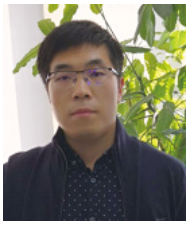
业务视角下车险数据安全策略与应用研究

文 | 中国保信 王立友



车险业务部 业务一处 副经理

先后在精友时代整车部、人保财险总公司车辆保险部，负责车辆承保管理、核保管理、核心系统需求管理等工作。目前在中国保信负责全国车险信息平台核心系统建设和维护，陆续完成了全国 36 个省市车险平台的物理和数据大集中，并实现了全国版本统一；负责开展配套全国商业车险改革、车船税联网征收、公安交管数据交互等全国项目落地实施。

当前，互联网技术飞速发展，以网络方式获取和传播信息已经成为现代社会的重要特征之一，网络技术的成熟使得网络连接更加容易，但随之而来的网络攻击、系统入侵等安全事件时有发生。2016 年 11 月，我国正式发布了《中华人民共和国网络安全法》，该法案明确提出网络运营者应采取数据分类、重要数据备份和加密等措施，防止网络数据被窃取或者篡改，加强对公民个人信息的保护，防止公民个人信息被非法获取、泄露或者非法使用。全国车险信息平台作为与保险公司实时交互的综合性生产支持平台，各类数据的内外部交互频率和范围逐年增大，数据安全防护逐渐成为车险行业关注的重中之重。

一、宏观政策推动数据安全快速发展

当前社会已步入大数据时代，人们之间的交流越来越密切，生活也越来越方便，大数据就是这个高科技时代的产物。国家各部门在加速推进“大数据战略”的同时，也在不断加强信息安全保护的工作。2015 年 9 月，国务院发布《促进大数据发展行动纲要》，基于国家战略的大数据顶层设计，在推动大数据发展方面提出了重要部署，其中一项重要任务是强化安全保障，提高管理水平，促进健康发展，健全大数据安全保障体系，强化安全支撑。

2016 年 3 月，第十二届全国人大四次会议通过《关于国民经济和社会发展第十三个五年规划纲要》，提出实施国家大数据战略，同时要强化信息安全保障。同年 11 月，全国人民代表大会常务委员会发布《中华人民共和国网络安全法》，加强对公民个人信息的保护，防止公民个人信息被非法获取、泄露或者非法使用。至此，信息安全以国家法律的形式正式颁布实行。

二、行业数据安全风险分析

信息泄露是政企机构面临的重要安全风险之一。2017 年以来，国内外均有大量重大的信息泄露事件被媒体曝光，泄露信息少则数十万条，多则数亿条，我国个人信息安全和隐私保护面临着严峻形势。个人信息作为数据信息的核心内容，面临着采集、存储、加工、各环节的使用规范化问题，与个人隐私息息相关。目前，一些行业个人信息泄露事件频发，不法分子甚至还会利用已经泄露的海量数据信息进行关联分析，甚至做出客户画像，精准定位用户身份后，实施精准诈骗。

为了更加全面的分析保险相关行业内信息安全风险及由此引发的其他安全问题，从数据全生命周期出发，对国内外数据安全状况进行了研究分析，以达到消除数据安全盲区，确保各项业务数据可知、可控的目标。

（一）接口传输安全风险

系统接口包括内部接口和外部接口，内部接口主要是平台内部各组件之间的接口，外部接口包括数据源到平台设施之间的接口、平台设施到数据消费之间的接口。系统存在多种途径供上层应用访问，但若权限控制不当，则会容易出现非授权用户越权访问或者合法用户对数据的非授权访问。数据源头与信息系统之间、信息系统与上层应用之间通过不安全的通道进行数据传输时，可能出现中间人攻击等安全隐患。

（二）应用支撑安全风险

在数据分析、数据交换、数据变现等数据应用过程中，系统应用支撑层对敏感数据未经加密或脱敏（或脱敏算法安全性较弱），容易造成敏感数据泄露。涉及上层系统应用和业务应用两个方面。一方面系统对数据导出行为不予控制，后台数据导出和系统间的数据导出，会引发数据泄露。另一方面业务基于对信息系统的访问完成其业务功能，业务应用自身可能会存在漏洞或业务逻辑权限处理不当情况，也会导致非授权用户越权访问或获取数据操作权限。

（三）数据存储安全风险

数据存储安全是业务数据安全的重要一环，安全风险具体包括以下内容：一是存储环境，存储系统自身安全配置（操作系统、中间件）不符合安全配置要求，为攻击者所利用，造成数据非授权访问；二是存储手段，数据加密存储以及访问控制机制不完善造成数据泄露；三是存储管理，大量结构和非结构化数据分散存储在不同的处理节点中，难以进行安全一致性管理，造成部分节点安全短板，导致敏感数据泄漏；四是数据残余管理，在数据生命周期结束后，数据未被彻底删除，或存有敏感数据的介质未被销毁，一旦数据被恢复就会引发数据泄露的风险；五是数据容灾备份，不完善的容灾备份机制会使得发生意外情况时，数据

无法及时恢复，从而影响业务的正常开展。

（四）基础管理安全风险

基础管理是指对支撑业务系统的服务器、机房、网络设备等设施的安全管理，基础设施的规范管理直接影响到业务系统能否正常运转。目前，行业内业务系统及上层应用大多由第三方厂商支撑建设，并参与运维。开发或运维人员往往拥有管理员权限，在安全管控手段不足的情况下，存在个别开发或运维人员从后台直接导出高价值敏感数据的风险，人员管理职责分配不当导致权限过于集中，缺少多人授权管控机制，容易引发敏感数据泄露风险。

三、从业务视角来看车险数据安全策略

车险业务在财险业务中占有六成以上份额，随着汽车保有量的不断增加，车险行业在数据安全方面投入也逐步加大。数据安全从业务视角来看，业务发展离不开数据的支撑，但不能忽视数据被业务逻辑洞穿的安全风险。业务视角下数据安全侧重于业务数据全生命周期的安全风险，关注业务数据流向，应用场景，业务运行中涉及到的各类业务执行角色，分析业务处理活动中权限、信息泄露、用户冒用、数据篡改等安全威胁及风险业务安全评估框架。

（一）数据全生命周期及安全需求定义

从业务数据全生命周期的角度来评估，我们对数据的全生命周期定义为五个组成部分，如下图 1 所示：

图 1. 数据生命周期组成

常见的各数据生命周期的安全需求点（包括但不限于）如图 2 所示：

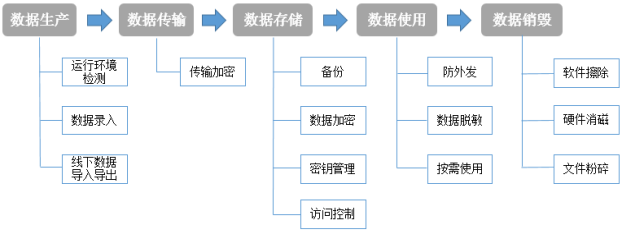


图 2. 数据生命周期安全需求点

（二）建立车险数据分类

依据当前数据情况，将车险业务数据进行分类：人员、车辆、承保、理赔、风险、交管类信息等，后续根据业务发展，适时进行扩充和完善，如表 1 所示：

表 1. 车险业务数据分类目表

序号	代码	类别	类别说明
1	01000001XX	人员信息	包括人员身份标识信息以及相关的属性信息
2	01000002XX	车辆信息	包括保险公司标的车、三者车信息
3	01000003XX	承保信息	投承保、批改过程中产生的保险相关信息
4	01000004XX	理赔信息	理赔过程中产生的保险相关信息
5	01000005XX	风险信息	由历史数据衍生的风险因素等信息
6	01000006XX	交管信息	从交管单位获取的相关信息
……	……	……	……

（三）划分数据安全等级

数据安全分级充分考虑数据对车险行业安全、客户财产安全的重要程度，以及数据是否涉及行业的商业机密、客户隐私等敏感信息，基于不同敏感级别的数据在遭到破坏或者泄露后对车险行业、客户的合法权益的危害程度，将不同类别数据的安全等级划分为三级，如表 2 所示：

表 2. 车险业务数据分级表

等级与敏感程度关系	敏感程度		
	高敏感级 [1]	中敏感级 [2]	低敏感级 [3]
等级划分	3 级	2 级	1 级

按照此敏感程度级别，分别对上述各类别进行敏感等级划分。在划分中，对于当多个字段组合能够明确指向一个主体的时候，其敏感程度升级，比如：某一个用户的出生日期、年龄、性别、居住地址同时泄露时，可以十分明确该用户的信息，其字段的组合应该属于第 3 级。

（四）建立分类管控体系

不同级别业务数据在生命周期不同阶段、不同应用场景下的安全管控要求不同，应随等级逐级增强，表中要求的每一级内容均是在上一级要求基础上新增要求，从而展现出不同级别数据在生命周期各阶段需要实施具体的安全管控处理。同时，还需结合技术可行性的评估分析，制订符合数据安全需求的具体管控方案。以不同阶段划分的各级别有关管控要求如表 3 所示：

表 3. 数据生命周期不同环节数据安全管控要求

级别 / 阶段	1 级	2 级	3 级
数据采集	确保数据采集的合法性、正当性和必要性，并且根据业务的需要，对数据进行分类标识	对采集到的数据进行完整性和一致性校验	记录并保存数据采集过程
数据传输	保证数据传输的完整性	保证数据传输的完整性	保证数据传输的机密性
数据存储	建立数据安全存储策略、用户标识与鉴别策略、数据安全访问控制策略	保证数据存储的完整性	保证数据存储的机密性
数据使用	保证数据的完整性，按照“最小开放范围”的原则开放使用	保证数据的完整性，明确使用各方的数据保护责任，未经各方同意，禁止向其他主体开放和共享	保证数据的机密性，如确实需要共享，在完成数据脱敏后，选择性的使用开放
数据销毁	鉴于保险数据的特殊性，生产环境和历史数据对费率精算、NCD 系数计算等均有指导意义，建议做好数据的存储和备份工作，不建议进行数据销毁		

[1] 高敏感级：是指可以明确标识用户身份或者标识业务唯一性的重要数据，如果其遭到破坏或者泄露后将对车险行业的正常经营秩序造成重大影响，直接威胁客户的隐私及合法权益。

[2] 中敏感级：是指涉及用户敏感信息及行业重要信息的数据资源，如果遭到泄露和破坏可能影响车险行业的正常经营秩序和客户的隐私及合法权益。

[3] 低敏感级：是指车险业务经营过程中涉及的通用数据，如果遭到泄露和破坏对行业秩序和客户隐私的影响较小或无影响。

四、有关启示和建议

数据安全治理绝非一日之功，它是一个动态的、需要不断去完善的过程。伴随着科技的进步发展，外部挑战和威胁日益突出，防御成本也越来越大，需要在业务发展和技术迭代的同时，注重高效的安全管理机制，建立规范的数据安全交互标准，提高业务人员安全意识和防控能力。从业务视角来看，有如下建议：

图 3. 数据安全工作推进步骤流程图

一是管理先行。建议完善业务数据安全治理框架，例如《数据安全保障体系框架》等制度建设，从制度层面指导各项业务的开展与应用。

二是风险评估。对数据全生命周期各个阶段面临的风险及威胁进行准确的监控及定位，根据数据的价值和特征进行风险评估，避免盲目开展业务合作造成的数据洞穿安全风险。

三是技术保障。围绕数据全生命周期进行分析，开展数据、人员、业务等方面的技术能力建设，推进数据脱敏、数据标签、业务态势感知等安全设施建设。

四是规范行业标准。在行业应用阶段，统一行业数据规范，进一步推动建立行业业务数据系统安全标准。