.
[7] 黄胜文，高增．石油销售企业数字化转型探索 [J]. 北京石油管理干部学院学报，2022,29(02):72-76.