数字化转型中通信企业信息安全管理策略优化研究

徐伟炎[1] 陈卓玲[2*]
1. 中国电信股份有限公司宁波分公司 浙江 宁波 315000
2. 中国电信股份有限公司浙江分公司 浙江 杭州 310000

摘 要：伴随数字经济蓬勃兴起，通信企业作为数字基础设施关键承载主体，信息安全管理遭遇技术架构趋向繁复、业务场景日益多元的严峻考验。此项探究依托风险治理理论，搭建起“技术架构—业务场景—管理体系”三维解析框架，深入探究云计算、5G 及物联网等新技术应用引发的安全威胁演变态势，精准指出传统安全策略于动态风险评估、数据流转管控、跨域协同防御等环节存在的适配性不足。借由对中国电信、中国移动、华为等企业的实例剖析，给出涵盖构建动态风险评估体系、推进零信任架构部署、开展数据分类分级治理、强化组织能力成熟度建设的策略优化方向。

关键词：数字化转型；通信企业；信息安全；管理策略；风险防控

引言

当5G浪潮奔涌、云计算技术迭代、人工智能蓬勃发展，通信企业正经历从基础通信服务提供商向数字生态缔造者的深刻战略转变，业务形态突破传统语音通信范畴，智慧家居、工业互联、车联网等新兴应用场景不断拓展；技术架构摆脱封闭专有体系束缚，朝着云网协同、端边联动的开放式格局演进。这种变革使得企业信息安全边界持续模糊与延伸，安全威胁呈现出主体繁杂、手段智能、后果严重等新特征。审视当前现状，多数通信企业信息安全管理存在风险感知滞后于技术革新、资源调配难以匹配风险程度等问题，难以抵御数字化转型带来的新型安全挑战。本文紧扣通信行业特性，融合典型企业实践探索，系统剖析信息安全管理策略优化路径，致力于为企业构建适配数字化转型的安全防护体系提供理论指引。

1 数字化转型对通信企业信息安全的多维影响

1.1 技术架构变革带来的安全边界重构

云计算与虚拟化技术的深度渗透瓦解了传统IT架构的物理隔离屏障，通信企业核心业务系统逐步向多云混合架构过渡，衍生出数据跨域流转、虚拟资源不当使用、第三方云服务商风险传递等新状况。某省移动公司BOSS系统迁移至混合云架构后，因虚拟机逃逸漏洞致使客户信息泄漏风险骤增30%，原本基于防火墙的边界防护策略在云环境下难以发挥效用。5G网络所采用的网络切片技术虽优化了资源调度效能，然而切片间隔离机制存在薄弱环节，恶意用户极有可能借由切片边界入侵核心控制平面，2023年某运营商测试环境便出现过利用切片配置漏洞实施越权访问的情况。

物联网设备井喷式增长促使通信网络从“人与人连接”转型至“万物互联”格局，巨量终端接入衍生设备身份核验缺失、数据传输无加密保障、固件漏洞长期存在等安全隐患。某通信企业智慧社区项目内，未授权智能电表终端遭恶意代码植入，引发区域性网络拥塞，将传统针对入网接口的安全策略在物联场景下的防护盲区彻底暴露。边缘计算架构部署推动数据处理节点向网络边缘迁移，构建“云-边-端”三级架构，边缘节点因轻量化设计致使计算资源有限，难以部署传统安全防护组件，2024年某工业互联网平台就因边缘服务器补丁更新滞后，被攻击者借远程代码执行漏洞盗取工业控制数据。

1.2 业务模式创新引发的风险场景演化

于ToB业务范畴，通信企业针对工业制造、智慧医疗等产业供给定制化方案，业务流程深度融入客户核心体系，致使安全责任界限含混不清，一通信企业为汽车制造商供应车联网服务之际，由于未能精准辨识车载终端与云端通信存在的安全隐患，遭黑客借诊断接口侵入车载网络，进而引发车辆远程受控的安全事故，充分显现出跨行业业务协作中风险传导机制匮乏之态[1]。在ToC业务领域，短视频、直播等新兴应用的广泛传播促使流量呈井喷式增长，DDoS攻击规模跃升至Tbps层级，2023年某运营商CDN节点遭遇800Gbps攻击，造成区域性用户访问受阻，传统依托带宽阈值实施的流量清洗策略，已难以抵御超大规模的攻击威胁。

数据要素市场化配置促使通信企业开展数据资产运营，客户信息、网络信令数据等跨域共享诉求，与数据安全保护间的矛盾日趋尖锐，某通信集团在携手第三方开展精准营销之际，因数据脱敏处置未臻完善，致使

200万用户位置信息遭泄露，这充分彰显出数据共享场景中，分类分级治理、访问控制策略的关键意义。数字化转型进程中引入的人工智能客服、自动化运维系统，鉴于算法漏洞、训练数据受污染等状况，或会沦为新型攻击入口。2024年，某企业的AI客服系统被植入恶意指令，致使自动回应用户敏感信息查询，暴露出智能系统安全测试与监控策略的缺失。

2 通信企业信息安全管理策略的现状与问题

2.1 传统安全策略的适配性缺口

当下众多通信企业推行的“合规驱动型”安全策略展现出显著阶段性特点，将获取等保2.0、ISO27001等认证视为核心任务，存在“着重认证而轻视持续防护”这种结构性不合理之处。其安全架构规划沿用传统的“城堡式”防御模式，过度倚重防火墙、入侵检测系统（IDS）、安全网关等边界防护设备，在云网融合架构下暴露出防护体系衔接不畅的状况。以某省联通公司的安全评估为例，其部署的传统安全设备对于云内服务器间的横向移动攻击（像利用Kerberos漏洞实施的黄金票据攻击）检测比例仅达45%，针对RESTful API接口里常见的注入攻击、身份验证失效等漏洞（占OWASP Top 10攻击的60%）几乎毫无识别能力，这充分暴露出在零信任环境里边界防护存在能力空白。

现存风险评估机制存有显著时效性短板，多以年度或半年度的人工审计为主，对诸如5G切片隔离失效、物联网终端固件漏洞这类新型风险，难以及时察觉。某通信企业风险评估报告显示，识别5G网络切片因配置错误引发的跨切片渗透风险，以及物联网终端默认密码漏洞，平均滞后时长在6至8个月，这直接致使安全补丁部署延迟，攻击面暴露时长被拉长至行业平均水平的3倍不止[2]。再者资源配置失衡状况突出，安全预算中高达70%用于购置硬件设备，而安全运营中心（SOC）搭建、人员安全意识培育、红蓝对抗演练等管理层面投入却显匮乏，某电信企业复盘安全事件发现，70%的重大安全事故，像用户信息大量泄露、核心网设备瘫痪等，根源在于操作流程漏洞，比如权限审批流程缺失、变更管理失控，并非技术设备存在缺陷，这清晰反映出“重硬件轻管理”策略致使安全能力出现断层。

2.2 新型风险的治理机制缺失

通信企业于数据安全治理层面，尚未构建起完备的数据全生命周期管控体系，数据采集阶段，物联网终端与用户APP等未建立统一的认证授权机制，设备指纹未绑定，传输通道亦未加密。以某智慧城市项目为例，由于摄像头未对数字证书进行校验，恶意设备得以伪造数据嵌入核心系统，在数据存储环节，客户信息分散于三十余个异构数据库之中，就某移动公司而言，其30%的用户位置信息存储在无脱敏组件且未录入资产目录的边缘节点，难以实现安全策略的统一部署。

通信企业的数据共享依赖人工审批流程，动态访问控制机制缺失，在与金融机构协作过程中，某通信企业采用Excel手动标注数据敏感程度，却因权限设置不当，致使第三方获取到用户通话详单。部分领先企业创新构建三维数据标签体系，将用户信息划分为P0、P1、P2三个安全级别，针对P0级数据启用动态令牌认证等防护措施。某省电信公司部署数据标签管理平台后，审批效率大幅提升40%，权限配置错误率降低75%。

供应链安全管理现处“重采购轻管控”困境，企业多仅关注供应商合规文件，忽视开发环节安全与漏洞响应能力，某通信企业就因供应商未告知路由器开源组件Log4j漏洞，全网设备遭植入后门[3]。解决之策在于构建供应商安全评估矩阵，借威胁情报平台监控漏洞，如此可降低60%供应链攻击风险，某设备商推行供应链安全计分卡制度，量化考核供应商指标，有效提升其安全水平，应急管理体系存在“孤岛化”弊端，各系统应急预案各自为政，缺乏协同配合。某省通信网络遭遇APT攻击时，网管隔离链路，客服却未更新故障提示致投诉暴增，计费系统也未能识别虚假充值请求，引发15分钟计费异常，先进企业打造“预案标准化-演练常态化-响应自动化”体系，开发统一应急指挥平台，实现攻击事件关联分析与指令同步，某通信集团应急演练数据亮眼，故障定位时间由20分钟骤减至3分钟，策略联动耗时从15分钟缩至18秒，整体恢复效率提升70%。此外，引入“红蓝对抗+混沌工程”演练模式，推动应急从“事件驱动”向“风险预控”转变。

3 数字化转型中信息安全管理策略的优化路径

3.1 构建动态风险驱动的安全治理体系

打造涵盖“资产识别-威胁建模-风险评估-策略生成”的全链条动态管理机制，要构建技术工具与管理流程深度交融的立体化架构[4]。资产识别阶段，攻击面测绘技术融合网络空间搜索引擎和主动探测手段，不断扫描互联网暴露的IP地址、开放端口与应用服务，定位路由器、边缘计算节点、API接口等资产。某通信企业的攻击面管理平台嵌入资产指纹识别算法，能自动分辨合法资产和影子资产，像员工私自搭建的云存储桶，把资产发现率从60%提升到95%，还找出200多个未管理的影子资产，切实缩小攻击暴露范围。

威胁建模采用STRIDE方法，围绕5G网络切片场景，

剖析切片标识伪造、配置篡改、用户行为抵赖等威胁向量，搭建含30多个子场景的威胁矩阵。某设备商研发时用此方法，借威胁建模推动代码审计和架构优化，让产品发布前高危漏洞减少40%，从根源降低设计缺陷风险。风险评估创新整合定量模型与行业参数，用层次分析法确定网络重要性、数据敏感程度、业务影响范围的权重，打造通信行业专属风险评估矩阵。某通信集团风险评估系统依据实时采集的漏洞库、威胁情报和业务流量数据，每15分钟更新风险热力图，当边缘节点漏洞利用可能性超0.75阈值，自动启动“补丁推送-流量镜像-访问限速”三级响应，把漏洞暴露时间从48小时缩至2小时。

策略生成借助安全编排自动化与响应（SOAR）平台，构建风险等级和防护措施对应关系。低风险事件，像已知漏洞的非关键资产，自动生成工单告知运维团队；中风险事件，比如异常数据访问，触发微分段策略修改和日志强化审计；高风险事件，若出现APT攻击特征匹配情况，实时切断连接并开展全链路溯源[5]。某省公司于云网融合场景运用此技术，安全策略生效时间从人工操作的30分钟锐减到自动化执行的15秒，达成“风险识别-策略响应”的闭环协同。

3.2 实施技术架构与管理体系的协同优化

技术上推动零信任架构实施，打造“身份为基石、设备可信任、流量必验证、访问最小化”的安全架构，身份治理运用生物特征、设备指纹和行为轨迹的多因素认证，某通信企业内部系统接入认证里，身份冒用风险从0.5%降到0.05%。设备信任评估采用动态安全评分，实时监测终端补丁、软件完整性及网络行为，限制不达标设备访问，某省公司物联网终端接入管理中，未授权接入事件减少80%。管理上搭建覆盖决策、管理、执行三层的安全责任体系，建设首席信息安全官统筹战略，把安全绩效纳入业务部门KPI考核，某电信企业将安全指标考核权重提至30%，促进业务与安全融合，组织能力建设构建“培训认证-应急演练-攻防实战”提升体系，某通信企业建网络安全实训基地，借模拟真实攻击开展红蓝对抗，安全团队应急响应速度加快50%，漏洞修复效率提高30%。

于数据治理范畴，开展数据分类分级管理，构建涵盖客户信息、网络数据、业务数据的三级分类架构，依不同数据等级制定有差异的保护策略。某移动公司把用户位置信息、通话记录划定为核心数据，对其进行加密存储、访问审批、操作审计的全流程管理，数据泄露事件减少60%。数据共享过程中运用联邦学习、安全多方计算等技术，在保障数据隐私的同时释放数据价值，某通信企业与金融机构合作时，借助联邦学习技术开展用户信用评估模型协同训练，防止原始数据外泄。

结语

数字化转型促使通信企业信息安全管理进行从技术架构到管理体系的全面变革。本研究分析转型引发的安全挑战与现有策略适配问题，提出动态风险驱动治理体系、零信任架构落地路径、数据分类分级治理手段等优化举措。实践显示，通信企业要摆脱传统合规主导的安全思路，构建“技术能落地、管理可操作、风险可衡量”的新型安全能力架构。后续研究可深入探究人工智能在安全风险预判、区块链于安全审计中的应用，以及行业安全协同机制搭建，为数字经济下通信企业信息安全管理提供更具前瞻性方案。

参考文献

[1]夏博强.基于云计算的海上平台智能网格管理策略研究[J].电子元器件与信息技术,2023,7(07):143-146.

[2]陈昌茂.H公司信息系统安全管理关键影响因素研究[D].华南理工大学,2023.

[3]何黎明.数字化转型背景下集团型公司财务集中控制策略研究[D].河南财经政法大学,2021.

[4]熊祖雄.简析大数据背景下信息通信网络安全管理策略[J].网络安全技术与应用,2021,(03):125-127.

[5]邓瑶.SWD公司信息化建设的管理策略研究[D].哈尔滨工业大学,2020.