目 录

研究背景……1

综合形势篇……2

第一章 全球公开数据安全事件形势分析 ……2

一、 事件类型 ……2

二、 行业分布 ……3

三、 事发原因 ……3

四、 事件影响 ……4

数据泄露篇……7

第二章 境内机构数据泄露情报监测分析 ……7

一、 行业分布 ……7

二、 泄露类型 ……7

三、 个人信息 ……9

四、 关键字段 ……10

五、 典型案例与安全建议……11

第三章 互联网平台数据泄露监测分析……13

一、 行业分布 ……13

二、 泄露类型 ……14

三、 泄露原因 ……15

四、 典型案例 ……15

运营风险篇……19

第四章 API 敏感数据传输风险分析 ……19

一、 API 安全检测行业分布……19

二、 敏感数据传输风险……20

三、 个人信息传输风险……21

四、 各行业敏感字段举例.....21
五、 典型案例与安全建议.....22

第五章 数据跨境流转安全风险分析.....24

一、 跨境数据流转监测.....24
二、 关键敏感字段.....25
三、 行业对比.....26
四、 典型案例与安全建议.....26

附录 1 2023 数据安全政策与法规建设盘点.....28

一、 十六部门联合发布《指导意见》，1500 亿市场呼之欲出.....28
二、 数字中国建设顶层规划将数字安全被列为“两大能力”之一.....28
三、 央行发布数据安全管理办法， 填补该领域制度空白.....29
四、 财政部发布重磅文件， 数据资产入表全面启动.....29
五、 各地开通公共数据授权运营， “数据二十条”加速探索落地.....30
六、 促进开放和发展，网信办出台数据跨境流动规定.....30
七、 国家数据局正式揭牌， 数据要素万亿市场加速开启.....30
八、 北京数据基础制度先行区启动运行.....31
九、 工信部起草数据安全行政处罚裁量指引.....32
十、 国家数据局首提“数据要素×”， 2000 亿市场激活安全需求.....32

附录 2 2023 年全球数据泄露事件泄露数据排行榜.....33

附录 3 2023 年全球数据勒索事件勒索赎金排行榜.....34

附录 4 CEATI 联盟.....35

附录 5 奇安信数据安全事业部.....36

附录 6 奇安信行业安全研究中心.....37

附录 7 天际友盟.....38

研究背景

近年来，数据已成为产业发展的创新要素，不仅在数据科学与技术层次，而且在商业模式、产业格局、生态价值与教育层面，数据都能带来新理念和新思维。大数据与现有产业深度融合，在人工智能、自动驾驶、金融商业服务、医疗健康管理、科学研究等领域展现出广阔的前景，使得生产更加绿色智能、生活更加便捷高效，逐渐成为企业发展的有力引擎， 在提升产业竞争力和推动商业模式创新方面发挥越来越重要的作用。

一些信息技术领先企业向大数据转型，提升对大数据的认知和理解的同时， 也要充分意识到大数据安全与大数据应用也是一体之两翼， 驱动之双轮，必须从国家网络空间安全战略的高度认真研究与应对当前大数据安全面临的复杂问题。如：数据安全保护难度加大、个人信息泄露风险加剧等。

数据技术时代，数据成为业务发展核心动力，也成为黑客的主要目标。对于数据拥有者来讲，数据泄露几乎等同于经济损失。在开放的网络化社会，蕴含着海量数据和潜在价值的大数据更受黑客青睐，近年来也频繁爆发信息系统邮箱账号、社保信息、银行卡号等数据大量被窃的安全事件。分布式的系统部署、 开放的网络环境、复杂的数据应用和众多的用户访问，都使得大数据在保密性、完整性、可用性等方面面临更大的挑战。

为更加充分的研究政企机构数据安全风险，奇安信行业安全研究中心联合、奇安信数据安全事业部、奇安信威胁情报中心、网络安全威胁情报生态联盟（CEATI）、天际友盟等研究机构， 针对政企机构数据安全状况及风险展开深入研究。

本次研究分别从公开事件、数据泄露情报、数字品牌风险等几方面，针对数据安全（包括数据泄露、数据篡改、数据破坏等）展开深入的研究。希望该项研究能够对全国各地政企机构展开数据安全防护等建设规划有所警示和帮助。

综合形势篇

第一章 全球公开数据安全事件形势分析

本章内容主要基于《安全内参》平台收录的全球范围内公开的数据安全重大新闻事件展开全球数据安全形势分析。

一、 事件类型

2023 年 1 月~12 月，《安全内参》共收录全球政企机构重大数据安全新闻事件 246 起，平均每月 20.5 起，其中， 数据泄露事件为 166 起，占比 67.4%，泄露数据超过 51.8TB，共计 103.8 亿条。

数据安全事件主要包含数据泄露、数据破坏和数据篡改三大类型。其中，数据泄露问题已经逐渐成为核心痛点。从过去 3 年间，在全球所有公开的重大数据安全事件中，数据泄露事件的占比从 41.2%一路增长到 67.5%，而数据破坏事件的比例则从 42.0%下降到 11.4%。

造成数据泄露事件占比持续攀升的原因主要有两个方面： 首先， 全球化的地下黑产数据交易活动日趋频繁和成熟，窃取和非法贩卖数据不仅有利可图，而且回报丰厚， 从而推动了数据泄露事件的持续高发。其次，数据泄露事件往往会给社会治安造成严重影响，因此也日益受到媒体的关注。“附录 2 2023 年全球数据泄露事件泄露数据排行榜”，给出了 2023 年全球公开数据安全事件中， 数据泄露数量最多的 10 个安全事件。

特别值得关注的是， 勒索事件在所有数据安全事件中占比高达 27.2%，而且越来越多的勒索团伙开始从加密勒索转向数据勒索。传统的勒索组织主要通过加密数据的方式向受害者勒索赎金。2020 年以后，部分定向勒索组织开始采用加密勒索与数据勒索相结合的方式进行双重勒索，即勒索团伙在加密数据之前，先将大量商业机密数据窃取出来，如果受害者不肯支付赎金，勒索者不但不会向受害者提供解码密钥，还会威胁公开其窃取的商业机密数据。

但 2023 年的情况显示，已经有越来越多的勒索活动完全放弃了加密数据的传统攻击方式，而是转为单纯的以窃取机密数据并威胁公开的方式进行数据勒索。 2023 年，全球赎金最高的 10 起勒索组织攻击事件（详见“附录 3 2023 年全球数据勒索事件勒索赎金排行榜”），平均勒索赎金高达 2397 万美元，其中 7 起事件都是单纯的数据勒索事件。按照某些勒索团伙的说法，放弃加密数据的攻击方式，可以尽可能的减小勒索活动对社会面的影响，即在不直接影响生产的情况下完成勒索。数据勒索带来的巨大收益很有可能会吸引越来越多的黑产团伙参与其中。

二、 行业分布

2023 年 1 月~12 月，全球政企机构重大数据安全公开事件中， 18.6%为政府机构； 其次是制造业， 占比 15.9%为； 生活服务行业排第三， 占比 11.8%。下图给出了 2023 年 1 月~12 月， 全球政企机构重大数据安全事件所涉及到的十大行业分布。

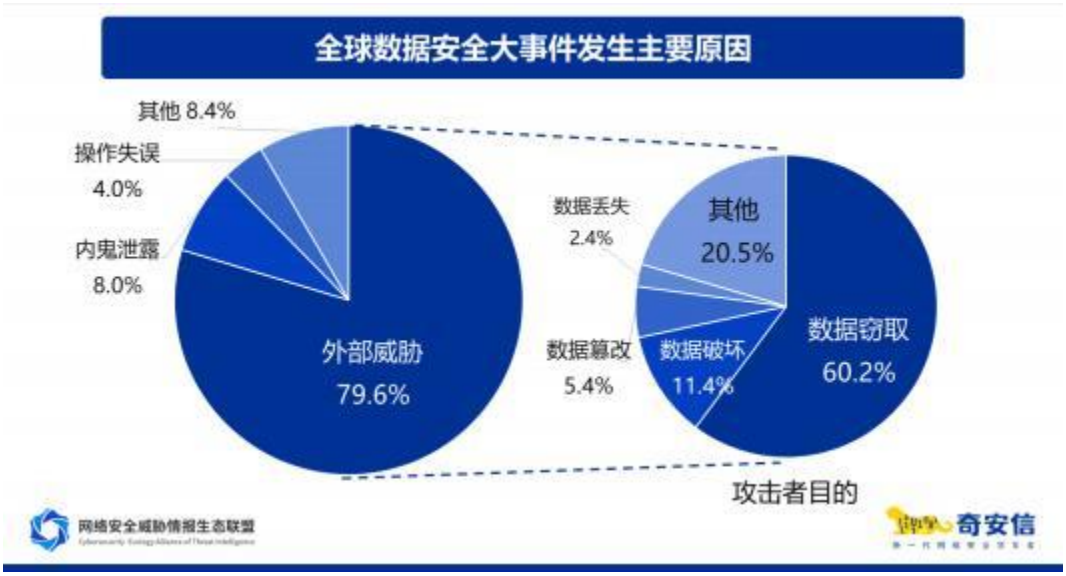
制造业的数据安全问题应当引起特别的关注。传统制造业企业很少产生数据，也很少收集、存储和计算数据。但智能制造技术的持续发展，使得部分制造业企业的生产过程全面数字化。特别是智能汽车、智慧安防、智能家居、可穿戴设备等新型联网工业品的普及， 使得相关制造业企业逐步转型成为重要的数据收集者和数据运营者，并且这些数据中往往包含大量的用户个人信息， 数据一旦泄露， 会严重危害公共安全。

三、 事发原因

从 2023 年 1 月~2023 年 12 月，政企机构重大数据安全事件发生的原因来看， 将近八成安全事件是由于外部攻击导致的， 但也有 8.0%的重大数据安全事件是由于政企机构存在内鬼。

存在漏洞是数据安全事件发生的重要原因之一。如果网络应用或系统存在安全漏洞，攻击者可以通过注入恶意代码、反序列化、权限绕过等方式利用漏洞获取用户敏感信息，或通过发起拒绝服务攻击超负荷消耗系统资源，使其无法正常运行或提供服务，对企业造成严重影响。

内鬼作案也是数据安全事件发生的重要途径。我们不仅要防外也要防内，做好数据操作的审计，防止非授权信息读取，防止越权的敏感信息读取，包括一些过度的数据读取其实也是一种泄露，比如： 在办一些业务的时候本来只用知道该用户的姓名、性别及年龄，但是在相关资料上还能看到其联系方式、工作单位等信息， 这样的过度读取或者暴露个人信息的行为也不合适。



如上图所示，从攻击者目的来看， 60.2%的外部威胁目的为数据窃取；其次为数据破坏，占比 11.4%。

综合数据安全事件类型与发生原因来看，72.7%的数据泄露事件由外部威胁导致。外部威胁（外部攻击）是造成数据泄露、数据破坏与数据篡改的最主要原因。

可见， 外部威胁是数据安全事件发生的最大威胁。

四、 事件影响

根据数据的敏感度， 我们把政企机构泄露的信息划分为以下几个类型：

1）个人信息：公民个人身份、账号卡号及行为信息等数据，主要包括：姓名、身份证、性别、婚姻状况、固定资产、电话、地址、邮箱、账号、密码、工作、出行、防疫、保险信息等。本节包括实名信息（如姓名、电话、身份证、银行卡、家庭住址等信息）、账号密码（如： 各类网站登陆账号密码、游戏账号密码、电子邮箱账号密码等）、行为数据、保单信息、人脸指纹等个人信息。

2）商业机密：企业经营活动中的商业机密信息， 主要包括：客户信息、员工信息、投资人信息、经销商信息、业务合同、工程项目、内部报告、研究成果、核心数据库数据等。

3）政府机密：有关政府部门的内部机密信息，主要包括： 邮件、会议、重大项目、重要文件、国家事务决策文件等信息。

4）软件源代码：企业开发的软件或网站系统平台的源代码，一般属于企业的核心研发机密。