对地市级烟草企业网络安全体系建设的思考

李 明
（陕西省烟草公司宝鸡市公司，陕西 宝鸡 721000）

摘 要：近年来，随着互联网技术的迅猛发展，烟草商业企业对互联网的应用需求体现在卷烟营销、专卖管理、企业管理和烟叶生产等各个方面，也体现在客户关系管理、服务消费者等方面。在大数据背景下，烟草企业必须要加强信息安全保护，从制度、人员、环境和硬件、防范等方面着手，不断筑牢企业网络安全防线，实现网络安全平稳运行，保障企业生产经营便捷、安全、稳定。笔者结合自身工作实际，阐述了烟草商业企业加强网络安全体系建设的背景和重要意义，分析了原因，并提出了对策。

关键词：烟草；网络；安全；体系；建设
【DOI】10.12231/j.issn.1000-8772.2022.09.148

随着企业数字化转型的迅猛发展，互联网作为企业生产经营的必要载体和工具，是现代企业高质量发展必不可少的应用手段。“没有网络安全就没有国家安全，没有信息化就没有现代化”。近年来，无论是国家还是企业对加强网络安全建设提出了具体要求，烟草行业作为国民经济的重要组成部分，在建设现代化企业的征程中必须高度重视互联网信息安全，完善网络安全管理制度，从人员管理、环境建设和运行维护、风险防范等方面入手，织牢织密网络安全防线，切实为实现企业高质量发展筑夯实网络基础。

1 网络安全体系建设的背景

2021 年，中国互联网络信息中心（CNNIC）发布《中国互联网络发展状况统计报告》显示，我国有网民 10.11 亿，宽带用户规模和移动终端拥有数量居世界首位。随着互联网的快速普及和应用，为社会大众的生活和企业的生产经营带来巨大的便利，国家网络空间法制化的进程也在持续加快，网络安全成为互联网快速发展的重要保障。2016 年，国家网信办等部门联合发布了《关于加强网络安全标准化工作的若干意见》，从工作机制、标准化体系建设、国际标准化等方面提出了具体的措施和意见，是我国安全标准化工作的纲领性文件，为全国网络安全体系建设提供了根本遵循。

对烟草行业网络安全体系建设而言，近年来，行业紧紧抓住行业改革创新和推动高质量发展的重要机遇，持续推动企业数字化转型，以全国烟草行业生产经营管理一体化平台建设为重要抓手，积极构建以数据驱动、平台赋能的产业链供应链一体化协同应用体系，不断增强数字驱动企业发展的内生动力。

地市级烟草商业企业作为企业生产经营的主体，也是网络安全体系建设的主体，其不仅要落实好国家局、省局关于网络安全体系的重要部署，而且要保障行业生产经营的各项业务在网络上运行顺畅，不断提升员工网络安全素养，防范网络安全风险，健全网络安全评价体系，抵御网络攻击，确保网络平稳有序运行。同时要注重网络安全体系的构建，从网络系统硬件、软件设计着手，明确网络层、链路层、物理层的传输协议，减小网络安全防护问题的难度，不断提升网络各个节点的信息安全。

2 烟草企业加强网络安全体系建设的重要意义

互联网被广泛应用在烟草商业企业生产、销售、管理、存储和运输等环节，其不仅建立了自己系统内生产经营的内部网络，也需要与相关的供应商、服务商和物流运输商、零售客户及消费者形成相关的链条和网络。在网络的架构和传输过程中，各个层级的网络信息和行为都会产生存储行为，这使得网络安全体系建设成为企业关注的焦点问题，也使得企业需要保护自身的信息安全，从而实现自身生产经营的平稳安全。笔者认为，烟草企业加强网络安全体系建设的重要作用主要体现在以下几个方面。

（1）加强网络安全体系建设，是企业数字化转型的基础。近年来，随着互联网技术的快速发展，建设数字化、智慧化和现代化企业成为共识，而数字化转型也成为烟草商业企业的必由之路。烟草行业作为国民经济的重要组成部分，其涉及的产业链多，对互联网的应用需求大，而实现网络对企业发展的顺畅保障，必须加强网络安全体系建设。烟草商业企业只有建成网络安全体系，才能抵御外来侵害，保障自身用网安全，保证各个业务层级的顺畅运行，保证相关业务方的权益，保证国家利益和消费者利益。

（2）加强网络安全体系建设，是提升网络防护能力的必要选择。必须要深入贯彻国家对网络安全建设的各项决策部署，牢固树立正确的网络安全观，不断提升企业管理层、职工和相关方的思想意识，提升防护技能，不断提升用网的安全水平。一方面，随着互联网技术的不断进步，网络入侵的手段越来越复杂，对网络防护的要求也越来越高，必须要建立高效、先进、完善的网络安全体系，抵御非法网络入侵行为；另外一方面，通过强有力的网络安全体系，提升自身的网络安全建设水平和风险防范层级。

（3）加强网络安全体系建设，是提升企业风险防范能力

的重要手段。近年来,烟草行业的发展过程中呈现出了数字化、智能化和集约化的发展趋势,信息技术广泛的应用在卷烟营销、物流配送和客户服务等领域;同时,信息化技术的发展也进一步优化了人力资源,减少了对人力要素的依赖程度。但是,对信息化的依赖程度越高,对网络安全风险防范的手段越要提高,如此才能保障网络的应用顺畅高效。网络安全风险作为企业运营风险的重要部分,企业必须高度重视,开展针对性的研究,提升信息安全风险防控意识,不断提高企业整体信息安全风险防控能力。

3 地市级烟草商业企业在网络安全体系建设中存在的问题和不足

近年来,地市级烟草商业企业不断加强网络安全投入,不断提升整体网络安全的硬件和软件防护水平,在网络安全基础体系建设上取得了明显的成效,保障了企业的平稳有序运行,有效提升了服务零售客户、消费者水平,但是笔者结合工作实际,认为还存在以下问题和不足:

一是网络安全管理标准化水平还有待提高。在网络的具体运行过程中,地市级企业建立了市局(公司)-区县局(分公司)两个层级的网络安全体系,但是在运行过程中对网络安全责任不明确,没有实施清单制管理,有时候区县局(分公司)存在着只用不管的现象,尤其是账户及数据管理不严格,账户的密钥登记不高,数据管理不严格,对网络安全的正常运行造成较大风险。

二是网络安全与信息化建设不同步。随着互联网技术的快速发展,烟草企业每年都要建设相应的信息化软件和硬件,不断提升自身的信息化运行水平。但是在建设过程中,对网络安全的布局偏少,对网络安全相应的建设力度不够,在关键信息基础设施建设时没有与安全技术措施同时规划、建设和使用。尤其是近年来,随着移动支付技术的发展,行业有关与第三方移动支付系统对接时,缺乏必要的信息安全评价,将企业内部数据接入到有关的互联网应用和服务中,造成数据信息安全风险。

三是员工网络安全责任意识还有待提高。在网络的运行过程中,网络安全风险时刻存在,防范网络安全风险是每个企业员工的应尽职责,也是构筑企业安全防线的重要力量。但是在实际工作中,员工对网络安全的防范意识还不强,对网络安全的防范能力还不高,尤其是主动性不高,对各种网络风险的分析、防范、抵御措施不够完善。对企业生产经营数据的保密意识不强,通过即时聊天软件发送有关信息,造成企业数据外泄的风险。

四是地市级烟草商业企业网络安全的专业管理人员力量薄弱。网络安全的软、硬件架构的任务主要在市级局(公司),市级局(公司)的网络安全管理人员需要承担计算机机房、网络链路、信息系统、信息化终端及维护、安全培训等诸多管理工作,但在人员配备上人员较少;在县级局(分公司),主要是网络的应用层面,对网络系统的日常维护,大多数为兼职人员,业务上存在不专业等情况,也为网络安全工作的开展带来一定的挑战。比如,专业的网络安全管理人员还需要对员工开展日常的培训、提升全员的网络安全防范技能,而人员的减少造成了有关工作的滞后。

4 对网络安全体系建设存在问题的原因分析

笔者通过分析地市级烟草商业企业网络安全体系中存在的问题,结合实际分析后,认为产生以上问题的原因主要体现在以下几个方面:

一是烟草行业信息安全风险防控体系较为分散。烟草行业的涉及的产业面广,作为地市级烟草商业企业,其不仅在角色上需要与上游的烟草工业企业产生信息联系,与下游的零售客户、烟农产生信息联系,由于联系的主体不同,烟草行业主体之间很难就信息安全风险防控形成统一的认知和行为方式,从而造成了烟草行业整体防范和控制信息安全的能力薄弱。具体到地市级(公司)其处于信息的中间节点,接收和传送的信息量大,无论是传输风险还是存储风险都比较大,对提升网络安全也造成了较大的困难。

二是烟草行业信息安全管理机制还不健全。地市级烟草商业企业目前应对重大安全风险的能力还不强,自身信息管理机制建设相对滞后,没有形成统一、健全、完善、高效的信息管理机制。比如信息存储标准、传输标准、使用标准和风险应对标准等规范性制度,对潜在的网络风险辨识和防控上缺乏针对性,在网络安全风险防控上产生漏洞。同时,烟草商业企业信息管理机制建设相对滞后,导致一些行业信息难以在行业范围内共享、传播,从而导致烟草商业企业整体的网络安全管理机制运行迟缓,甚至出现漏洞,造成信息安全风险防控阻力大。

三是企业信息安全风险防控的持续性还有待增强。随着信息技术的发展,也对烟草商业企业信息安全防控要求和等级提出了更高的要求,因为网络的环境是持续变化和发展的,这也要求烟草行业的信息安全防控建设永不止步,保持信息发展的步伐,根据不同阶段的信息安全风险制定和采取相应的防控策略。但是,结合目前的信息安全防控来说,更多的以被动式的政策性导向风险防控为主,主要是依靠政府网信等部门下发相关的制度和文件后,企业才开始按照文件要求进行信息安全风险问题自检自查和整改,这种被动式的防控缺乏持续性,主动防控的意识和能力不足,并且防控的内在动力不足,措施不够精准,时效性不强,难以真正达到防控的效果。

5 对烟草商业企业网络安全体系建设的思考和建议

笔者结合烟草商业企业网络安全体系建设的实际,结合目前存在的问题,对存在问题的根源进行了深入分析,并就新时期加强网络安全体系建设和网络安全标准化工作提出了建议。

(1)要始终贯彻落实《网络安全法》。烟草商业企业作为国有企业,必须认真贯彻落实《网络安全法》,深刻领会《网络安全法》的现实意义和立法主旨,始终把网络安全作为企业高质量发展的重要前提,牢固树立依法治网管网的理念,

加强全员网络安全意识培养，塑造企业网络安全文化，建设坚实的网络安全屏障，有效防范和化解各类网络安全风险，让企业的网络安全工作始终在国家法律、法规的轨道上运行，不断提升网络安全的法制化水平。

笔者认为，贯彻落实好《网络安全法》必须从以下几个方面持续发力：第一，网络空间的维护不仅仅要依靠政府部门，也需要企业、社会组织、技术社群和公民的共同努力，作为企业要切实落实好自身网络安全主体责任，明确自身在网络安全建设中的角色定位，扎实履行企业责任，全面参与到网络安全建设的工作中来。第二，要强化网络监测与应急处置工作，把网络监测作为网络风险防范的重要措施，加强对各类网络风险的评估，建立相应的网络风险应对应急预案，定期开展相关演练，不断提升风险的处置能力；要定期开展网络攻防演练，掌握网络安全体系应对的现状和等级，及时发现安全漏洞，处置网络隐患，提升网络安全等级。企业要建立统一高效的网络安全风险报告机制和研判机制，地市级烟草商业企业要成立网络安全建设的专门部门，定期研判企业网络安全形势，分析弱点和漏洞，不断提升网络安全建设成效。第三，要切实保障网络关键信息基础设施建设，不断健全、建强网络安全基础设施，加强网络的软、硬件建设，定期更新网络安全软件，提升网络设备硬件性能，提高网络密钥等级，提升网络存储能力，确保关键信息基础设施的运行安全。

（2）要不断提升职工网络安全能力。随着互联网、大数据的快速发展，无论是信息量的存储量和传输量都在呈级数增长，而在信息化和数据化时代，更注重对信息和数据的处理应用，挖掘和发现数据背后隐藏的规律和价值，为实现更加便捷的生活提供保障。作为烟草商业企业，更要不断的挖掘和利用企业生产经营中的数据，加强处理、分析，为企业的管控和发展决策提供依据。而在现实过程中，必须要依靠职工的执行才能发挥作用，而职工的不当操作很容易会造成信息泄露的问题，形成信息安全的内部威胁。因此，在实际的工作过程中，必须要提升职工网络安全素养，知道网络安全的风险和防范措施，不断规范员工用网能力，提升自身的信息安全保护能力。在这个过程中，企业应当针对涉密计算机操作、行业数据库操作、信息上传接收等职工信息行为，加以规范，并设置相应配套制度，确定安全风险操作清单，从源头上消除人为因素对企业数据安全带来的影响。

（3）要不断加强对网络安全工作的领导。作为地市级烟草商业企业，要加强对网络安全工作的领导，主动担负起网络安全工作主体责任，发挥其顶层设计和统筹协调作用，明确本单位网络安全工作的推进方向、工作重点和目标任务；要定期组织开展网络安全工作的研判，主动掌握本单位网络安全工作的现状，明确工作任务，强化工作督导，确保各项安排部署落到实处。要健全网络安全的责任体系，强化网络安全全员责任意识，明确各层级的责任清单，确保网络安全责任落实到岗、责任到人。要不断加强网络安全信息化基础设施建设，结合自身特点加强前瞻性思考、全局性谋划、系统性设计、战略性布局，制订符合自身发展的企业网络安全规划，在终端、应用、系统、网络和物理五个层面，通过广泛采用安全防护技术和安全产品，在身份认证、访问控制、内容安全、监控审计、备份恢复等网络安全防范关键节点加强针对性技术管控，保障当前网络安全的稳定可靠，切实为企业正常生产经营提供坚实可靠的网络保障。

（4）不断丰富网络安全管理手段。企业要充分运用行业安全运维平台，加强网络安全体系标准化建设，逐步形成标准化、流程化、一体化的安全运维管理机制和模式，要建立统一管理、分级负责、流程规范、安全高效的网络安全管控机制，保证应用系统的运行安全、信息安全、人员安全、资产安全。在网络安全隐患整改方面，针对历年网络安全专项检查、自查等发现的问题，企业要建立问题整改清单，实行销号管理，全面落实整改，并就整改情况及时向有关部门报告。同时，结合行业各级网络安全月度运行通报、专项检查等反馈问题，结合实际工作对照自查自身是否存在类似问题并予以整改。在应急处置方面，要精细编制年度网络应急演练计划，每年至少开展一次实战演练，每季度开展一次预案演练，定期上报演练结果，每年滚动完善演练方案，不断提升演练的适应性，实现常态化的应急演练。严格考核问责建立网络安全责任制检查考核制度，完善健全考核机制、流程、方法。将网络安全工作责任制考核结果纳入考核评价中，不定期开展督查检查，每季度开展通报，对发生重大网络安全事件的逐级倒查，追究当事人、网络安全责任人直到主要负责人责任，按照有关法律、法规严肃处理。

6 结束语

总之，地市级烟草商业企业要充分认识加强网络安全体系建设的重要意义，始终把贯彻落实《网络安全法》贯穿始终、不断加强对网络安全工作的领导、不断丰富网络安全管理手段、不断提升职工网络安全能力，切实为企业高质量发展提供坚实的网络保障基础。

参考文献

[1]张晶，李洪洋，张智钧，李佳怡，王梁.大数据时代数据安全治理的网络安全策略[J].网络安全技术与应用，2021(01).

[2]陈兴毕，李源，殷耀华，胥强，高进舟，杨勇.基于烟草工控系统网络安全风险评估的研究与应用[J].信息技术与网络安全，2019(07).

[3] 樊金健，谢一飞. 基于安全域划分的网络安全体系设计——保障烟草工业企业安全生产[J].工业技术创新，2019(02).

作者简介：李明(1982,3-)，男，河南洛阳人，汉，本科，助理工程师，研究方向：网络信息安全。