

Research on Data Security in the Context of Digital Transformation of Power Grid Enterprises

Tao Liu

Jinan Licheng District Power Supply Company of State Grid Shandong Electric Power Company, Jinan, Shandong, 250000, China

Abstract

With the booming development of China's digital economy, digital transformation has become an important lever for the power industry to enhance its ability to serve the real economy, shape core competitiveness, and move towards high-quality development. In this context, new technologies such as big data, artificial intelligence, industrial Internet and massive digital products are applied to the process of digital transformation of power grid enterprises, and data security issues become more and more critical. Firstly, this paper introduces the core meaning of data security and its practical application in power grid enterprises, clearly pointing out the importance of data protection for the stable operation of the country and enterprises. Secondly, an in-depth analysis was conducted on the data security threats faced by power grid enterprises in the digital transformation environment. Finally, a data security strategy for the digital transformation of power grid enterprises was proposed to better maintain the country's energy security and economic prosperity.

Keywords

power grid enterprise; digital; data security

电网企业数字化转型背景下的数据安全研究

刘涛

国网山东省电力公司济南市历城区供电公司, 中国·山东 济南 250000

摘要

随着中国数字经济的蓬勃发展,数字化转型已经成为电力行业增强服务实体经济能力、塑造核心竞争力、迈向高质量发展的重要抓手。在此背景下,大数据、人工智能、工业互联网等新技术以及海量数字产品应用到电网企业数字化转型的进程中,数据安全问题变得越来越关键。首先,论文介绍了数据安全的核心含义及其在电网企业的现实运用,明确指出了数据保护对国家和企业的稳健运行的重要性。其次,深入剖析了电网企业在数字化转型环境下面临的数据安全威胁。最后,提出了电网企业数字化转型的数据安全策略,以期更好维护国家的能源安全与经济繁荣。

关键词

电网企业; 数字化; 数据安全

1 引言

在数字化转型的持续推进中,电网企业等关键的基础设施单位正在遭遇前所未有的大量数据安全的威胁。数据作为电网企业的主要财产之一,其保护度与安全性对国家的能源稳定及经济增长有着至关重要的影响。但是,数据量的指数级扩大、种类繁多且新的技术被普遍使用,电网企业的数据安全遭受了越来越大的压力。所以,构建合理的并有效地实施的数据安全计划,强化数据的安全控制与防范措施,已经成为电网企业在数字化进程中的首要任务。

2 数据安全在电网企业中的重要性

2.1 数据安全的基本概念

基本理念在于确保信息的安全,包括保全信息的完好性、可使用度及隐私权,以防非许可者获取或者修改这些资料。对于电网企业而言,保障数字安全的必要性显而易见,由于作为重要的基础建设设施之一,因此它们的运作内容及数据信息涵盖了国家安全、民众生活质量与经济发展等多项因素,如果数据信息遭到外流或是被人为变更,可能会给国家和公众带来巨大的损害。

近几年来,随着数字化转型的加速推进,电网企业面对前所未有的数据安全挑战。数字化转型导致电网企业的运营数据量急剧增加,数据种类也更加多样,包括结构化数据、半结构化数据和非结构化数据等。与此同时,随着云计

【作者简介】刘涛(1988-),男,中国山东文登人,本科,工程师,从事5G通信及大数据在电力行业的应用研究。

算、大数据、物联网等技术的广泛运用,电网企业的数据边界也在不断扩展,进而增加了数据泄露的风险。

为处理这些难题,电网企业需构建精确且高效的信息保护方案。第一步要确定信息安全的指导方针,这应包含合法性、全面性、灵活性和实用性等因素。第二步是必须执行具体的防护手段,如强化权限管理、优化数据存储与复原流程、提升密码学及通信保密水平等。第三步还需定期检查并评价信息的保障成效,以便尽早识别并解决问题可能带来的安全隐患。

2.2 数据安全在电网企业中的实际应用

对于电网企业而言,保障数据的安全使用不仅仅影响其常规运作,而且对国家能源稳定有着直接的影响。近些年,由于电网企业的数字化进程加快,大量的核心业务资料被整合并储存,如客户用电情况、设备运转状况等。如果这类数据遭到泄漏或者修改,可能会导致严重的问题出现,如供电系统瘫痪、恶意的网络攻击等。所以,在电网企业内,确保数据的安全运用变得至关重要。

为解决此一难题,电网企业需进一步强化其数据保护策略。首要任务是构建一套全面且细致的数据保全规章制度,明晰各层级职员的责任与权利分配,以保障信息在传递、储存及操作过程中保持稳妥无虞。接着,该公司应当利用前沿科技工具,如数据加密、访问限制、漏洞检测等,以此提升数据防卫性能。同时,电网企业也应该增强职工的信息安全教育,增进职工对于数据安全的认识深度。

2.3 数据安全对电网企业的重要性

对于电网企业来说,保护信息的安全至关重要。伴随着数字化的深度演进,电力行业正面对着空前的数据压力。因为数据是公司的关键资源,它的保密程度决定了公司的平稳运作及长期的发展。如果数据遭到了泄漏或者修改,那么不仅仅会给公司带来严重的发展损害,还会对全国的电能系统造成安全隐患,乃至危害国家的能源保障。

因此,电网企业在其数字化的转变过程中,应把信息保护视为关键任务,构建全面的信息保障系统,利用最前沿的科技工具与策略来保证信息的稳固性和可信度。唯有如此,电网企业才能够在严酷的市场环境下保持优势地位,并为国家能源稳定及经济增长作出更深远的贡献^[1]。

3 电网企业数字化转型背景下的数据安全挑战

3.1 数字化转型对数据安全的影响

在深度推动数字化变革的过程中,电网企业遭遇了史无前例的数据保护难题。这主要是因为企业的所有业务流程都在向数字化的方向转变,涵盖从数据收集到储存、分析、传递再到使用的全过程。在这个阶段中,数据量的扩大、类型的变化及流通性的增强对数据保密产生了巨大的威胁。根据最新的研究结果显示,近年来的各行业各类信息泄漏案件数量正在逐年攀升,而且这些案例中的许多都是由于数字化

改革的不当操作导致的。

多维度地来看,数字化的变革对于数据安全的威胁是全方位的。首当其冲的是,伴随着公司经营活动的数字化进程,电网企业的关键数据资源愈发丰厚且多元化,涵盖诸如消费者资料、电网运作数据及能源买卖数据等,如果这些敏感的信息遭到盗取或者修改的话,将会给公司的营运和品牌形象带来巨大的冲击。同时,数字化改革促使电网企业同其他行业进行了深入的整合,使得数据分享和交流更为频繁,这无疑增大了数据泄密的可能性。另外,数字化升级引入的新科技、新型应用大量出现,如互联网、云计算、大数据分析等,这些新兴工具不仅提高了电网企业的运转效能,同时也引发了一系列的安全漏洞和潜在风险。

针对数字化的转变可能带来的影响,电网企业必须实施一些有效的策略以保护其数据的安全。首要任务是构建全面的信息安全管控系统,设定清晰的数据安全的目标、准则及职责,保证信息安全工作有条不紊地推进。接下来,应强化科技开发与创新,持续增强数据保卫的能力,如利用前沿的加密手段、网络攻击防御工具等来防止信息的泄漏或修改。同时,也需加强对职工的信息安全教育和训练,增进电网企业对于数据安全的关注度和处理技巧^[2]。

3.2 电网企业面临的数据安全挑战

面对数字化的转变过程中的众多信息安全的难题,电网企业正日益受到数据的深度依赖的影响。技术进步使得电网企业更需要通过数据来指导商业策略与运营效率提升,但这也引发了诸如数据被盗取、修改或未经授权访问等问题。近些年,电网企业的数据安全问题频发,包括高等级的持久性的网络威胁等复杂的攻击方式。这类的袭击可能会使企业的机密资料外流,同时也会给电网的基础设施带来严重的损害,乃至危害国家的稳定性和民众的生活质量。

由于电网企业的业务数据巨大,在处理数据以及分析数据过程中,同时进行数据管理工作会出现信息拥堵的情况,影响数据处理的效率。电网企业需要搭建能够承受巨大的数据冲击管理平台,但是要使数据管理平台能够在如此庞大的数据冲击中正常运行,其日常维护的成本也会大大增加。所以数据管理平台能否对数据进行有效的分类、筛选、过滤,对电网企业经营数据处理的效率有很重要的意义。另外,大数据时代下大量的数据在数据管理平台上进行交换、处理、分析,如果没有有效的安全防范机制,数据安全是存在较大风险的^[3]。

3.3 电网企业数据安全问题的原因分析

在电网企业推进数字化的进程中,数据安全的挑战日益凸显。这主要归因于多种因素的共同作用。首先,是技术进步迅速,使得黑客及恶意侵入者采取了更为狡猾且不易察觉的方式来实施攻击。近年来的数据显示,对电力的网络袭击案件呈现出显著上升趋势,尤其是涉及高阶持久性的威胁(APT)等复杂攻势。这种类型的攻击通常无法通过传统的

防护策略予以辨识,因此对于电网企业的信息保护构成了重大风险。其次,电网企业在其数字化的转变进程中,必须融合众多商业与客户的数据,其中可能包含了公司的关键竞争力及顾客的信息保护问题。但在此类信息的集成与分享过程当中,因为缺少适当的数据处理和保密措施,常常会引发数据外泄或滥用的潜在威胁。最后,电网企业在其数字化的转变中也常常遇到人力匮乏与技巧缺乏的挑战。因为数据安全的科技发展迅猛,需要员工具有高超的技术能力和专业的素质。但是,当前电网企业的数据保护人员数量并未达到足够的程度,这也部分地影响到电网企业对数据安全的防护力量。

4 电网企业数字化转型背景下的数据安全策略

4.1 数据安全策略的制定原则

在设定电网企业数字化转型的数据安全策略时,首要的考虑因素是策略的制定准则。这些准则不仅为策略的设立提供了导向,也保障了策略的有效性和适应性。其中,明确性、可行性、灵活性以及成本效益性是关键的原则。

原则明确性要求数据安全策略需要明确、详尽,以便清楚地指导公司如何保护数据。这就要求在策略中不只是一要设定数据安全的目标和标准,还要清晰地指出责任主体、操作步骤以及违规行为的处罚等,以保证每一个员工都能清楚地了解自己的职责和行动路径。

实施性的准则要求我们根据公司的现实状况与资源条件来设定数据安全的策略。这就表示我们的方案不仅仅应考虑到理论上的数据保护,还需兼顾实践中其有效性和实用性。以电网企业为例,电网企业可能会思考怎样既能保证数据的安全又能维持电力的平稳运作及持续供应。

遵循成本效益性的准则意味着我们在设计与执行数据保护措施的过程中必须全面权衡其所产生的费用及收益。这就提示公司在构建方案的时候,不但需评估防护投资所需的花费,还需要预估该决策实行后的财务成果及其社会影响。例如,合理的保密政策能有效减低信息被盗取的可能性,从而避免了由于资料外泄而导致的经济亏损和名誉受损。

4.2 数据安全策略的具体措施

完善数据信息安全规定,确保电网企业数字化转型顺利有序。制定科学的数据安全规范,强化网络安全,防范信息网络犯罪,提升数据安全保护工作,借鉴先进管理模式,解决存在问题,提升数字化转型质量。

提升全员数据安全意识,降低信息安全风险。工作人员应辨别真伪信息,保护数据隐私,管理账户,备份数据。

企业更新补丁,完善访问验证,宣传安全意识,减少风险操作。

制定数据安全防范标准,营造安全网络环境。加强数据安全治理,增强基础设施建设,保障数据传输安全。升级系统,过滤敏感词,封锁聊天系统,分析安全风险,利用大数据技术提高安全水平。

严防外部手段侵害数据安全,打造安全数字化平台。提高网络稳定性,规避不合法入侵。利用病毒检测技术,创新网络安全技术,设计访问系统,管理用户身份和权限。优化数据共享路径,提升数字化转型工作质量。

4.3 数据安全策略的实施效果评估

在电网企业数字化的进程里,对于数据保护措施执行成效的评价变得至关重要。这种评价不仅仅是对该措施方案的测试,也是判断电网企业是否能顺利完成其数字化转型的关键指标。通过评价结果,公司能够迅速识别出方案中的缺陷和欠缺之处,进而采取相应的措施加以改善和提升。

为了衡量并评价数据安全的执行情况,须运用严谨且有效的技术与模式。例如,可以通过比较实施措施之后发生的数据泄漏次数及数据复原所需的时间等参数,以定量的形式评判其成效。同时,也能够利用问卷调查或面对面的交流方式,获取员工对于该项措施有效性的看法,以此更加深入理解其实际影响。

5 结语

面对数字化的变革之路,电网企业不仅要应对内外的各种信息安全的难题。论文对数据安全的核心含义、实践运用及数字化转型环境中的问题进行了深入探讨,并提出了一系列合理且有效的信息安全方案和方法。该方案覆盖了自设定准则至执行细节的所有环节,目的是构建全面的安全数据库系统,维护重要数据资源,保证公司的稳健运营。此外,还需要必须持续提升科技研发能力,强化员工培训,及时更新数据安全防御机制以适应时代的变化更加有效地抵抗各种安全威胁,保障国家的能源安全和社会安定,提高电网企业数字化转型工作质量。

参考文献

- [1] 迟克寒,李凤丽,冀爽.网络信息安全对电网企业数据的保护作用[J].现代企业文化,2023(10):53-56.
- [2] 白津夫.国有企业数字化转型与产业链现代化[N].经济参考报,2020-05-11(007).
- [3] 黄涛,余先敏.基于电网企业安全监督的大数据分析[J].企业科技与发展,2022(11):72-74.