数字化转型背景下电信企业信息安全治理研究

黄 洁
中国电信股份有限公司伊犁哈萨克自治州分公司，新疆 伊宁 835000

[摘要]在数字化转型这一背景之下，云计算、大数据、人工智能以及5G等各类技术于电信企业当中得到了广泛的应用，这不仅推动了业务方面的发展，而且促使管理领域发生了变革，与此也使得信息安全风险变得更加复杂。电信企业属于关键信息基础设施范畴，其信息安全治理的水平对于企业的稳定运行以及社会公共安全而言有着极为重要的影响。文章就数字化转型背景下电信企业信息安全治理的相关问题展开分析，还对提升信息安全治理能力的具体实施路径进行了探讨，期望能够为电信企业在实现安全与发展协调推进方面给予一定的参考。

[关键词]数字化转型；电信企业；信息安全；安全治理
DOI：10.33142/sca.v8i12.18750 中图分类号：F275 文献标识码：A

Research on Information Security Governance of Telecommunications Enterprises under the Background of Digital Transformation

HUANG Jie
Ili Kazakh Autonomous Prefecture Branch of China Telecom Corporation, Yining, Xinjiang, 835000, China

Abstract: In the context of digital transformation, various technologies such as cloud computing, big data, artificial intelligence, and 5G have been widely applied in telecommunications enterprises. This not only promotes business development, but also leads to changes in the management field, making information security risks more complex. Telecommunications companies belong to the category of critical information infrastructure, and their level of information security governance has a crucial impact on the stable operation of the enterprise and social public safety. The article analyzes the relevant issues of information security governance in telecommunications enterprises under the background of digital transformation, and explores specific implementation paths to enhance information security governance capabilities, hoping to provide some reference for telecommunications enterprises in achieving coordinated promotion of security and development.

Keywords: digital transformation; telecommunications companies; information security; security governance

引言

随着数字经济快速向前发展，新一代信息技术也得到了广泛运用，数字化转型已然变成电信企业提高运营效率以及服务能力的关键战略走向。云计算、大数据、人工智能还有5G等技术都融入到了电信网络以及业务系统之中，在推动业务模式创新以及管理方式变革的时候，还让信息系统架构变得更为复杂，数据资源也高度集中起来，信息安全风险呈现出多样且动态的特性。作为国家关键信息基础设施的重要部分，电信企业在确保通信网络稳定运行以及用户信息安全方面肩负着重责，信息安全治理水平直接关乎企业可持续发展以及社会公共安全。在数字化转型不断推进的形势下，信息安全问题已经从单纯的依靠技术来防护的问题转变成了涉及制度建设、组织管理以及风险控制的综合性的治理难题。鉴于此，本文围绕数字化转型背景下电信企业信息安全治理来开展研究，通过对电信企业信息安全治理的实际状况以及主要挑战加以分析，去探讨提升信息安全治理能力的具体实施途径，期望能给电信企业达成安全与发展协同推进给予一定的参考。

1 电信企业数字化转型的技术特征

电信企业数字化转型的技术特征主要表现为网络运维的自动化与智能化、基础设施的云化与虚拟化以及系统架构的融合化发展。通过引入人工智能、机器学习和大数据分析技术，电信企业不断提升网络运维的智能水平，实现对故障、资源和性能的精细化管理；依托云计算和网络功能虚拟化技术，构建灵活可扩展的IT基础设施，为业务的快速部署和资源动态调配提供支撑；同时，通过数据

融合与平台化建设，打破传统业务域之间的数据壁垒，强化数据治理和业务洞察能力。在此基础上，5G 技术与边缘计算的深度集成进一步满足了多样化业务场景对网络性能和可靠性的需求，而 IT 与 CT 技术的深度融合，则有效提升了网络运维效率与业务目标之间的协同水平，为电信企业数字化转型提供了坚实的技术基础。

2 电信企业信息安全治理现状与问题分析

2.1 电信企业信息安全治理体系现状

随着数字化转型持续推进，电信企业搭建起涵盖网络、系统、数据以及业务全流程的信息安全治理体系。从架构来看，多数电信企业依照国家网络安全法律法规、行业规范，凭借企业内部安全管理制度构建信息安全治理架构，把信息安全融入企业整体治理与风险管理体系。在组织方面，信息安全治理一般由企业高层推动，相关部门协同参与，涉及网络安全、数据安全、系统安全及运行安全等方面；在制度层面，电信企业大多制定了信息安全管理办法、数据管理规范以及应急处置流程，对系统建设、业务运行和人员行为加以约束；在技术层面，逐渐引入身份认证、访问控制、安全审计以及态势感知等手段，针对关键信息基础设施和核心业务系统开展分级分类防护。

2.2 信息安全组织架构与责任分工分析

在当下的治理实践当中，电信企业大多都搭建起了相对完备的信息安全组织架构，并且把信息安全管理方面的职责融入到了企业的整体管理体系里面。就组织架构的设置情况而言，信息安全相关的工作一般是由企业高层来统一给予领导，像信息技术、网络运维、业务管理以及审计等诸多相关部门会一同参与到其中，由此便形成了多个部门协同开展工作的管理局面。各个层级的组织在信息安全治理工作当中肩负着不一样的职能，其中高层主要侧重于战略层面的决策以及总体上的管控事宜，而中层部门则是负责落实各项制度、开展风险识别以及做好日常管理工作，至于一线从事业务和技术工作的人员，则是直接去承担那些具体的执行任务[1]。不过，在实际的运行过程当中，因为业务条线众多、系统规模庞大、管理层级较为复杂，所以不同部门在信息安全职责的边界界定、协作机制的构建以及权责的划分等方面，依旧存在着一定程度的交叉与模糊不清的情况，信息安全责任在纵向的传导过程以及横向的协同配合当中很容易受到各种影响，最终会对整体的治理效能起到一定的制约作用。

2.3 信息安全制度与流程执行情况分析

在电信企业的信息安全治理实际操作当中，信息安全方面的制度以及相关流程，大体上已经构建起一个比较完整的框架体系，这里面包含了安全管理制度、操作规程、应急响应流程还有责任分工等诸多内容。然而在具体的执行环节，依旧存在着一些颇为凸显的欠缺之处。部分制度仅仅停留在文本形式上，其更新速度赶不上云计算、大数据、人工智能等新技术的实际应用状况，这就使得制度和业务的发展出现了脱节的情况，在实际的操作过程当中，这些制度所具有的可执行性以及指导性都显得不是很强。制度落实方面存在着“重制定、轻执行”这样的情况，安全流程在日常的运维工作以及业务高峰期的时候，很容易就会被简化掉，甚至会被绕过去，特别是在系统变更、权限审批以及外包运维管理等这些环节，流程执行的力度不够严格，存在着一定的管理漏洞。再者说，跨部门之间的协同配合不够充分，这也是对流程执行产生重要影响的一个因素，信息安全责任在网络、业务、运维等部门之间，其边界划分得并不清晰，如此一来，在制度执行的过程当中，就容易出现互相推诿或者重复管理这类的情况。

2.4 技术防护与监测能力建设现状

在信息安全治理的具体实践当中，电信企业不断加大针对技术防护以及安全监测能力方面的投入力度，进而逐步搭建起能够涵盖网络、系统还有数据等多个层面的技术防护体系。从技术防护这个角度来讲，企业在核心网络以及关键业务系统里都部署了像防火墙、入侵检测与防御、身份认证、访问控制以及数据加密这类安全技术，以此来对重要信息系统展开分级分类式的防护操作。而在安全监测这块，凭借集中运维平台以及安全管理系统，对网络的运行状态、系统的日志以及异常行为加以持续不断的监控与分析，从而达成对部分安全事件的实时发现与响应效果。不过，伴随云化架构、业务平台化以及数据集中化的程度一步步提高，信息系统的结构变得越来越复杂起来，安全监测的对象以及数据规模也在快速地扩大[2]。如此一来，现有的技术手段在监测覆盖的范围、关联分析的深度以及风险识别的及时性等诸多方面便面临着一定的压力，技术防护与监测能力实际所呈现出来的效果在不同的业务场景之中也体现出了一些差异化的特征。

3 电信企业信息安全治理实施路径与保障措施

3.1 完善信息安全制度与标准体系

在数字化转型不断向前推进的大背景之下，完善信息安全制度以及标准体系，对于电信企业来讲，其是提升信息安全治理能力所不可或缺的基础性保障所在。从一个方面来讲，得依据国家层面有关网络安全、数据安全还有个人信息保护等方面的诸多相关法律法规的要求，对现有的信息安全管理制度展开系统的梳理与整合工作，进而形成

一套能够贯穿网络建设、系统开发、业务运行、数据管理以及运维管理整个过程的制度体系，以此来保证各类安全要求能够在企业内部做到有章可循、有据可依。从另一个方面来讲，要围绕电信业务自身的特点以及数字化应用的具体场景，去建立起统一、清晰并且具有可操作性的信息安全标准，把安全要求进一步细化成为具体的各项技术规范以及操作准则，并且把这些规范和准则融入到项目建设、业务上线以及日常管理流程当中。与此借助制度和标准所具备的动态更新机制，能够及时地对新技术的应用情况以及业务模式的变化作出响应，以此来强化制度体系的适应性以及前瞻性，促使信息安全治理在企业内部达成规范化、制度化以及常态化的运行状态，从而为实现整体的安全治理目标给予强有力的支撑。

3.2 加强信息安全技术防护与能力建设

在数字化转型这样的大背景之下，电信企业所面临的各种安全威胁呈现出复杂化、隐蔽化以及系统化等诸多特点。所以，强化信息安全技术防护以及相关能力的建设，已然成为确保业务能够连续开展以及数据安全无虞的关键所在。电信企业应当从整体架构这个层面上去对安全技术布局加以统筹安排，围绕着通信网络、业务系统、云平台还有数据资源等这些重点方面的对象，去构建起一个多层次且具备纵深防御特性的技术防护体系，要让安全能力能够贯穿在整个系统从规划到建设再到运行直至维护的整个过程之中。在此基础之上，还应当进一步强化安全监测以及分析的能力，借助集中化的安全管理平台，针对网络流量、系统日志以及用户行为展开持续不断的监控活动，并且对其进行关联分析，以此来提高对于异常行为以及潜在风险的识别精准度以及响应处理的效率[3]。与此由于云计算、大数据以及人工智能等一系列技术在电信业务当中得到了极为广泛的运用，所以在信息安全技术能力的建设方面，还得着重关注其能否适应业务融合以及架构发生变化的情况，促使安全防护从原先单一设备的防御模式朝着体系化并且智能化的方向不断演进，让技术防护能力可以与业务发展的规模以及复杂程度相契合，进而切实有效地支撑电信企业在数字化转型过程中实现安全稳定的运行状态。

3.3 推进安全意识培训与专业人才培养

在电信企业信息安全治理具体实施进程当中，推动安全意识培训以及专业人才的培养工作，这无疑属于提升整体防护能力的关键保障举措之一。一开始，得面向全体员工去构建起分层分类的信息安全意识培训体系，并且依据岗位职责方面存在的不同差异来制定出具有针对性的培训相关内容。对于管理层而言，应当着重强化其安全治理方面的理念认知、合规责任的理解以及风险决策的能力提升；而对于技术人员来讲，则需凸显网络安全、数据安全以及系统防护等方面的专业技能方面的培训内容；至于普通员工，那么侧重点就放在日常操作规范、数据保护意识以及常见安全威胁的识别能力上，以此来防止因为人为出现的失误而引发相应的安全事件。接着，要结合电信业务自身的特点以及新技术的发展走向趋势，持续不断地开展专业化且实战化的培训活动，借助案例分析、攻防演练以及应急演练等多种方式，提升员工面对复杂安全场景时的应对能力，从而让培训的实际成效得以进一步增强。与此还应当对信息安全专业人才的培养以及引进机制予以完善。从一个方面来讲，可通过内部选拔、岗位轮换以及专项培养计划等方式，打造出一批既了解通信业务又熟悉信息安全技术的复合型人才团队；从另一个方面来讲，要积极地引进高水平的网络安全专家以及技术骨干，以此来补充关键岗位所需的力量。

3.4 强化安全合规与监督考核机制

在电信企业开展信息安全治理工作期间，强化安全合规以及监督考核机制，这对于各项安全制度能够切实有效地落实下去而言，是极为重要的保障措施。一方面要建立起与国家层面的网络安全相关法律法规、行业监管方面的要求以及企业自身的内部制度相互衔接起来的合规管理体系，把信息安全合规方面的具体要求细化落实到像网络建设、系统运维、数据处理、业务外包等一系列具体的业务环节当中去，进而形成清晰明了且具备实际操作性的合规清单以及责任台账，以此来保证每一项工作都能够做到“有章可循、有据可查”。另一方面需进一步完善监督检查机制，采用日常巡查、专项检查以及内部审计相互结合的方式来对安全制度的实际执行情况展开常态化的监督，尤其要着重加大对权限管理、系统变更、数据使用以及第三方合作等存在较高风险的环节的检查力度，以便及时地发现其中存在的隐患并加以整改。除此之外，还要构建起科学合理且行之有效的考核评价体系，把信息安全合规的具体情况纳入到部门以及个人的绩效考核范围之内，明确各项考核指标及其所占的权重，对于那些执行情况到位并且取得明显成效的部门给予相应的激励，而对于出现违规行为的情况则要实行责任追溯以及问责处理，以此来强化制度所具有的约束作用[4]。与此还需引入信息化的相关手段来为监督考核提供有力支撑，借助安全管理平台达成过程留痕、数据可视化以及自动预警等效果，从而提升监督工作的效率以及透明程度。

3.5 构建持续改进的信息安全治理机制

在数字化转型进程逐步推进且安全威胁始终处于演变态势的背景之下，构建起能够持续改进的信息安全治理机制，这无疑是保证电信企业信息安全体系可以实现长期且有效运行的重要保障所在。信息安全治理绝不能仅仅停留在开展一次性制度建设或者采取阶段性管理举措这样的层面，相反，应当形成一套贯穿于规划、实施、评估以及优化整个过程之中的动态管理机制，借助定期对安全风险变化情况、治理效果状况以及管理短板方面加以评估的方式，及时地去调整治理的重点所在以及管理的方式方法。电信企业有必要把风险评估、安全审计还有运行反馈等诸多环节都纳入到常态化的管理流程当中来，让信息安全治理能够随着业务的发展进程、技术的更新换代以及外部环境的变化情况不断地进行迭代升级操作。与此通过针对治理经验展开系统的总结以及对改进成果予以持续的固化处理，促使信息安全管理从单纯的被动响应模式朝着主动预防模式转变，进而强化治理体系所具备的适应性、韧性以及可持续性，以此为电信企业数字化转型给予稳定且长期的安全保障。

4 结语

在数字化转型不断向前推进这样的大背景之下，电信企业的信息安全治理已然变成了保障其业务能够稳定地运行以及达成高质量发展的极为关键的基础所在。仔细分析电信企业数字化转型所呈现出的技术方面的特征还有其信息安全治理当下的实际状况可以发现，信息安全方面存在的那些问题已经开始从单纯的某一技术层面逐渐朝着制度层面、组织层面以及管理层面等多个不同的维度去不断地延伸拓展开来，并且对于信息安全治理的要求也在随着时间的推移而不断地提高起来。本文紧紧抓住电信企业在信息安全治理过程当中所实实在在面临的种种现实问题，深入探讨了与之相对应的实施的具体路径以及相关的保障举措，其根本目的就在于促使信息安全治理能够和数字化转型一道实现协同并进的发展态势。在未来，伴随着新技术以及新的业务形态不停地涌现出来，电信企业的信息安全治理依旧需要持续不断地加以完善并且做出动态性的调整，唯有如此才能够使得整体的安全水平得以不断地提升上去，进而为整个行业能够健康良好地发展以及社会公共安全能够得到切实有效的维护给予强有力的支撑与保障。

[参考文献]

[1]崔亮亮.绽放信息通信技术服务能力[N].通信产业报,2025-09-08(16).

[2]晓镜.为数字化转型提供充沛动能[N].人民邮电,2023-05-19(01).

[3]杨官荣.信息通信企业携手助力昆明数字化转型[N].昆明日报,2025-05-13(01).

[4]董鑫.电信企业多维筑牢出海“数字保障网”[N].国际商报,2025-09-25(03).

作者简介：黄洁（1979—），毕业于南开大学信息安全专业。