第 4 卷◆第 1 期◆版本 1.0◆2026 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

通信运营商网络安全合规治理实践研究

韩筱
中国移动通信集团贵州有限公司
DOI:10.32629/acair.v4i1.19346

[摘　要] 随着数字中国和新型信息基础设施建设的加速推进,网络安全已由单一技术问题上升为涉及国家安全、社会稳定和企业高质量发展的系统性工程。通信运营商在网络安全合规治理中承载着保障公共通信安全的重要责任。本文以通信运营商为研究对象,立足当前网络安全形势新变化,系统梳理企业在网络安全合规治理中面临的突出问题,从制度建设、技术创新和人才培养三个维度,总结其在合规治理实践中的主要举措与实施路径,并对治理成效进行评估分析。
[关键词] 网络安全；合规治理；通信运营商
中图分类号：E965　**文献标识码**：A

Research on Cybersecurity Compliance Governance Practices of Telecommunications Operators

Xiao Han
China Mobile Communications Group Guizhou Co., Ltd.

[Abstract] With the acceleration of digital China and the construction of new information infrastructure, network security has evolved from a single technical issue to a systematic project involving national security, social stability, and high-quality development of enterprises. Communication operators bear the important responsibility of ensuring public communication security in network security compliance governance. This article takes communication operators as the research object, based on the new changes in the current network security situation, systematically sorts out the prominent problems faced by enterprises in network security compliance governance, summarizes their main measures and implementation paths in compliance governance practice from three dimensions: institutional construction, technological innovation, and talent cultivation, and evaluates and analyzes the governance effectiveness
[Key words] Cybersecurity; Compliance Governance; Telecommunications Operators

1 引言

网络空间已成为继陆、海、空、天之后的第五空间,是国家综合实力和治理能力竞争的重要领域。近年来,随着信息技术与经济社会深度融合,网络安全风险呈现出跨领域、系统化、隐蔽化的新特征,传统以技术防护为核心的安全模式已难以适应现实需要。通信网络作为数字经济运行的基础底座,其安全稳定直接关系社会运行秩序和人民群众切身利益。通信运营商作为区域内重要的通信基础设施运营主体,在推进信息化、数字化发展的同时,面临网络攻击手段持续演进、合规要求不断提高等多重挑战。如何在保障业务发展的同时,构建系统、有效、可持续的网络安全合规治理体系,成为亟需研究和实践的重要课题。在此背景下,本文基于通信运营商网络安全合规治理的实践经验,对其治理路径进行系统总结,力求从实践层面为通信行业网络安全治理提供可复制、可推广的参考范式。

2 网络安全合规治理的现实背景与问题分析

网络空间是继陆、海、空、天之后的第五空间,已成为国家战略博弈的新领域。随着数字化转型的加速,目前的网络安全形势,已从过去的技术性对抗演变为涉及国家、社会、企业和个人的综合博弈,进入了新的历史转折点。在去年召开的全国网络安全和信息化工作会议上,总书记鲜明提出“举旗帜聚民心、防风险保安全、强治理惠民生、增动能促发展、谋合作图共赢”的使命任务,明确“十个坚持”重要原则,把对网信工作的规律性认识提升到全新高度。统筹发展与安全,筑牢国家网络安全屏障,推动网信事业高质量发展是当前网络安全主要任务,在这一背景下,需要清醒认识形势,把握历史机遇,迎接前所未有的挑战。

2.1网络安全形势的新变化

从国际层面看,网络空间博弈日趋激烈,网络攻击目标不断

向政治、经济和民生设施领域延伸，网络安全已成为国家安全的重要组成部分。部分国家加快推进网络军事化进程，对全球网络空间稳定构成严峻挑战。

从中国国内现状看，当前各类设施基本已完成标准化的信息技术和网络技术的转换，并融入互联网，在提升了运行效率的同时，也给攻击者带来了新的攻击渠道。攻击者可能从网络空间入侵，通过长期、隐蔽的渗透式攻击，实现对基础设施的非接触式破坏。过去五年，针对企业的典型渗透入侵并勒索基础设施、窃取敏感数据的事件层出不穷。未来，随着移动互联网和人工智能的普及应用，网络安全风险将日益凸显。

从企业自身看，通信运营商作为通信行业的中坚力量，不仅是网络信息安全的捍卫者，也是经济发展的推动者。一方面，通信运营商承担着提供通信网络服务的重任；另一方面，信息化发展与网络安全相辅相成，信息化发展速度越快，网络安全风险指数也越大。要积极探索网络安全与信息化建设协同发展及深度融合路径，既要推动信息化高质量发展，也要筑牢网络安全防护屏障。应进一步加强其防护能力，从技术、制度、人员等方面多措并举，构建监测、预警、响应于一体的安全治理体系，实现网络安全与信息化发展的有机统一。

2.2合规治理短板的系统剖析

通信运营商始终坚持以人民为中心的发展思想，积极履行社会责任，高度重视网络安全治理的系统性与长期性。面对合规治理的现实挑战，运营商主动担当作为，以高度的使命感和责任感，对历史问题进行深刻复盘，开展举一反三、对标对表的深入排查，精准挖掘网络安全治理中的薄弱环节和潜在隐患，切实提升安全防护能力，为社会公众提供更加安全、稳定、可信的数字化环境。

一是管理层面存在薄弱环节。面对当前网络安全治理中的短板，聚焦实际生产中易发、高发的问题，深入剖析根本原因，发现主要症结在于安全责任意识尚未全面渗透到管理体系和工作实践之中，具体表现为以下两方面。一是制度执行的不到位。部分单位对网络安全相关制度的理解停留在表面，缺乏系统性、主动性，执行过程中未能做到严谨细致，导致制度要求与实际操作之间存在偏差。二是安全意识的薄弱。部分员工对网络安全的认知仍存在误区，在日常工作中，安全操作规范执行不严格，对潜在风险警觉性不高，面对安全威胁时应对滞后，影响了企业整体的安全韧性。需强化制度建设与执行力度，推动全员安全意识提升，构建全方位、多层次的网络安全防线，切实履行企业社会责任，为社会公众提供更安全、更可信的数字化服务环境。

二是自主创新能力相对不足。在技术飞速发展的背景下，网络攻击的形式愈加复杂和多样化，不断挑战当前的防护模式。首先是自主核心技术研发投入不足，部分安全技术仍依赖外部供应商，受限于第三方产品的适配性和可控性，难以满足复杂多变的安全需求，影响了整体防御体系的自主可控能力；其次是研发成果与实际应用场景的结合尚不紧密，难以形成强有力的攻防能力。需要加大研发投入，聚焦技术核心攻关，同时加强产研结合，构建适应安全需求的自主创新生态体系，全面提升对新型攻击的应对能力。

三是网络安全队伍建设存在一定的断层问题。首先人才梯队储备不足，部分岗位存在技能单一、专业能力固化的问题，难以适应日益复杂的安全环境和综合性治理需求。其次人才培养与实际业务需求的结合不够紧密，部分技术人员虽具备一定的安全知识和理论基础，但由于培训模式与实际业务场景脱节，技能转化率较低，制约整体安全防御能力的提升。

3 网络安全合规治理的主要实践路径

面对日益复杂的网络安全形势，通信运营商始终牢记央企使命，坚定履行社会责任，秉持“人民至上、安全至上、创新驱动”的原则，持续构建安全可信的通信网络环境，为国家安全、社会稳定、人民福祉提供坚实保障。

3.1以人民为中心，夯实制度与管理基础

一是强化安全意识教育，构建全民安全防线。2025年，围绕《网络安全法》《数据安全法》《个人信息保护法》《反电信网络诈骗法》等核心法规，组织网络安全专题宣贯，覆盖全体网络条线人员、核心系统岗位人员及第三方维护团队，全面提升全员安全意识，确保网络安全理念深入人心。二是健全安全管理制度，夯实治理根基。立足行业监管要求，制定并完善《通信网安全监测与处置细则》等一系列规章制度，形成 “全链条、闭环化、责任到人”的安全治理体系。严格执行信息安全等级保护制度，落实“谁接入、谁负责”原则，实现分级授权、精细化管理。三是强化技术管控，筑牢安全屏障。提升漏洞治理能力，2025年调整漏洞扫描频次，公网暴露面资产由每月扫描1次提升至4次，内网资产由每季度扫描1次提升至每月1次，严格执行“5+2+3”漏洞处置原则，确保高危风险快速闭环整改。目前，已累计完成漏洞整改323个，整改率100%，全面清除公网暴露面13000余个资产的高中危漏洞。四是深化互联网暴露面治理，提升资产安全管控能力。依托自研“巡御”系统，已累计完成1500余次全量扫描，补齐安全短板，确保互联网暴露面整体风险大幅降低。五是构建多源威胁监测预警体系，提升预警响应能力。通过整合威胁情报平台、内部安全监测系统，建立“预测—分析—预警—处置”的全流程管理机制，实现威胁信息的精准识别与快速响应。2025年以来，已预警高危公共安全风险26起，累计排查业务设备12万余次，发现并处置潜在安全风险337个，整改率100%，有效降低了网络攻击对社会通信环境的威胁。

3.2以创新驱动为引领，提升技术防护能力

科技创新是网络安全能力提升的核心驱动力。通信运营商坚定实施创新驱动发展战略，聚焦网络安全核心技术攻关，自主研发了具有行业领先水平的安全产品，不断提升对抗新型网络威胁的能力。

针对内网横向攻击威胁，“伏兵”系统以“智能安全大脑”为核心，通过智能化调度和动态化的欺骗部署技术，能够实时调整诱饵位置和策略，灵活应对不断变化的网络攻击场景，突破了传统静态防御的局限性，实现对威胁的精准诱捕与行为分析，目

前已在内网部署软探针500余个。极大提升了内网横向攻击的探测效率，一是从原有的人工监测告警、配置蜜罐、安装探针、配置探针四个步骤缩减至一键自动部署，部署上线时间由至少1周时间缩短至30分钟以内，显著提升主动防御效率。二是与其他安全设备联动，实现从传统单一设备模式到多个系统协作模式的转变。三是溯源反制能力提升，通过全面的攻击者画像，将溯源反制成功率由原先的10%提升至50%以上。

针对互联网暴露面资产安全运维，我司自研的“巡御”系统可直击安全管理难、人工维护效率低等行业痛点，通过智能化的安全运维能力，实现了从资产扫描、漏洞检测到压力测试、敏感信息保护的全流程自动化管理。特别是在实时端口监测、敏感页面识别和资产安全巡检方面效率得到明显提升，截止目前共发现并关闭高危及非高危端口786个、收敛暴露面资产8000余个、整改高中危漏洞50个，做到“高中危漏洞清零、高危端口清零、弱口令清零、网站信息泄露清零”，4个清零，显著提升了对外暴露资产的感知能力。

3.3以人才强基为支撑，构建长效保障机制

通信运营商始终坚持“人才是第一资源”的理念，聚焦人才梯队建设、专业技能提升和使命感培养，构建“知识赋能、实战驱动、责任引领”的三位一体网络安全人才培养体系。一是推进课程建设。梳理网络安全的课程知识体系，依托天巡实验室开展“4+1”的专业课程，建设《数字经济时代下企业应对网络安全合规及风险治理新思路》《企业视角看数据安全与网络安全：理解内涵演进，落实合规治理》《网络安全攻防渗透讲解》《CTF实战技能特训》等4门课程，1门《模拟城市攻防》实验课程。通过课程夯实网络安全人才的基础知识和能力，结合当前最近理论和技术进展，注重培养利用知识解决复杂问题能力。二是加强产学研用深度融合，搭建了贴近实战的城市仿真攻防靶场，将传统网络安全、工业互联网、车联网等产业环境融入靶场，构建多场景、多层级的复杂攻防演练平台。靶场能够模拟实际业务场景下的多维度网络攻击和防御行为，为学员提供高仿真训练环境。攻防靶场通过模块化训练，让学员全面掌握从漏洞挖掘到威胁对抗的核心技能，提升学员综合能力。三是构建网络安全人才梯队。在通信运营商网络安全专业队伍架构下持续深化人才培养，全力打造一支政治过硬、技术专精，能够对内、对外提供高质量安全服务的网络安全专家队伍，构建“培训达标－竞比拔尖－实训实战”三层渐进的网络安全人才梯队，目前团队成员达到40人，后备人员21人。2025年，团队成员平均每年参赛20余项（线上赛&线下赛），参赛超50人次，获省级三等以上奖项10余项，获奖超过10人次。同时，组织30人次参与集团及省内开展攻防渗透工作，覆盖多个业务系统及网络环境，实战能力显著提升。

4 网络安全合规治理成效评估

在风险治理方面，企业实现了公网暴露面高中危漏洞清零，显著降低了安全隐患；在安全管理方面，整体防护能力和应急响应水平明显提升；在技术层面，自主可控能力不断增强，为企业安全发展奠定了坚实基础。

5 结束语

网络安全合规治理是一项系统性、长期性工程。通信运营商的实践表明，只有坚持以人民为中心的发展理念，统筹制度、技术与人才建设，才能不断提升治理能力和风险防控水平。未来，随着数字经济深入发展，企业仍需持续推进治理体系优化与技术创新，为构建安全、可信的网络空间贡献更大力量。

[参考文献]

[1]王伟,李强.关键信息基础设施网络安全治理体系构建研究[J].网络空间安全,2022,13(06):1-7.

[2]刘志刚.数字经济背景下通信运营商网络安全合规治理路径探析[J].信息通信技术与政策,2023(04):45-50.

[3]工业和信息化部网络安全管理局.关键信息基础设施安全保护实践与思考[J].通信管理与技术,2021(05):12-16.

[4]陈立,周涛.企业网络安全风险治理框架与实践研究[J].信息安全研究,2022,8(09):835-842.

[5]黄健.新形势下通信行业网络安全合规管理体系建设探讨[J].邮电设计技术,2023(07):58-63.

作者简介：

韩筱(1987--),女,布依族,贵州黔南人,本科,研究方向：数据安全、安全合规、数据质量分析。