数据安全风险分析及应对策略

（2022 年）

前 言

数据作为一种新兴生产要素，已成为经济社会发展的核心驱动力，与此同时日益严峻的数据安全风险为数字化转型的持续深化带来严重威胁。为保障数字经济的健康有序发展，提高数据安全风险防控能力，国家、行业、地方相继出台多项数据安全法律法规，并接连开展相应的审查整治行动。总体来说，国内数据安全已进入合规合法的强监管新阶段。面对日益严格的合规要求及数字化场景下的新型安全威胁，本报告梳理了当前数据安全面临的几个突出问题：

一是 APP 对用户信息的过度采集。大量非必要的个人信息聚集，不仅滋生数据滥用等安全风险，也带来合规问题。

二是账号弱口令的使用普遍。低成本的攻击门槛，容易导致特权账号被盗取，带来内部管理难题的同时引入数据安全风险。

三是数据权限分配、使用不透明。当数据权限管理成为“黑盒”，越权访问、数据滥用等问题将无法管控。

四是 API 接口成为新型攻击手段。API 作为应用与数据服务的通信接口，应用场景广泛，已成为攻击者窃取数据的重点攻击对象。 **五是数据安全的持续状态难以保持。**一方面，应用数字化改造及数据消费场景较为复杂；另一方面，管理要求和技术落地存在一 定脱节，导致持续的数据安全状态难以保障。

针对以上问题，本报告结合实战化攻防演习的实践经验，提出 数据安全体系建设的行动思路和关键举措，旨在为组织开展数据安 全体系化建设提供参考和建议。

目 录

图 目 录

一、数字化时代数据安全发展现状

数字化时代，数据已成为数字经济发展的核心生产要素。2020 年全球 47 个国家数字经济增加值规模达到 32.6 万亿美元，我国数字经济规模位居世界第二接近 5.4 万亿美元[1]。在此背景下，数据安全已成为事关国家安全与经济社会发展的重大问题。

（一）数据安全进入法治化的强监管时代

法律制度是数据安全的重要保障。当前我国数据安全法律法规建设取得突飞猛进的进展。**国家层面**，2021 年 9 月 1 日《数据安全法》施行，首次从法律层面明确数据安全保护义务，为开展数据处理活动的组织和个人提供了行为指引，填补了我国数据安全保护立法的空白。2021 年 11 月 1 日《个人信息保护法》施行，立足于数据产业发展实践和个人信息保护的迫切需求，更全面地保障了个人权利，及时回应了国家、社会、个人对个人信息保护的关切。**行业监管层面**，2021 年 9 月 30 日工业和信息化部发布《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》并公开征求意见，旨在加快推动工业和信息化领域数据安全管理工作制度化、规范化，提升工业、电信行业数据安全保护能力，防范数据安全风险。2022 年 1 月 4 日，国家互联网信息办公室颁布《网络安全审查办法》修订版，将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查。**地方政府层面**，积极落实国家政策和上位法精神，陆续出台相关地方法律法规。2021 年 6 月 29 日《深圳经济特区数据条例》

出台，率先就数据保护和利用开展地方立法，规范数据要素市场化行 为，推动数据的有序流动和数据产业的健康发展。2021 年 9 月 30 日《上海数据条例（草案）》公开征求意见，征求意见稿在《数据安全 法》等上位法的框架下，结合上海实际，建立了全面的数据安全治理 体系。

（二）数据安全事件频发安全威胁日益严峻

根据风险基础安全（Risk Based Security）[2]的数据显示，2020 年全球数据泄漏达到 360 亿条，创历史新高。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、恶意流量、病毒木马等攻击手段，数据安全问题集中爆发在特权账号弱口令、数据权限滥用、API 接口攻击等方面。

弱口令成数据泄漏爆发点。由于弱口令账号的低攻击成本和高命 中效果，通过盗取弱口令账号以横向渗透获得特权账号，进而破坏或 泄露重要数据资源的攻击行为，给数据安全管理带来很大挑战。根据Verizon 发布的《2021 年数据泄露调查报告》[3]分析，61%的数据泄露与凭证数据泄漏有关。

API 成热门攻击入口。由于应用架构的快速演变，API 成为业务应用与数据服务之间的主要通信方式，这导致利用 API 接口成为新型攻击手段。2021 年 4 月，Facebook 5 亿用户数据在暗网公开售卖，起因为 2019 年某在线业务的 API 遭到误用，导致数据泄露，影响约 5.3 亿用户。

权限滥用仍是数据安全事件的重要触发点。不规范的数据权限管 理以及缺失的技术防护手段，极易发生由于权限滥用而引起的数据资 源被破坏、篡改、删除等安全事件。2020 年 2 月，港股某上市公司员工通过 VPN 登入服务器，对线上生产环境进行恶意删库，造成旗下数百万用户业务中断，直接赔付人民币 1.5 亿元[4]。

隐私泄露成为数据安全的重要威胁。由于个人隐私泄露导致的数 据诈骗、大数据杀熟以及个人生物特征信息滥用等问题，已经严重危 害了个人信息主体的合法权益。据市场调研公司 Canalys 统计，2020 年全球个人信息泄露事件超出过去 15 年总和，成为影响个人权益、组织发展甚至国家安全的重要因素[5]。

（三）技术架构演进伴生数据使用场景改变

2021 年 3 月 14 日，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》全文发布，就数字经济、数字社会、数字政府、数字生态建设做了重要部署。传统信息技术开始 向以数据和业务为核心的新一代信息技术转变。**组织内**普遍通过采用 大数据、云计算等新技术，帮助组织提升决策水平，构建新型业务模 式，实现产业升级；**组织间**则大幅增加信息化交互，合作关系也更加 密切，通过业务协同、数据共享实现流程优化、合作共赢已经成为共 识。由此可见，**数据应用场景和参与主体的日益多样化，使得数据伴 随业务及应用在不同载体间流动和留存，贯穿于信息化和业务系统的 各层面、各环节。**因此，在复杂应用环境下，保证重要数据、核心数