大数据与决策研究

2023 年第 39 期（总第 195 期）

广西壮族自治区信息中心
广西壮族自治区大数据研究院　　2023 年 10 月 26 日

广西数据安全趋势和治理对策研究

编者按：随着数字化时代的到来，数据已经成为数字经济发展的重要基石，跨企业、跨行业、跨国别合作模式的发展及数据的流转使用越来越凸显数据价值。但是，数据安全也逐渐成为阻碍数据要素流通及产生更高价值的重要因素之一。本文对我区数据安全发展趋势进行了研究，分析了存在的短板和弱点，并给出对策建议。

一、我区数据安全发展趋势

（一）数据安全基础制度体系基本形成。已颁布施行的《广西壮族自治区大数据发展条例》将数据安全作为独立章节，明确了数据安全全生命周期的顶层法律框架；出台了《广西政务数据安全管理办法》《广西电子政务外网运行管理办法》《壮美广西·政务云管理办法》等管理制度；建立重特大数据安全事件监测预警和应急管控处置机制、广西数字政府一体安全联席会议制度、数据安全协调机制及数据安全联络机制等工作机制；印发《广西政务数据安全保障实施方案》，提出了安全建设的路线图时间表，明确目标任务和责任要求，推动各级各部门的数据安全建设。

（二）数据安全防护体系逐步筑牢。政务关键信息基础设施和信息系统按网络安全等级保护的安全保护能力要求进行建设，形成从物理环境安全、通信网络安全、区域边界安全、计算环境安全和数字认证安全等多个层面的以边界防御为主的基础安全防护体系；建成“两地三中心”灾备服务体系，对政务数据形成有效保护；建成网络安全态势感知平台，形成常态化网络安全监测预警，对网络安全威胁行为和安全事件及时发现、预警和处置；建立多云共治平台、政务外网统一运维管理系统，实现各级各部门政务云、外网网络运行一体化监测，接入范围不断扩大。

（三）数据安全管理措施日益加强。加强对全区党政部门数字化建设中数据安全管理工作外包情况的督查管理，调

查摸排并督促各设区市和自治区各行业主管部门落实数据安全主体责任；组织对 70 多个区中直部门和设区市市级单位进行安全检查，对政务云及非涉密信息系统进行安全检查和评估；在政务数据资源管理与应用改革评估指标体系中设立数据安全管理专项考核指标；安全行政主管部门每年联合组织开展网络攻防实战演习，及时发现安全隐患，督查完成整改；定期开展信息系统漏洞扫描、网络安全自查、安全预警通报，强化关键节点网络安全保障，安全保障服务能力不断提高。

（四）信息系统数据安全形势依然严峻。针对关键信息基础设施和重点行业信息系统的探测、渗透和攻击逐渐增多，网络数据安全形势日益严峻。对比传统的网络安全威胁，数据安全威胁更加多样化，不再局限于利用安全漏洞和病毒木马等攻击手段，数据安全问题集中爆发在 API[1]接口攻击、特权账号弱口令、数据权限滥用及明文密码传输等方面。以政务信息系统为例，根据广西政务外网安全态势感知及数据安全监测平台监测结果显示，2023 年 9 月发生针对政务云网的网络攻击行为超过 43 万次，政务云上信息系统 API 接口共遭受 124 万次漏洞攻击，主要攻击方式是 SQL 注入、命令执行、代码执行、目录遍历、文件上传等类型，攻击行为次数有增无减，攻击方式复杂多变。

[1] API（Application Programming Interface，应用程序接口）是一种预先定义的函数，应用程序之间通过 API 请求获得数据。

（五）数据安全管理水平参差不齐。多数大数据发展和政务服务系统单位对数据安全管理较为重视。如信息系统采用了较完善的身份验证机制，通过双因子验证方式登录；联合公安、网信办等单位举办全市网络攻防演练活动，提升全市网络安全监测防护和应急处置能力；明确了数据安全组织机构及人员职责，安排了数据安全保障经费等。但更多部门在数据安全监管方面仍存在不少问题，如在数据安全管理制度方面较为欠缺，尚未印发信息系统数据安全管理制度，未设立数据安全岗位，未与单位内部数据岗位人员签订保密协议明确相关义务，信息系统安全技术措施较薄弱，存在较多明文密码传输、API 返回大量敏感数据和信息等问题。部分国有企业也开始重视数据安全管理工作，如明确了数据安全领导机构及实施机构的职责，形成了包含数据分类分级、第三方人员保密等管理制度的信息安全管理体系等。

（六）数据安全行业发展潜力有待挖掘。截至 2022 年末，全国现有数据安全企业约 39153 家，其中广西数据安全企业数量约为 687 家，占全国数据安全企业总数 1.75%，整体而言，广西数据安全市场发展空间较大。南宁市（61.7%）、柳州市（13.2%）、桂林市（7%）数据安全企业占据前三名，占比达到 81.9%，数据安全企业分布趋势与各市城市发展水平基本一致。部分省份数据安全岗位薪酬变化如图 1 所示，从 2021 年和 2022 年部分省份数据安全相关岗位招聘的平均薪酬中可以看出，四川、宁夏、广西、新疆、甘肃、陕西等

省份在数据安全人才招聘中的投入比 2021 年增多，但是广西对于数据安全人才薪资投入涨幅较小，对数据安全行业人才吸引力略显不足，仍有较大的提升空间。

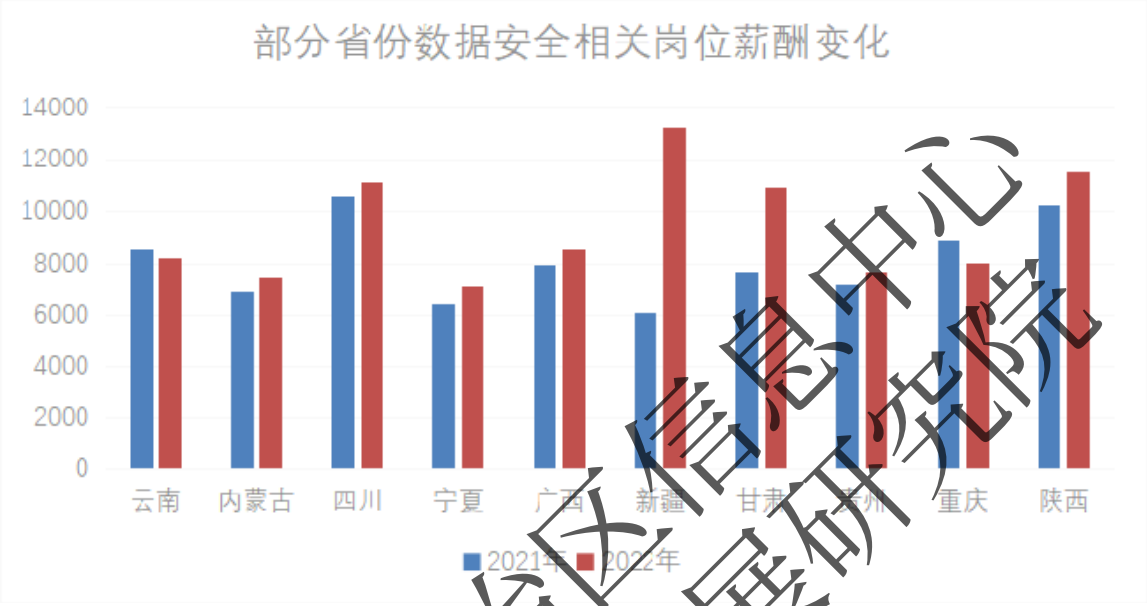

图 1 部分省份数据安全岗位薪酬变化

二、我区数据安全防护能力存在的短板

（一）数据安全工作保障措施有待加强。一是职责分工不清。很多设区市机构缺乏职责部门，或与同级部门间职责分工未明确。如市大数据管理部门与网信、公安等部门未明确职能范围，导致数据安全统筹管理责任模糊。**二是财政资金支持不足。**很多设区市的信息化建设经费少，大多投入基础设施建设中，数据安全方面的投入不足，缺乏足够的资金保障，难以支撑开展数据安全保障措施的建设。如信息化建设项目开工数量偏少，各级财政基本无前期专项经费预算；信息化项目建设资金较为缺乏，特别是数据安全方面，信息化平台搭建及安全保障遇到发展瓶颈；市政务云运营费多年

没有落实等。**三是缺乏专业技术人才。**没有足够的数据安全领域专业技术人才，编制少，或者招不到合适的人才，数据安全工作难以得到专业的支持和指导。**四是数据安全管理机制有待健全。**数据安全管理制度体系仅建立基础制度体系，缺少数据安全风险评估等更具体的工作规范和要求；未建立相应的数据安全评估和监督机制，缺乏对数据安全风险的整体研判和预警，无法及时发现和解决安全风险。

（二）数据安全技术支撑体系有待完善。一是数据安全防护水平相对薄弱。目前采用的数据安全产品均为单独的某一技术防护手段，如访问控制、数据脱敏、数据加密等数据安全防护技术。单点的防护手段不利于数据安全技术之间的协调联动。**二是数据安全服务能力不足。**没有提供统一的数据安全资源服务，各单位自行建设安全防护能力时缺乏指导，导致很多单位虽然部署了网络安全设备和策略，但是对外部攻击的应对能力较弱，黑客攻击、病毒入侵等事件时有发生。**三是缺少数据安全监测手段。**很多单位缺少完善的数据安全监测手段，没有建设数据安全监测系统对本单位数据安全态势进行监测。

（三）单位内部数据安全工作有待做实。一是未建立数据安全领导机构。很多单位未建立数据安全领导机构，一些单位的数据安全组织机构虽然存在，但是目标任务责任不清，措施不到位，难以有效保障数据安全工作落实。**二是未明确数据安全岗位人员及职责。**大多数单位对数据安全重视

程度不够，未建立数据安全团队，未设立数据安全岗位，无法有效开展数据安全工作。**三是信息系统数据安全管理不严格。**很多承载重要民生数据的信息系统存在大量明文密码传输、暴露大量敏感信息的现象，存在接口配置不当、漏洞修复不及时等问题，增加了数据泄露的风险。**四是对第三方公司监管欠缺。**很多单位的信息系统和数据是由第三方公司开发和维护的，但是对第三方公司的安全管理和服务质量监管不到位，导致系统存在大量漏洞及数据安全隐患。**五是缺乏数据安全培训。**部分单位没有重视数据安全培训的重要性，缺乏针对性的数据安全培训和宣传，导致职工缺乏数据安全意识，难以有效预防和应对数据安全事件。如在网络攻防演练中，弱口令问题连续4年成为网络攻防演习中最突出安全问题。

三、我区数据安全治理对策建议

（一）以数字化思维强化数据安全意识。保障数据安全是数字化发展的底线，必须坚持安全与发展并重，树立数字化思维理念，从自治区层面进一步强化数据安全意识，加强数据安全建设的统筹规划和监督管理。加强对各地各部门的数据安全进行监管和检查，指导各地各部门加强本地区、本部门以及相关行业、领域的重要信息系统及数据安全监测预警，强化日常监测、通报预警、应急处置。要把安全意识转化为安全行动，建立数据安全全生命周期的安全保障意识，从制度流程、人员能力、管理体系、组织建设和技术工具等方面落实数据安全能力建设。各级各部门要多渠道多方式加

强数据安全意识教育和培训，把安全意识贯穿到各部门推进数字化建设应用的全过程。

（二）以标准规范制度引领数据安全建设应用。坚决贯彻落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》等有关规定，以及国家、自治区关于加强数据安全工作的部署要求，健全完善数据安全领域的标准规范制度，抓紧研究制定我区数据安全评估、监测预警、应急处置、监督管理、责任追究、安全培训、考核评价、分级分类指南等标准规范制度。充分发挥好我区数据安全协调机制作用，督促各部门特别是市县级数据安全行政主管部门建立健全数据安全工作机制，完善数据安全领域的相关制度，指导各单位夯实数据安全合规性建设，护航数字化深入发展。

（三）以安全防护能力建设筑牢安全底座屏障。加快推进数字政府一体安全项目建设，构建数据安全监管平台，实现对全区各级各单位政务数据安全、合规运行情况进行监管，增强数据安全监测预警和应急响应能力，形成监测、预警、通报和整改的闭环机制，构建横向贯通、上下联动的一体化安全监管能力体系。加强数据安全监管检查，督促各部门把安全规范标准要求落到安全措施建设的实处，确保安全建设合规性。充分利用鹏城靶场广西分靶场，为各部门提供可复用共享的安全技术测评、网络安全攻防演练平台，持续扩大多云共治平台、政务外网统一运维管理系统的接入范围，降低各部门网络安全监控防护成本，提升整体安全防范效能。

（四）以构建数据安全生态激发产业活力。推动制定有利于企业发展和创新的政策，积极引入头部安全企业在我区设立分支机构，鼓励和扶持我区本地企业投入数据安全研究和技术研发，构建数据安全企业认证体系，提供更多适应市场需求的数据安全产品和服务。加强数据安全人才培养，鼓励高等院校、科研机构、企业等创新人才培养方式，深化产教融合，加快培养一批实用型、复合型的数据安全专业技术人才和优秀管理人才。充分发挥数字广西专家委员会、广西大数据学会等智库平台作用，通过举办论坛、研讨会、沙龙等形式，汇聚广泛的技术、人才资源，加强数据安全领域的交流合作。

（数据安全课题研究组）

广西壮族自治区信息中心
广西大数据发展研究院

编辑部地址：南宁市体强路 18 号广西信息中心 1412 号房

联系电话：0771-6113592

电子邮箱：dsjyjs@gxi.gov.cn

网　　址：http：//gxxxzx.gxzf.gov.cn/

扫描二维码获取
更多决策参考信息