数据安全治理白皮书

数据安全治理委员会 编著

前言
Preface

该白皮书由中国网络安全与信息化产业联盟数据安全治理委员会（简称数据安全治理委员会）起草编著，通过对国内外当下的数据安全情势与市场趋势进行解读与前瞻，结合国际相关标准与框架，提出符合中国信息化建设阶段和需求的数据安全治理理念与框架，旨在帮助政府与企业进行数据安全建设的整体思考与规划，为数据安全建设的设计与实施者提供具有参考价值的数据安全治理整体方案及案例实践。白皮书中阐述的数据安全治理体系是以数据资产的正常使用为前提，保障数据在各使用场景下的安全，促进数据价值的释放与共享。

白皮书主要撰写单位：北京安华金和科技有限公司、北京数字认证股份有限公司、北京炼石网络技术有限公司、中金金融认证中心有限公司、北京亿赛通科技发展有限责任公司。

主要撰写人：刘晓韬、杨海峰、闻璐、宣淦森、付蓉洁、沈雪峰、李伟明、刘思成、李敏、岳小杰、柴思跃、李贺等。

■委员会介绍

中国网络安全与信息化产业联盟数据安全治理委员会（以下简称数据安全治理委员会）是在中国网信联盟的指导与支持下，由北京市“数据库安全保障小组组长单位”安华金和牵头，联合业内知名企业发起的专业技术创新工作组织，这也是迄今为止，全国首家数据安全领域的专项委员会。

委员会将在中国网信联盟的指导下，在行业专家及学术专家的支持下，以行业数据安全应用为目标、以产业协作为主线、以技术创新为核心，形成在数据安全领域的技术研究、思维碰撞、学术探讨、行业实践分享的交流平台，探索和推

动政府、行业、企业在数据安全治理工作上的思路、规范和技术实践，以期达成在数据即资产时代，既保障数据安全又促进数据的分享和使用。

2018 中国数据安全治理峰会，数据安全治理委员会正式成立并对外发布《数据安全治理白皮书》1.0 版本。2019 年，延续 1.0 版本，数据安全治理委员会编写团队共同编著修订了 2.0 版本。未来，委员会各成员单位将发挥各自所长，持续开展产业研究与方案整合，共同推动数据安全治理理念与框架在各行业中的应用落地与经验分享，以期为各级政府与企业单位提供具有行业针对性的数据安全治理方案与技术支撑，帮助共同实现数据资产的价值释放。

■ 主任单位介绍

北京安华金和科技有限公司（以下简称安华金和），公司 2009 年 3 月 2 日成立至今，一直专注于数据安全领域，是中国专业的数据安全产品及解决方案提供商，由长期致力于数据处理和信息安全领域的专业人士共同创造。安华金和能够提供数据库安全全线产品及方案，并以此为支撑，全国首家提出“数据安全治理”框架，提供涵盖人员组织、安全策略、流程制定及技术支撑全方位的整体安全思路与方案。

围绕公司使命与愿景，安华金和主营业务方向分为三大部分：

1. 围绕数据库安全，安华金和推出全线数据库安全产品及解决方案。

2. 推进数据安全治理理念在各行业的方案落地和实践。

3. 面向公有云和私有云环境特性，提供云数据安全全线产品，为公有云和私有云用户提供数据安全整体解决方案。

目录

Catalog

《数据安全治理白皮书》2.0 版本修订说明

《数据安全治理白皮书》2.0 版本中，针对以下内容进行修订完善：

1、增加数据库防勒索技术，针对数据库勒索手段进行分析，同时提出防勒索技术；

2、增加个人信息收集与隐私政策测评报告相关解读；

3、国内外数据安全事件概要更新至 2019 年；

4、增加数据安全相关法规和标准列表说明；

5、数据安全治理外部所要遵循的策略中增加个人信息安全管理规范、银行业金融机构数据治理指引；

6、附录 C 数据安全治理实践增加教育部数据安全治理实践、市政务云数据治理实践、国家电网数据安全治理实践三个新的行业实践；

7、附录 D 国内外重要数据安全事件例举增加万豪集团 5 亿用户数据或外泄和 Oracle Rushql 勒索病毒事件；

8、增加数据透明加密保护技术；

9、增加数据库防勒索技术；

10、全文内容文字和段落结构的优化。

一. 数据安全建设需要系统化建设思路

数据治理或者数据安全概念，对于大多数 IT 和安全从业者来说，认知度比较高，但数据安全治理，似乎是个新名词。实际上，对于拥有重要数据资产的政府部门或企业，对于数据资产的保护，涉及到数据安全治理方面，或多或少都有实践，只是尚未体系化、标准化。比如，运营商行业的客户数据安全管理规范及落地的配套管控措施，一些政府部门的数据分级分类管理规范。在国外由 Microsoft 推出的 DGPC 方案（Data Governance for Privacy Confidentiality and Compliance 缩写），就是专门强调隐私、保护与合规的数据治理技术框架；Gartner 研究中在 2015 年提出了数据安全治理这一概念和相应的原则与框架，2017 年 Gartner 全球安全大会中多位分析师在数据安全、信息安全治理、安全治理的相关研究报告中，多次提及并加以强调，并且认为数据安全治理已成为了数据安全中的 “风暴之眼”（The Eye Of Storm），2018 年，Gartner 首次在数据安全治理方向上专门推出研究报告《如何使用数据安全治理》，以此为组织中的 CDO、CSO、CISO 提供数据安全价值。本次白皮书编著过程中，我们希望能够系统化针对数据安全治理的概念、规范、技术和相关实践进行介绍，将数据安全治理视作为一种系统化解决数据安全问题的合理方法论和实践工具进行推广和应用。

1.1 数据安全成为安全的核心问题

回看过去二十余年，政府与企业的信息化程度不断加深，IT 系统的复杂度与开放度随之提升；伴随云计算、大数据、人工智能等新兴技术的飞速发展，数据作为支撑这些前沿技术存在与发展的生产资料，已经成为组织的核心资产，受到前所未有的重视与保护。

随着数据成为资产，成为基础设施，组织通过数据组织生产力，数据成为国家发展的重要原生动力；数据驱动商业（data drive business）成为新的商业发展的最大创新源泉。人类经过几百年的科技高速发展后，即将迎来智能时代，智能时代的决策基础就是数据和算法，数据的安全问题将引发企业和社会决策的安全问题。

当前，无论是数据和资产交易市场的形成，还是勒索病毒的演进，都在证明数据面临的风险越来越大。由于勒索软件攻击拥有低成本、高产出等特性，网络犯罪集团可以通过不断推出新的变种版本，来躲避杀毒软件的查杀。而一旦中招，受害者往往为了减少损失，会选择支付赎金，无疑助长了勒索软件的泛滥态势。

美国安全公司 Carbon Black 发布了最新的勒索软件调查报告，和去年相比，暗网经济中勒索软件的市场规模猛增了 2502%。2017 年，暗网上勒索软件的相关产品销售额高达 623 万美元，是 2016 年 25 万美元的 25 倍。在暗网上大约有超过 6300 个网络市场提供勒索软件的交易，其品类则更超过了 4.5 万种。2016 年不法黑客通过勒索软件总共获得了 10 亿美元的收入， 2017 年获利远远超过 2016 年，未来更会极具上升。数据的安全问题，已成为企业资产安全性、个人隐私安全性、国家和社会安全的核心问题。

由于数据库承载着核心数据，经历 2016、2017 两年的“完善”，2018 年勒索软件已经从乱枪打鸟，转向精准攻击。越来越多的勒索软件开始加入针对数据库的攻击模块。数据库文件现在已经成为勒索软件优先加密的对象。

除去常规勒索软件对数据库文件加密外，有两种利用供应链针对数据库的勒索软件正在大肆兴起。第一种是通过供应链直接对数据库服务器进行攻击。2018 年 12 月 14 日一款通过“驱动人生”升级通道的木马突然爆发，仅 2 小时内就攻击用户电脑 10 万多台。值得注意的是，这款软件除了会利用高危漏洞在企业内网呈蠕虫式传播，并进一步下载云控木马外，还有专门的暴力破解模块，用来破解 sqlserver 数据库的 sa 用户密码。一旦破解成功就会换一组新的 sa 密码。从而控制用户数据库实施勒索。第二种是对数据库客户端发动攻击。Oracle Rushql 勒索软件就是这样的例子。该软件捆绑在被感染的绿色版 / 破解版 PS/SLQ developer 安装程序上，一旦用户连接到数据库，就会立即执行“Afterconnet.sql”中的代码，在用户的数据库中创建多个存储过程和触发器，并判断数据库创建时间是否大于 1200 天。如果大于 1200 天，重启数据库后会触发病毒触发器，加密并删除 sys.tab$，导致用户无法访问数据库中所有的数据库对象集合（schema），提示“你的数据库已经被 SQL RUSH Team 锁死，请发送 5 个比特币到这个地址……”的勒索信息，并设置定时任务，如果在期限内不交赎金，就删除所有的表。对于数据库的勒索攻击成为网络攻击的一种新常态，攻击方式不断花样翻

新，防不胜防；而企业一旦遭到攻击面临的将是严重影响正常运作。

除了潜伏在暗处的勒索软件外，个人数据隐私也快速从道德约束向法律约束过度。在2018 年个人数据隐私保护只是一个重要话题，但 2019 年就将通过法律、监管和技术手段共同构建个人数据隐私保护。2018 年底发布的《App 个人信息收集与隐私政策测评报告》和四部委联合开展的《APP 违法违规收集使用个人信息专项治理》行动，说明个人信息数据是企业的核心资产，企业在强调权利的同时，也应切实担负起保护用户隐私安全的责任。如果企业行为可能给用户造成危害，企业有责任和义务保护用户数据。同时，个人隐私的保护也要面临法律先行，目前我国没有统一的个人信息保护法，虽然《网络安全法》作为我国网络领域的基础性法律将个人信息保护列入其中，既是出于国家网络空间主权和网络安全考虑，也是对当前个人网络信息安全严峻现实的直接回应，但远不能全方位地保护个人信息安全，也存在个人信息保护的法律漏洞。但是通过过去的一系列个人信息泄露案件给社会带来的不良影响，使人们充分意识到了个人信息泄露和滥用所带来的严重社会危害，同时也催生个人信息保护立法落地。

随着人工智能（AI）、大数据的发展，数据已经成为数字化转型时代的核心竞争力，是能源时代的“石油”，数据安全保卫战也将全面打响。2018 年纳入立法计划的《数据安全法》在刚刚过去的 2019 年两会被大量的讨论和关注。目前，大数据在三个方面存在巨大的安全风险：个人数据过度采集和使用，造成重大社会安全风险；数据处理缺乏防护措施和手段，存在严重技术安全隐患；隐私信息易于获取，导致地下网络犯罪高发。这些数据安全风险将严重影响大数据战略的发展，迫切需要从法律层面通过国家立法来保障数据安全。

在数据保护手段层面，商用密码管理要求正式进入等保 2.0 的安全检查要求，对于密码的使用具有了更强的要求和指导性。同时通过等保 2.0 的落地实施和检查，加密保护技术将具有更强的落地能力和实施检查能力。

1.2 数据泄露路径多元化

过去几年间，大型数据泄露事件层出不穷，这其中不免存在媒体聚焦度提升带来的舆论转移，但究其根本是社会各界对于数据资产安全的关注度与日俱增。从刚刚发生的 Facebook 数据泄露事件看全球数据安全态势，AWS、德勤、网易、Equifax、京东、优酷、58 同城等商业巨头纷纷中招，政府机构和组织也不能幸免，考生信息、公民医疗信息等民生数据泄露事件正在倒逼政府主管机构和企业对数据安全建设重视与落实。

下面对近年国内外影响严重的部分数据泄露事件进行整理，通过对数据泄露事件的源头、数据量、成因等信息进行了解，让我们对目前国内外数据安全现状有更直观的了解：

分类	序号	事件名称	事件时间	泄露人员	泄露数据量或非法所得
国外	1	万豪数据泄露事件	2018 年 11 月	黑客通过喜达屋系统盗取	5 亿数据
	2	华住酒店数据泄露事件	2018 年 8 月	身份不详调查中	5 亿数据
	3	数据代理商 Exactis 数据泄露	2018 年 6 月	配置错误导致	2.3 亿数据
	4	Facebook 数据泄露事件	2018 年 3 月	共享第三方，剑桥分析公司，特朗普团队大选数字合作公司	5 千万条
	5	印度国家身份认证系统被攻击事件	2018 年 1 月	黑客入侵导致	11 亿数据
	6	美国国家安全局泄露绝密数据	2017 年 11 月	内部人员，存储服务器技术人员错误配置	100GB 以上
	7	德勤数据泄露	2017 年 10 月	黑客，利用早先获得的管理员账号的黑客	500 万条
	8	Equifax 信息泄漏露事件	2017 年 9 月	黑客，利用应用漏洞攻击的黑客	1.43 亿条
	9	亚马逊 AWS 服务器存储文件泄露	2017 年 8 月	内部人员，Election Systems & Software 公司	180 万条
	10	共和党数据库泄露	2017 年 6 月	合作方，受雇于共和党的一家网络数据供应商 Deep Root Analytics	2 亿条
	11	Dun & Bradstreet 数据库遭泄露	2017 年 3 月	合作方，疑似以往出售过数据的企业用户	52GB 数据库遭到泄露，涉及千万美国军方企业信息
	12	MongoDB 再出安全事故	2016 年 10 月	黑客，利用引擎软件发现敏感数据的黑客	5800 万条
	13	美国班纳健康中心患者信息遭泄露	2016 年 7 月	黑客，通过销售端系统入侵的黑客	370 万条
	14	ADP 税务福利信息泄密	2016 年 5 月	黑客，上次入侵获得用户数据的黑客	64 万条
	15	英国信用卡数据外泄	2015 年 8 月	黑客，直接入侵的黑客	240 万条
互联网	16	美团外卖信息泄露	2018 年 4 月	身份不详，调查进行中	数十万条
	17	58 同城简历数据泄露事件	2017 年 3 月	黑客，通过黑产软件	爬虫软件每小时可以采集数千份用户数据
	18	京东数据泄露门	2016 年 12 月	内部人员，2016 年底入职京东的试用期的网络工程师郑某鹏，黑产团伙的重要成员	数千万条
	19	优酷数据泄露事件	2016 年 –2017 年	黑客，长期持续撞库攻击的黑客	1 亿条
	20	网易邮箱数据泄露事件	2015 年 10 月	黑客，疑似拖库黑客	5 亿条
	21	腾讯 QQ 群数据库泄露	2013 年 11 月	黑客，业务漏洞获取权限的黑客	7000 万多个 QQ 群，12 亿 QQ 号

分类	序号	事件名称	事件时间	泄露人员	泄露数据量或非法所得
政府部门	22	南京公务员泄露居民信息	2018 年 1 月	内部人员，副主任科员刘某	82 万条
	23	明星购房信息泄露	2016 年 3 月	内部人员，青岛市不动产登记中心工作人员	明星购房信息
	24	国家旅游局安全事件	2015 年	外部不法分子	6000 万客户、6W+ 旅行社账
	25	12306 网站用户信息外泄事件	2014 年 12 月	黑客，撞库黑客	13 万条
	26	车管所违章记录被篡改	2014 年 11 月	合作开发方，公安车管系统软件供应商	1.4 万条
	27	国家宏观经济数据泄露	2010 年 –2011 年	内部人员，原国家统计局干部孙振、原中国人民银行干部伍超明、4 名证券行业从业人员	多次泄露
教育	28	学信网疑被拖库	2016 年 4 月	黑客，疑似拖库黑客	35G（蓝点网）
	29	教育考试信息泄露	2016 年 8 月	黑客，直接攻击的黑客	5 万
社保	30	篡改退休人员数据非法牟利	2010 年 –2011 年	内部人员，某市社保局退管中心蔡某、市社保局信息中心陈某	非法所得 280 万
	31	非法获得养老金	2005 年 –2008 年	内部人员，外部勾结；某区社保事业管理处副主任王某、某银行电脑维护员向某	非法所得 190.5 万
	32	冒领他人社保	2005 年 –2009 年	内部人员，某市社保局支付股股长胡某	非法所得 99 万
医疗	33	疾控中心信息泄露	2016 年 7 月	黑客	30 个省的 275 例
	34	上海新生儿信息外泄	2016 年 7 月	离职人员，韩某原是上海疾控中心工作人员，张某原是黄浦区疾控中心工作人员	20 万新生儿信息
金融	35	湖南某银行信息泄露	2016 年 10 月 14 日	内部人员，某农商支行行长夏某、中信银行员工戴某、韩某	50 万余份公民个人征信报告
	36	信诚人寿内控、信息安全均曝漏洞	2016 年	黑客，意图牟利的不法分子	千万客户信息
	37	工行快捷支付被曝存在严重漏洞	2015 年	黑客，截取短信验证码的犯罪分子	多起
其他	38	深网视界	2019 年 2 月	未做安全配置导致	680 万条个人数据
	39	国泰航空信息泄露事件	2018 年 10 月	原因在调查中	940 万乘客信息
	40	博士黑客贩卖公民信息	2018 年 4 月	内部人员，某国有大型科技公司数据库相关工作人员	500 余万条，60G 的容量

表 1　国内外数据泄露事件概要

就这些事件的分析来看，既有黑客的攻击，更有内部工作人员的信息贩卖、离职员工的信息泄露、第三方外包人员的交易行为、数据共享第三方的数据泄露、开发测试人员的违规等；究其原因既有安全意识的薄弱，也有由于安全体系的老旧或安全策略的过时而导致的数据泄露。

这些复杂的泄露途径无一不在证明：传统网络安全中以抵御攻击为中心、以黑客为防御对象的策略和安全体系构建存在重大的安全缺陷，传统网络安全为中心需要向以数据为中心的安全策略转变。

在过去的 2018 年，来自国际的一些权威机构发布的报告显示，2018 年全球公开披露的超过 6500 起数据泄露事件中，有三分之二来自商业部门，有 12 起数据泄露事件涉及人数超过 1 亿甚至更多。导致数据泄露的常见原因中，黑客攻击占据绝大多数，但因内部漏洞而导致数据泄露的事件记录远远超过黑客窃取。这些惨痛教训进一步证明了数据泄露途径的多样性。

1.3 数据安全相关法规和标准大爆发

安全事件层出不穷，企业资产和国家安全面临挑战，个人隐私大范围泄露，在数据高度发展的时代，这些都为社会的安定、个体自由与安全带来了巨大挑战。因此各国都相继出台了大量的法规，对个人、企业和国家重要数据进行保护。这里列出一些重要的法规包括：

欧盟在 2015 年出台，2018 年 5 月正式生效的一般数据保护条例，全称为《General Data Protection Regulation》（简称 GDPR）。

我国在 2016 年出台，2017 年 6 月 1 日正式生效的网络安全法，全称《中华人民共和国网络安全法》。

我国在 2018 年正式出台，5 月 1 日正式生效，个人信息安全规范，GB/T 35273《信息安全技术个人信息安全规范》。

我国已经在制定即将颁布的《数据出境管理办法》、《重要数据管理办法》、《中华人民共和国密码法》等。

2018 年进入立法阶段的《个人信息保护法》和《数据安全法》也被列入十三届全国人大常委会立法规划，2019 年呼之欲出。这两项法律的出台将对我国的个人隐私和关键数据安全起到关键性作用，为数据收集、存储、处理、传输、共享、删除等全生命周期管理的角度制定完善的法律体系。

2018 年，随着网络安全法的实施，和个人信息安全规范出台，很多国家重点行业通过制定相应的行业规范，来加强数据保护和监管。

分类	序号	内容
金融行业	1	商业银行信息科技风险管理指引
	2	金融和重要领域国产密码应用解决方案
	3	金融和重要领域国产密码应用试点工作实施方案
	4	金融和重要领域国产密码应用试点工作应急处置方案
	5	金融和重要领域国产密码应用试点工作密码应用方案审查要点
	6	金融行业信息系统信息安全等级保护测评指南
	7	银保会数据治理指引
	8	银行业金融机构数据治理指引
	9	证券公司集中交易安全管理技术指引
	10	证券公司全面风险管理规范
	11	证券期货业数据分类分级指引
	12	证券基金经营机构信息技术管理办法
	13	证券期货行业数据分类分级指引
	14	证券期货业信息安全保障管理办法
	15	证券期货业信息系统安全等级保护基本要求
	16	政务信息资源共享管理暂行办法
	17	中国银行业信息科技“十二五”发展规划监管指导意见
	18	中国银行业信息科技“十三五”发展规划监管指导意见
	19	中国人民银行办公厅关于开展支付安全风险专项排查工作的通知
	20	保险机构信息化监管规定
医疗	21	全国医院信息化建设标准与规范
	22	健康医疗信息安全指南
	23	区卫生健康信息化建设指南
运营商	24	中国移动大数据安全管控分类分级实施指南
	25	中国移动大数据安全脱敏实施指南
教育	26	教育部机关及直属事业单位教育数据安全管理规范
	27	教育部机关及直属事业单位教育数据管理办法
	28	教育行业等级保护定级指南
	29	教育信息化 2.0 文件
政府	30	政务信息资源共享管理暂行办法
	31	国密信息系统密码应用基本要求

表 2　各行业数据安全法律法规

这些行业规范都将对企业和政府单位的 IT 安全策略制定和安全体系的架构产生重要影响；在这些法规中都将数据作为了最为重要的防护对象，提出了重要的安全要求；对于这些法规的遵守将影响企业的声誉、合规甚至存亡。

我们也能够看到，随着国内外法律法规的制定和落地实施，2018 年，在很多大企业、组织和大量高速发展的企业中，数据安全问题和风险已经成为了企业风控部门，甚至是经营决策部门关心的问题之一，并且有越来越被重视的趋势。

1.4 数据安全建设需要有系统化思维和建设框架

随着数据安全的重要度提升，用户在这个方向的投资也在增大，据 KVB Research2017 年大数据安全报告预测显示，大数据安全上 2017 年全球投资达到 102 亿美金，并且以 17% 的年复合增长率在扩大，到 2023 年将达到 309 亿美金，也就是 2000 亿人民币。

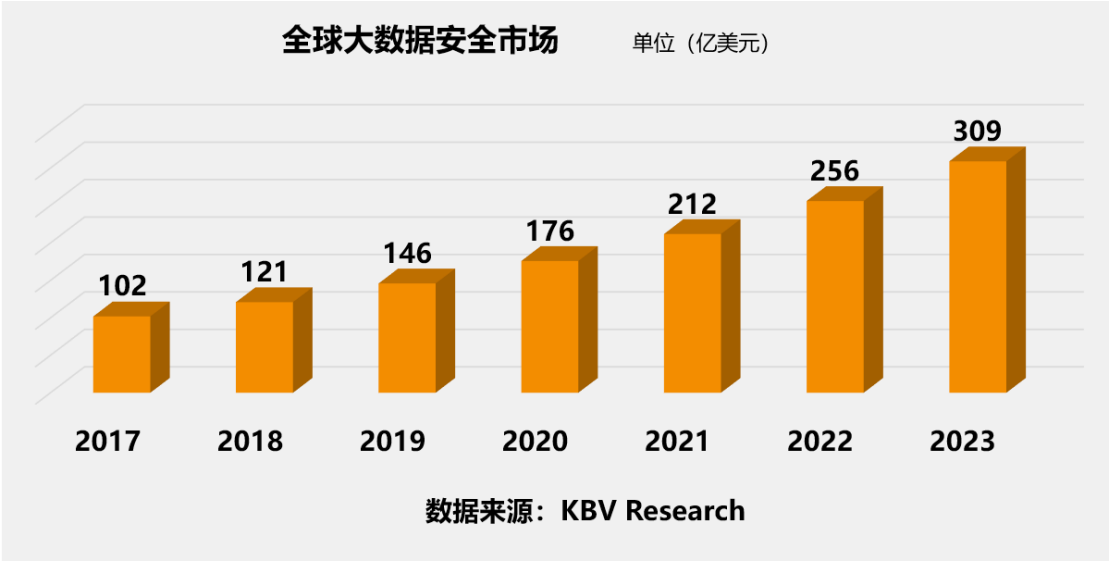


图 1 （KVB Research 在 big data security 上的市场预测）

而在我国随着网络安全法的出台，数据资产价值得到确认，政府机构和企业在这个方向的投资也在加大，以数据审计、脱敏和加密为目标的数据安全投资正在成为采购的热点。

当前这些采购大多以单独产品采购为主，这些采购的发起部门也各不相同。大型的 IT 组织正在陷入疑问，数据安全的建设是否有系统化的方法？是否要沿用传统的网络安全的处理策略，通过边界防护和防止攻击的方式来进行数据保护？数据安全的责任主体，是由数据存储所在的部门、数据处理的业务部门还是负责对数据进行运维的部门负责？这些不同的产品之间彼此割裂还是具有联动性质？这些产品的应用上应该采用什么样的安全措施等等，疑问丛生。

这些疑虑非常正常，因为数据与业务系统的高度融入，数据如何被使用、数据的价值更

被业务部门所识别；但是安全法规，又通常由单位或企业的安全或保密部门所负责；数据安全产品的采购和使用，需要系统化的方法，需要与数据处理的业务场景整合，既能保证数据使用行为不受影响，又能保证必要的安全措施能够得到保障。

数据安全治理的思路，正是这种将数据安全技术与数据安全管理融合在一起，综合业务、安全、网络等多部门多角色的诉求，总结归纳为系统化的思路和方法。

二. 数据安全治理基本理念

关于数据安全治理原则与框架，国际研究机构 Gartner 对此进行专属领域的研究，大型企业 Microsoft 从数据隐私合规角度也曾向市场提出隐私、保密和合规性的数据治理方案。从国际视角对此理解的基础上，我们在中国提出了数据安全治理理念与技术路线，填补了该理念在中国的空白，更有效推动实现该理念在国内的执行落地。

2.1 Gartner 数据安全治理理念

国际咨询机构 Gartner 认为数据安全治理不仅仅是一套用工具组合的产品级解决方案，而是从决策层到技术层，从管理制度到工具支撑，自上而下贯穿整个组织架构的完整链条。组织内的各个层级之间需要对数据安全治理的目标和宗旨取得共识，确保采取合理和适当的措施，以最有效的方式保护信息资源，这也是 Gartner 对“安全和风险管理”的基本定义。

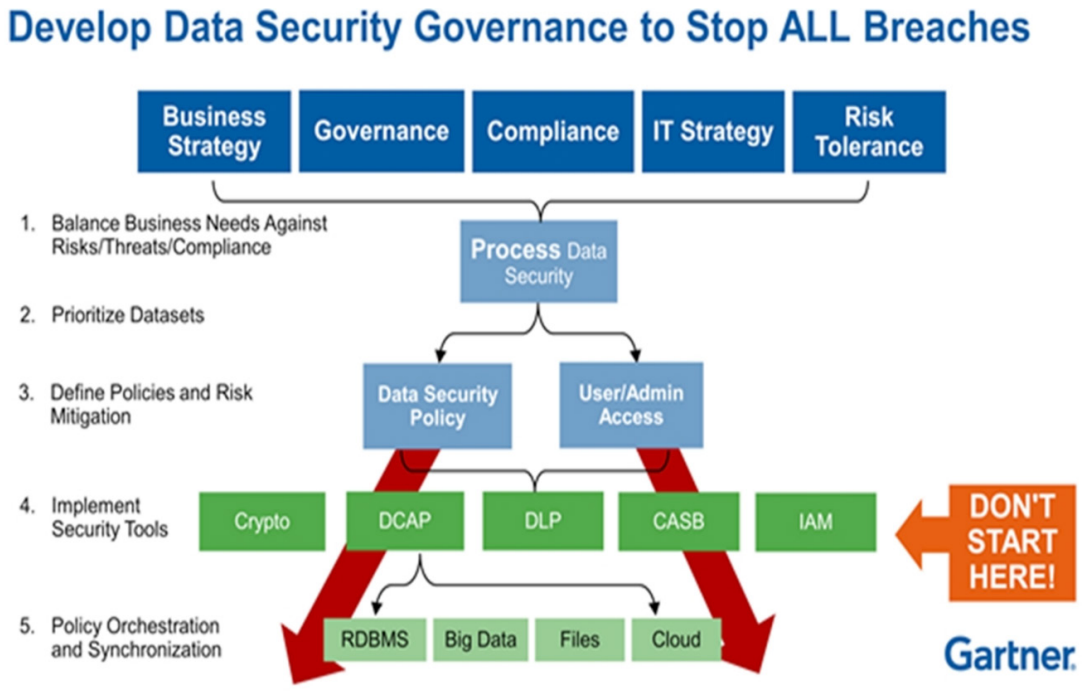


图 2　Gatner 数据安全治理框架

Step1：业务需求与安全（风险 / 威胁 / 合规性）之间的平衡

这里需要考虑 5 个维度的平衡：经营策略、治理、合规、IT 策略和风险容忍度，这也是治理队伍开展工作前需要达成统一的 5 个要素。

经营策略：确立数据安全的处理如何支撑经营策略的制定和实施

治理：对数据安全需要开展深度的治理工作

合规：企业和组织面临的合规要求

IT 策略：企业的整体 IT 策略同步

风险容忍度：企业对安全风险的容忍度在哪里

Step2：数据优先级

进行数据分级分类，以此对不同级别数据实行合理的安全手段。

Step3：制定策略，降低安全风险

从两个方向考虑如何实施数据安全治理，一是明确数据的访问者（应用用户 / 数据管理人员）、访问对象、访问行为；二是基于这些信息制定不同的、有针对性的数据安全策略。

Step4：实行安全工具

数据是流动的，数据结构和形态会在整个生命周期中不断变化，需要采用多种安全工具支撑安全策略的实施。Gartner 在 DSG 体系中提出了实现安全和风险控制的 5 个工具：Crypto、DCAP、DLP、IAM，这 5 个工具是指 5 个安全领域，其中可能包含多个具体的技术手段。

Step5：策略配置同步

策略配置同步主要针对 DCAP 的实施而言，集中管理数据安全策略是 DCAP 的核心功能，而无论访问控制、脱敏、加密、令牌化，哪种手段都必须注意对数据访问和使用的安全策略保持同步下发，策略执行对象应包括关系型数据库、大数据类型、文档文件、云端数据等数据类型。

2.2 Microsoft 的 DGPC 理念

由微软开发的隐私、保密和合规性（DGPC）框架的数据治理计划，是为了企业和组织能够以统一、跨学科的方式来实现以下三个目标，而非组织内不同部门独立解决这三个不同的问题：

1）传统的 IT 安全方法侧重于 IT 基础设施，通过边界安全与终端安全进行保护。重点应该加强对存储数据的保护，并随基础设施移动，加强保护；

2）隐私相关的保护措施必须超越与安全重叠的隐私保护措施，包括：重点获取、保护和执行客户对如何及何时收集、处理或第三方共享的行为保护措施；

3）数据安全和数据隐私合规责任需要通过一套统一的控制目标和控制行为，进行合理化处理，以满足合规。

DGPC 框架与企业现有的 IT 管理和控制框架（如 COBIT）以及 ISO / IEC 27001/27002 和支付卡行业数据安全标准（PCI DSS）等安全标准协同工作。DGPC 框架围绕三个核心能力领域组织，涵盖人员、流程和技术三个部分：

1. 人员

第一步是建立一个 DGPC 团队，由组织内的个人组成，并给予他们明确规定的角色和职责，为履行其所需职责提供充足的资源，并就整体数据治理目标提供明确的指导。

2. 流程

有了合适的人参与 DGPC 的工作，组织就可以专注于定义流程。首先，检查各种权威性文件（法律，法规，标准，公司政策和战略文件），明确必须满足的要求。其次，确定指导原则和政策，以产生适合这些要求的环境。最后，组织应该在特定数据流的场景下识别威胁数据安全，隐私和合规的风险所在，分析相关风险并确定适当的控制对象和行为。

3. 技术

Microsoft 开发了一种技术方法来分析特定的数据流，并识别信息安全管理系统和控制框架的更广泛的保护措施可能无法解决的剩余流量特定风险。这种方法具体落到风险 / 差距分析矩阵模型中。该模型围绕三个要素构建：信息生命周期，四个技术领域以及组织的数据隐私和保密原则。

A、信息生命周期

为了识别安全风险并选择合适的技术措施和行为来保护机密数据，组织必须首先了解信息如何在整个系统中流动，以及信息如何在不同阶段被多个应用程序和人为了不同目的被访问和处理。

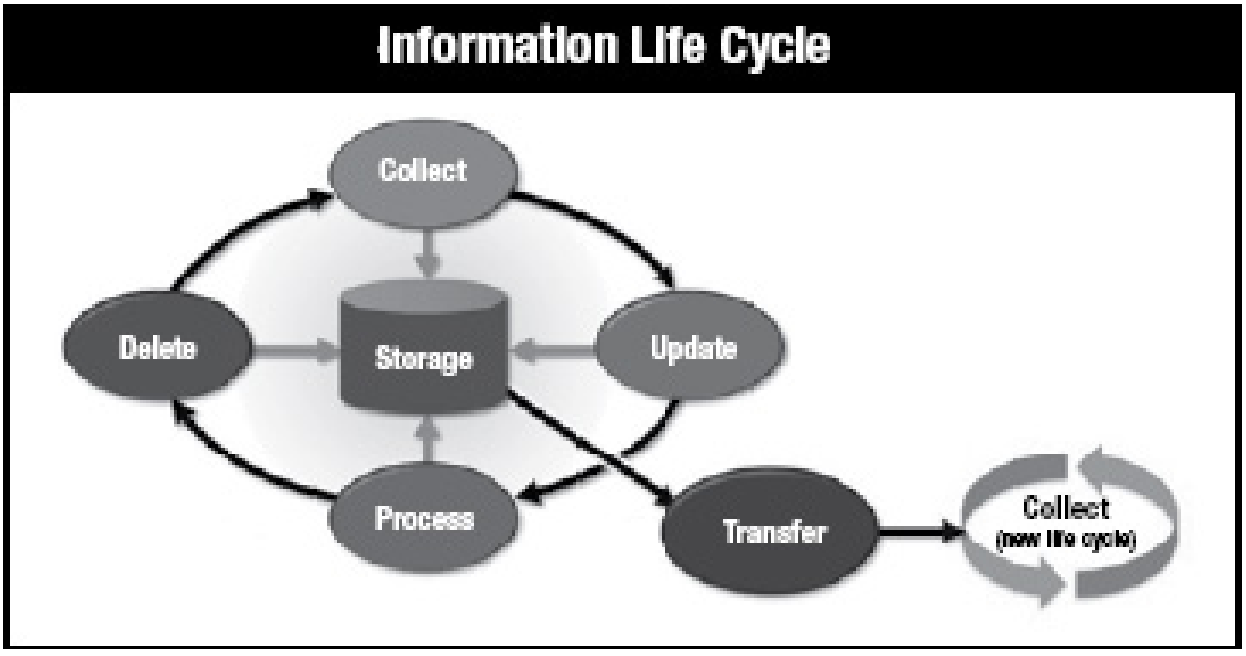


图 3　信息生命周期

B、四个技术领域

组织还需要系统评估保护其数据机密性、完整性和可用性的技术是否足以将风险降低到可接受的水平。以下技术领域为此任务提供了一个参考框架：

- 安全的基础架构：保护机密信息需要技术基础架构，可以保护计算机、存储设备、操作系统、应用程序和网络免受恶意软件、黑客入侵和内部人员窃取。
- 身份和访问控制：身份和访问管理技术有助于保护个人信息免受未经授权的访问，同时促进合法用户的可用性。这些技术包括认证机制，数据和资源访问控制，供应系统和用户账户管理。从合规角度来看，IAM 功能使组织能够准确地跟踪和执行整个企业的用户权限。
- 信息保护：机密数据需要持续保护，因为它们在组织内部和组织内共享。组织必须确保其数据库、文档管理系统、文件服务器和实践在整个生命周期内正确分类和保护机密数据。
- 审计和报告：遵从性控制的系统管理、监控与自动化审计对验证系统和数据访问控制是否有效，这些对于识别可疑或不合规的行为十分有用。

C、数据隐私和保密原则

以下 4 项原则旨在帮助组织选择能够保护其机密数据资产的技术和行为，以指导风险管理和决策过程。

- 原则 1：在整个机密数据使用期限内遵守政策。这包括承诺按照适用的法规和条例处理所有数据，保护隐私并尊重客户的选择和意愿，允许个人在必要时审查和更正其信息。
- 原则 2：尽量减少未经授权的访问或滥用机密数据的风险。信息管理系统应提供合理的管理、技术和物理保障，以确保数据的机密性、完整性和可用性。
- 原则 3：尽量减少机密数据丢失的影响。信息保护系统应提供合理的保护措施，如加密，以确保遗失或被盗数据的机密性。应制定适当的数据泄露应对计划和升级路径，所有可能参与违规应对的员工都应接受培训。
- 原则 4：记录适用的控制措施并证明其有效性。为帮助确保问责制，组织应遵守数据隐私和保密原则，应通过适当的监督、审计和控制措施的使用来加以验证。此外，组织应该有一个报告违规行为和明确定义的升级路径的流程。

D、风险 / 差距分析矩阵

该工具可帮助组织识别并解决现有保护工作的缺失：针对特定数据流中的隐私、机密和合规威胁的数据安全。该矩阵提供了数据现有和未来的保护技术、措施和行为，形成了统一视图。

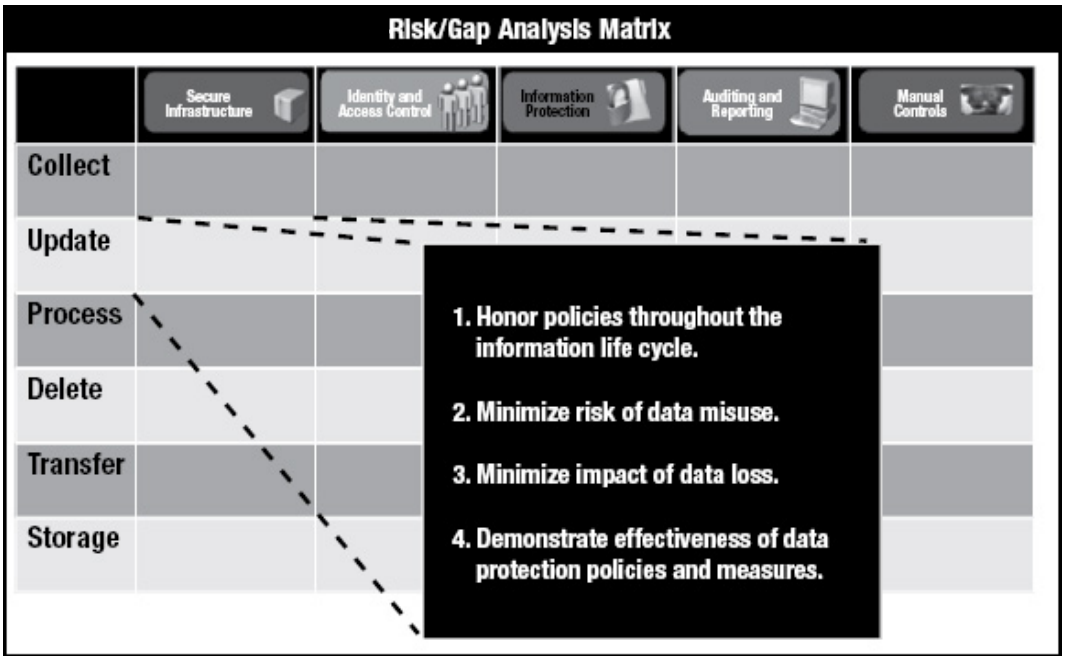


图 4　风险 / 差距分析矩阵

每一行描绘了信息生命周期中的一个阶段。矩阵中的前四列表示一个技术领域，而最右边的列表示控制行为，这些行为措施必须在信息生命周期的每个阶段满足四种数据隐私和保密原则的要求。

2.3 数据安全治理概论

在本白皮书里，综合了国际相关框架模型和我国一些具体的安全实践后，提出的一套在中国易于落地的数据安全建设的体系化方法论。

数据安全治理是以“让数据使用更安全”为目的的安全体系构建的方法论，核心内容包括：

（1）满足数据安全保护（Protection）、合规性（Compliance）、敏感数据管理（Sensitive）三个需求目标；

（2）核心理念包括：分级分类（Classfiying）、角色授权（Privilege）、场景化安全（Scene）；

（3）数据安全治理的建设步骤包括：组织构建、资产梳理、策略制定、过程控制、行为稽核和持续改善；

（4）核心实现框架为数据安全人员组织（Person）、数据安全使用的策略和流程（Policy & Process）、数据安全技术支撑（Technology）三大部分。

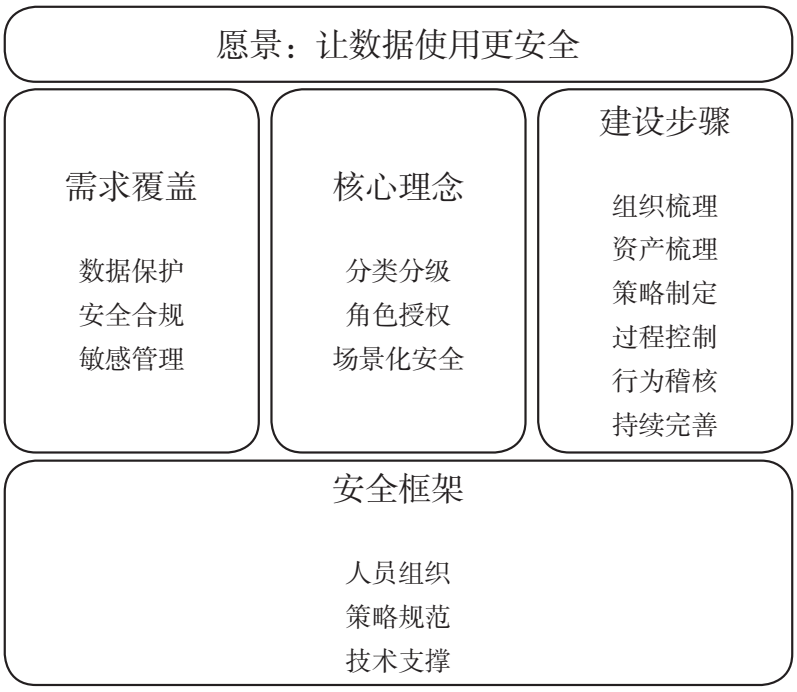


图 5　数据安全治理理念框架

2.3.1 数据安全治理的愿景

在这里，首先要强调的是，数据安全治理的目标是“数据安全使用”，我们不谈脱离了“使用”的安全，数据存在的目的就是为了使用，如果不是基于这个前提而谈的安全，最终有可能产生无法落地或者即使落地，也会差强人意。

2.3.2 数据安全治理的需求目标

围绕“让数据使用更安全”的愿景，数据安全治理覆盖了安全防护、敏感信息管理、合规三大目标；这三个目标比我们过去以防黑客攻击和满足合规性两大安全目标，更为全面和完善。过去二十多年信息化和互联网经济的发展，数据成为继现金和技术之后又一核心价值资产；数据黑产在过去十年里蓬勃发展，让每个人、每个企业和国家的数据都面临着巨大威胁；只有合理地处理好数据资产的使用与安全，企业与国家才能在新的数据时代稳健而高速发展。对于敏感数据的安全管理和使用，是数据安全治理的核心主题。

2.3.3 数据安全治理的核心理念

数据安全治理的核心理念包括：

数据的分级分类：首先是来自对数据的有效理解和分析，对数据进行不同类别和密级的划分；根据数据的类别和密级制定不同的管理和使用原则，尽可能对数据做到有差别和针对性的防护，实现在适当安全保护下的数据自由流动。

角色授权：在数据分级和分类后，重要的是要了解这些数据在被谁访问，这些人是如何

使用和访问数据的，要针对不同的角色制定不同的安全政策。常见的角色包括：业务人员（要进一步角色细分）、数据运维人员、开发测试人员、分析人员、外包人员、数据共享第三方等。

场景化安全：要针对不同角色在不同场景下，研究主要的数据使用需求；要在尽可能满足数据被正常使用的目标下，完成相应的安全要求和安全工具的选择。比如对于开发测试人员，在开发场景下，主要需要满足对生产数据的高度仿真模拟，对于仿真数据的加密、访问控制、审计等安全措施并非重要。对于运维人员，在备份和调优场景下，并不需要什么？提供行为审计、敏感数据掩码能力即可。

2.3.4 数据安全治理建设与演进模型

为了有效地实践数据安全治理过程，我们需要一个系统化的过程完成数据安全治理的建设，如下图：

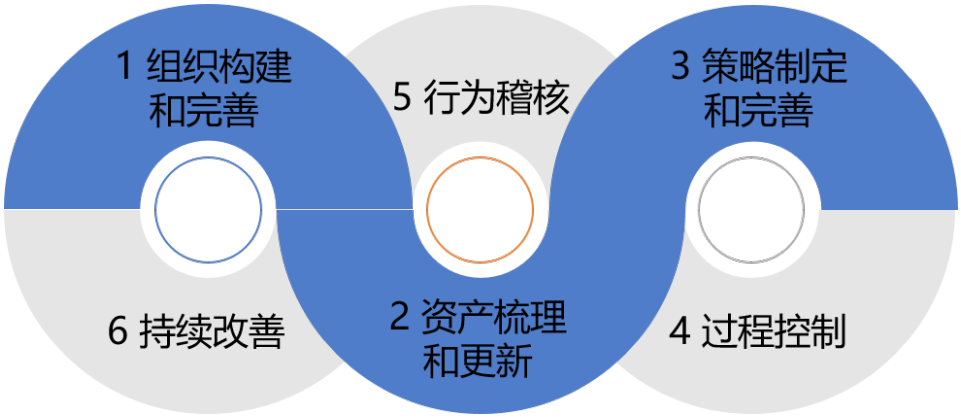


图 6　数据安全治理建设体系

组织构建：在数据安全治理中，首要任务是成立专门的安全治理团队，保证数据安全治理工作能够长期持续的得以执行。同时数据安全治理要明确数据治理相关的工作部门和角色（受众），使数据治理工作能够有的放矢。组织的构建规模和形式可以灵活，可大可小，最关键的是有专门的团队，以及能够调用多方部门协同参与到数据安全治理工作中。

资产梳理：在队伍构建后，重要的是对企业中的数据资产进行盘点，了解企业中都有哪些数据，这些数据中都有哪些是与外部合规有关的，哪些是企业的重要数据资产，这些数据是被谁访问的，这些数据是如何被访问的；

策略制订：根据梳理的情况，要对数据进行分级分类，要对人员进行角色划分，要对角色对数据使用的场景进行限定，要对这些场景下的安全策略和措施进行规定。

过程控制：不同的角色团队，要在日常的管理、业务执行和运维工作中，将相关的流程规定落地执行，要采用相对应的数据安全支撑工具，在办公和运维的过程中将这些工具进行融入。

行为稽核：要对数据的访问过程进行审计，要判断这些数据访问行为过程是否符合所制

定的安全策略；要对数据的安全访问状况进行深度评估，看在当前的安全策略有效执行的情况下，是否还有潜在的安全风险。

持续改善：对当前的数据资产情况进行进一步的梳理，看是否有增加的资产或访问角色；对稽核的情况进行梳理，看是否有未纳入管理的数据访问行为；观测最新的相关安全规范的变化情况，看是否有需要新增或移除的外部安全策略；了解企业新的业务系统或组织结构，看数据的访问权限和行为方式是否改变；根据以上情况，改组当前的数据安全组织结构，修订当前企业的数据安全策略和规范，持续保证安全策略的落地。

2.3.5 数据安全治理框架

在数据安全治理的框架中，需要建立专门的安全治理团队，保证数据安全治理工作能够长期持续的得以执行，组织落地是有效开展数据安全治理工作的基础。数据安全治理团队要覆盖到安全、业务、运维等多个部门。

数据安全治理的策略和流程，要以文件的形式明确企业（组织）内部的敏感数据有哪些，敏感数据进行分类和分级，对不同类别和级别的敏感数据的管理控制原则，不同的工作部门和角色所具有的权限，数据使用的不同环节所要遵循的控制流程。

数据安全治理的技术支撑，是要明确在数据安全治理的过程中，要采用什么样的技术工具帮助完成数据安全治理工作。包括早期策略制定前的数据梳理工具，数据访问过程控制中，采用什么样的技术手段帮助实现数据的安全管理过程，以及在后期对数据安全治理工作进行稽核的过程中采用什么样的技术工具进行辅助监管。这些技术手段可以包括数据的梳理、数据的访问控制、数据的加密、数据的脱敏、数据的水印、数据的隔离、数据的防注入、数据的审计、数据访问的风险分析等。

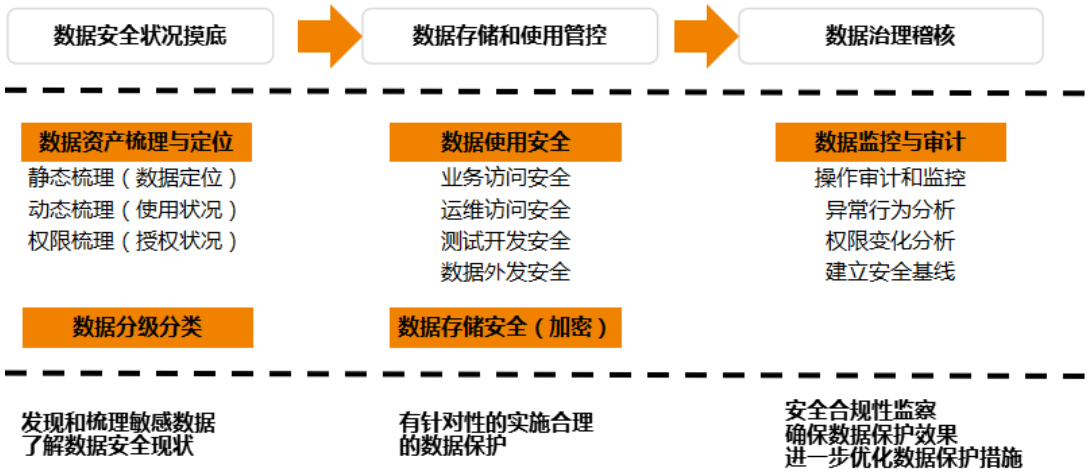


图 7　数据安全治理框架

2.3.6 数据安全治理与传统安全概念的差异

为了更加有效地理解数据安全治理概念与传统数据安全的差异，我们可以与传统安全理

念进行一个比较：

差异对比	数据安全治理	传统安全
目标方面	以数据的安全使用为目标	以数据的安全防护，不受攻击为目标
对象方面	面向内部或准内部人员，以这些人员行为的安全管控为主要对象	面向外部黑客，以对外部黑客或入侵者的防控为主要对象
理念方面	以数据分级分类为基础，以信息合理、安全流动为目标	以区域隔离、安全域划分为目标
手段方面	以信息使用过程的安全管理和技术支撑为手段	以边界防护为主要安全手段
融合方面	安全产品技术和流程管理深度整合	管理与技术相对分离

表 3　数据安全治理与传统数据安全的差异对比

当然数据安全治理并非是要取代传统安全体系，数据安全治理是在传统网络安全体系的基础上有效地实现对数据的安全管控；数据安全是在网络安全提供的有效边界防御的基础上完成对数据的高层安全保障。

2.4 数据安全治理与数据安全成熟度模型

数据安全成熟度模型（简称：DSMM）是另一个数据安全建设中的系统化框架，是围绕数据的生命周期、结合大数据业务的需求以及监管法规的要求，持续不断的提升组织整体的数据安全能力，以数据为核心的安全框架。

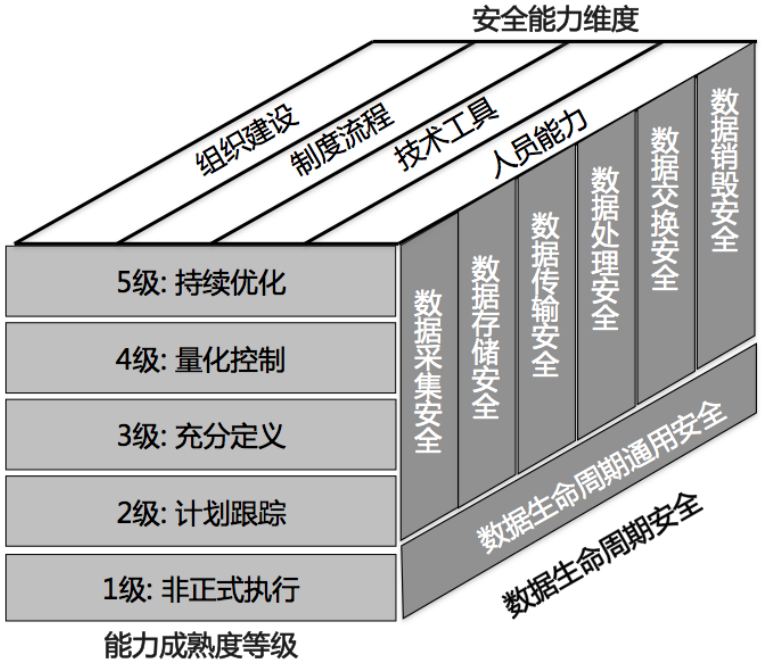


图 8　DSMM 核心框架图

模型包含以下三个维度：

1）数据生命周期安全：围绕数据生命周期，提炼出大数据环境下，以数据为中心，针对数据生命周期各阶段建立的相关数据安全过程域体系。

2）安全能力维度：明确组织机构在各数据安全领域所需要具备的能力维度，明确为制度流程、人员能力、组织建设和技术工具四个关键能力的维度。

3）能力成熟度等级：基于统一的分级标准，细化组织机构在各数据安全过程域的 5 个级别的能力成熟度分级要求。

DSMM 模型与 DSG 理论之间既有相同，又有区别；两个安全体系都强调以数据为中心建立系统化的数据安全体系，在数据安全的建设上，都不是强调唯技术论，都强调组织建设、制度流程和技术工具的综合作用。

但 DSG 和 DSMM 有以下重要区别：

1）DSG 是以数据的分级分类为核心，进行安全策略的设定；DSMM 是以数据的生命周期为核心，寻求安全策略的覆盖；

2）DSG 体系化建议了数据使用或服务的人员的角色，根据角色对数据使用的主要场景，提供建议的安全措施以及所要使用的安全工具；而 DSMM 更多的是提供一种评估方法，看数据使用的过程中，企业是否定义了明确的控制措施，并无具体化的方法推荐；

3）DSG 并不那么强调数据的生命周期，DSG 反对在数据的生命周期中不区分化的安全措施，DSG 强调针对数据使用场景，满足数据使用需求后的针对性安全措施；比如在开发测试环境，需要采用脱敏的技术获得高仿真数据，在这种场景下不强调审计、管控和加密等措施；

4）在 DSG 体系中，将安全体系的构建，明确归纳为安全政策的制定，技术支撑平台的建设，安全政策执行有效性的监督，安全政策的改善这一持续循环过程；而 DSMM 对安全成熟度进行了等级化分级，将持续改善定义为了最高级别；在 DSG 的理念中，无论完成了多少的安全建设，持续改善都是一个标准动作。

5）从本质上讲，DSG 更像一种方法论，帮助企业如何迅速构建一套行之有效的数据安全体系；而 DSMM 更像一种评估方法，像一个考试，让企业或监管机构来评价企业当前的安全建设状态。

2.5 数据安全治理与数据治理

信息系统建设发展到一定阶段，数据资源将成为战略资产，而有效的数据治理才是数据资产形成的必要条件。

数据治理是指从使用零散数据变为使用统一数据、从具有很少或没有组织和流程治理到

企业范围内的综合数据治理、从尝试处理数据混乱状况到数据井井有条的一个过程。

数据治理的作用就是确保企业的数据资产得到正确有效的管理，数据治理从组织架构、原则、过程和规则等方面确保数据管理的各项职能得到正确的履行。

数据治理其实是一种体系，是一个关注于信息系统执行层面的体系，这一体系的目的是整合 IT 与业务部门的知识和意见，通过一个类似于监督委员会或项目小组的虚拟组织对企业的信息化建设进行全方位的监管，这一组织的基础是企业高层的授权和业务部门与 IT 部门的建设性合作。从范围来讲，数据治理涵盖了从前端事务处理系统、后端业务数据库到终端的数据分析，从源头到终端再回到源头形成一个闭环负反馈系统（控制理论中趋稳的系统）。从目的来讲，数据治理就是要对数据的获取、处理、使用进行监管（监管就是我们在执行层面对信息系统的负反馈），而监管的职能主要通过以下五个方面的执行力来保证——发现、监督、控制、沟通、整合。

从严格意义上来看，数据安全治理是数据治理中的一个过程，在今天对数据资产高度重视和个人隐私数据高度监管的年代，数据安全治理更应该是数据治理的一个重要组成部门。

但从实际操作上来看，两者之间又有很大的不同：

1）从发起部门来看，数据治理主要是由 IT 部门在驱动；数据安全治理主要是由安全合规部门在驱动。当然两者的成功都要涉及到业务、运维和管理部门甚至公司最高管理决策层。

2）从目标上看：数据治理的目标是数据驱动商业发展，提升企业数据资产价值。而数据安全治理的目标让数据使用中更安全，保障数据的安全使用和共享，实质也是保障数据资产价值。

3）从工作内容产出上看：数据治理工作产出上，一个核心成果就是数据质量提升，通过数据的清洗和规范的过程，获得有质量的数据。而数据安全治理的重要产出，就是完成对企业数据访问的安全策略的分级分类，完成企业对数据的合规安全访问政策和措施。

4）从数据资产梳理上：数据治理的资产梳理的主要产出物，就是元数据。元数据管理，即赋予数据上下文和含义的参考框架。而数据安全治理中的资产梳理，要明确数据分级分类的标准，敏感数据资产的分布，敏感数据资产的访问状况和授权报告。

5）当然，在当前的数据治理中也逐渐在加大对数据安全上的一些要求，但相对而言还属于从属角色，不那么系统化；这就如同信息安全在 IT 建设中的关系一样。

三. 数据安全治理的组织建设

数据安全治理首先要成立专门的数据安全治理机构，以明确数据安全治理的政策、落实

和监督由谁长期负责，以确保数据安全治理的有效落实。成立的机构可以称为数据安全治理委员会或数据安全治理小组，机构的成员由数据的利益相关者和专家构成，这个机构通常是一个虚拟的机构，这里之所以称之为利益相关者，是因为这些人不仅仅是数据的使用者，可能是数据本身的代表者（比如用户），数据的所有者，数据的责任人。数据安全治理委员会或数据安全治理小组，这个机构本身既是安全策略、规范和流程的制定者，也是安全策略、规范和流程的受众。

DGPC 框架中，该机构一般称之为 DGPC 团队，或者叫 Data Stewards:

这个团队的职责是负责制定数据分类、保护、使用和管理的原则、策略和过程；

这个团队的构成是 IT、人资、法律、财务、业务和市场部门等所有参与人、知识产权、私密信息相关的部门；在一些大型的机构中甚至要包括主管的副总裁、董事会成员，因为数据安全问题，逐渐变成对企业生死相关的问题。

数据安全治理的人员中另一个关键角色就是数据安全的受众，这些受众是数据安全策略、规范和流程的执行者和被管理者；包括了数据的使用者、管理者、维护者、分发者；大多数数据利益相关者都属于数据安全治理的受众；将这些人员纳入到这个组织中，才能够使数据安全治理过程中制定的安全原则、安全措施和安全规范在具体执行中被有效地贯彻落地。

只有有效地构建一个涵盖业务、管理、安全、执行等部门的数据安全治理组织机构，才能做到业务和安全的有效平衡。

但数据安全治理的早期启动，可以由业务或安全部门来发起，逐渐完备整个组织的构成。

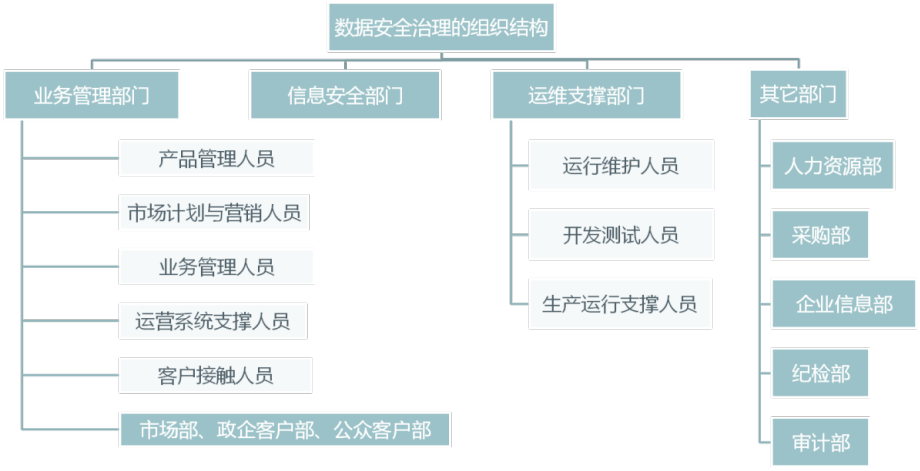


图 9　某运营商的数据安全治理的相关组织和角色结构图

（注：其中深色是部门，浅色是角色，这个结构中可以看到覆盖了业务、安全、运维和企业的相关管理支撑部门。）

四. 数据安全治理规范制定

在整个数据安全治理的过程中，最为重要的是实现数据安全策略和流程的制定，在企业

或行业内经常被作为《某某数据安全管理规范》进行发布，所有的工作流程和技术支撑都是围绕着此规范来制定和落实。但这个规范的出台往往需要经过大量的工作才能完成，这些工作通常包括：

A、梳理出组织所需要遵循的外部政策，并从中梳理出与数据安全管理相关的内容；

B、根据该组织的数据价值和特征，梳理出核心数据资产，并对其分级分类；

C、理清核心数据资产使用的状况（收集、存储、使用、流转）；

D、分析核心数据资产面临的威胁和使用风险；

E、明确核心数据资产访问控制的目标和访问控制流程；

F、制订出组织对数据安全规范落实和安全风险进行定期的核查策略；

G、整个策略的技术支撑规范。

4.1 外部所要遵循的策略

在我国，数据安全治理同样需要遵循国家级的安全政策和行业内的安全政策。

举例如下：

网络安全法

《中华人民共和国网络安全法》(以下简称：网络安全法)，由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于 2016 年 11 月 7 日通过并公布，自 2017 年 6 月 1 日起施行。

在该报告明确地对个人隐私数据和国家重要数据提出了保护要求，其中包含一些具体化的措施要求，比如：

（1）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（2）采取数据分类、重要数据备份和加密等措施；

该法案，对中国所有政府单位和企业的 IT 系统建设、数据采集和应用产业造成深远影响；并随之配套产生的《数据出境管理办法》、《个人隐私数据管理办法》、《大数据安全标准》等，将对数据安全行业的发展产生重要影响。

等级保护政策

全称为《信息安全等级保护管理办法》规定，由公安部牵头推动，国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

所有的政府单位、央企、金融单位、互联网企业等都将接受该管理办法的约束；等级保护在过去的 10 年中，是我国信息安全建设中最重要的需要遵循的法规。

GDPR

GDPR 即《通用数据保护条例》是欧盟在 2015 年颁布，2018 年 5 月 25 日正式实施，堪称史上最严格的数据保护法案：

GDPR 第八十三条规定了对不同违法行为的处罚标准：

1）对未采取技术或管理措施来避免、降低隐私侵权损害的数据控制者或处理者，最高可处以 1000 万欧元或全球营业额的 2%（以较高者为准）作为罚款。

2）对违反个人数据收集和处理原则，没有保障数据主体权利的数据控制者或处理者，最高可处 2000 万欧元或全球营业额的 4%（以较高者为准）作为罚款。

第三条第一款规定，只要数据的控制者或处理者在欧盟境内设有办公地点，无论收集数据和使用数据的行为是否发生在欧盟境内，都要遵守 GDPR 法案。哪怕只有一个人的办事处也属于适用范围。

第三条第二款还规定，在两种特殊情形下，只要是数据控制者或处理者收集或使用了欧盟内数据主体的个人数据，即使并未在欧盟境内设有办公地点，也要遵守 GDPR，这两种特殊情形是：

1）向欧盟内的数据主体提供商品或服务，无论是有偿还是无偿。

2）对欧盟内的数据主体在欧盟境内的行为进行监控的组织。

这一条款对于在华的与欧盟有关的外企，进军欧盟的中国企业，特别是互联网企业来说非常重要。

个人信息安全管理规范

国家编制的 GB/T 35273–2017《信息安全技术 个人信息安全规范》于 2018 年 5 月 1 日实施。该规范主要针对个人信息面临的安全问题，规范了个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄露等乱象，最大程度地保障个人的合法权益和社会公共利益。例如：

规范第六章“个人信息的保存”中指出：

“收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别个人的信息分开存储，并确保在后续的个人信息处理中不重新识别个人。”

该规范第七章“个人信息访问控制措施”也提出了对个人信息控制者的要求：

a）对被授权访问个人信息的内部数据操作人员，应按照最小授权的原则，使其只能访问职责所需的最少够用的个人信息，且仅具备完成职责所需的最少的数据操作权限；

b）宜对个人信息的重要操作设置内部审批流程，如批量修改、拷贝、下载等；

c）应对安全管理人员、数据操作人员、审计人员的角色进行分离设置；

d）如确因工作需要，需授权特定人员超权限处理个人信息的，应由个人信息保护责任人或个人信息保护工作机构进行审批，并记录在册；

上述两条规定，明确提出了针对个人信息的“数据脱敏”要求、“数据管控”要求和数据获取过程中的“内部审批”要求。

银行业金融机构数据治理指引

2018 年 5 月，中国银行保险监督管理委员会颁布了《银行业金融机构数据治理指引》，适用范围涉及银监局、各股份制银行、政策性银行、外资银行和金融资产管理公司。

该文件明确要求银行业金融机构应当将数据治理纳入公司治理范畴，并建立自上而下、协调一致的数据治理体系。具体执行上应遵循如下原则：

（1）数据生命周期全面覆盖原则；

（2）业务规模匹配原则；

（3）数据治理持续化开展原则；

（4）数据真实有效性原则；

该文件分别从数据治理架构、数据管理、数据质量控制、数据价值实现、监督管理等方面，规范了银行业金融机构的数据管理活动。

其它重要或行业相关的政策要求举例：

a）个人信息安全管理规范

b）中央企业商业秘密保护暂行规定

c）银行业金融机构数据治理指引

d）PCI-DSS、Sarbanes-Oxley Act（SOX 法案）、HIPPA

4.2 数据的分级分类

只有对数据进行有效分类，才能避免一刀切的控制方式，在数据的安全管理上采用更加精细的措施，使数据在共享使用和安全使用之间获得平衡。

（1）数据分级分类的原则：

分类：依据数据的来源、内容和用途对数据进行分类；

分级：按照数据的价值、内容敏感程度、影响和分发范围不同对数据进行敏感级别划分。

（2）数据分级分类方式

根据梳理出的备案数据资产，进行敏感数据的自动探测，通过特征探测定位敏感数据分布在哪些数据资产中；

针对敏感的数据资产进行分级分类标记，分类出敏感数据所有者（部门、系统、管理人员等）；

根据已分类的数据资产由业务部门进行敏感分级，将分类的数据资产划分公开、内部、敏感等不同的敏感级别。

下面是某运营商对数据分级分类的结果：

信息类别	信息项	分类信息内容
客户基本资料	政企客户资料	政企客户负责人信息、联系人信息、单位成员个人基本信息、业务合同、银行扣费帐户、政企客户编号、政企客户名称等
	个人客户资料	客户姓名、证件类型、证件号码、证件影印件、客户职业、工作单位、居住地址、联系地址、联系电话、银行扣费帐户、客户编号、年龄、性别等
	各类特殊名单	黑白红名单、钻金银名单等
身份鉴权信息	用户密码	用户服务密码、协同通信密码、189 邮箱密码、有线宽带密码等
客户通信信息	详单	语音、短信、彩信和上网详单等，内含主叫号码、主叫位置、被叫号码、时间等
	账单	每月出账的固定费用、通信费用、数据费用、代收费用
	客户当前位置信息	精确位置信息 (如小区代码、基站号、基站经纬度坐标等)
	客户消费信息	停开机、入网时间、在网时间、积分、预存款、信用等级、信用额度等
客户通信内容信息	客户通信内容记录	短信、彩信、协同通信、手机邮箱等通信内容
	移动上网内容及记录	移动上网访问内容、上传下载、客户端软件通信记录

表 4　数据分类表

信息类别	信息项	对三方价值	事故影响	分级定义
客户基本资料	政企客户资料	牟取暴利	造成政企客户流失、损失巨大	机密数据
	个人客户资料	价值较大	造成客户损失、损失大	敏感数据
	各类特殊名单	牟取暴利	造成投诉、损失大	敏感数据
身份鉴权信息	用户密码	牟取暴利	造成客户损失、损失巨大	机密数据
客户通信信息	详单	价值较大	造成投诉、损失大	敏感数据
	账单	价值一般	损失一般	普通数据
	客户当前位置信息	价值较大	损失一般	敏感数据
	客户消费信息	价值一般	损失一般	普通数据
	订购关系	价值低	无明显损失	普通数据
	增值业务订购关系	价值低	无明显损失	普通数据
	增值业务信息	牟取暴利	造成客户损失、损失大	敏感数据
客户通信内容信息	客户通信内容记录	牟取暴利	客户私密信息泄露，损失巨大	机密数据
	移动上网内容及记录	价值低	损失一般	普通数据
	增值业务客户行为记录	价值低	客户私密信息泄露，损失大	敏感数据
	领航平台交互信息	牟取暴利	损失一般	敏感数据

表 5　数据分级表

4.3 数据资产及使用状况的梳理

4.3.1 数据使用部门和角色梳理

在数据资产的梳理中，需要明确这些数据如何被存储，需要明确数据被哪些部门、系统、人员使用，数据被这些部门、系统和人员如何使用。对于数据的存储和系统的使用，往往需要通过自动化的工具进行；而对于部门和人员的角色梳理，更多是要在管理规范文件中体现。

对于数据资产使用角色的梳理，关键是要明确在数据安全治理中不同受众的分工、权利和职责。

组织与职责，明确安全管理相关部门的角色和责任，一般包括：

安全管理部门：制度制定、安全检查、技术导入、事件监控与处理；

业务部门：业务人员安全管理、业务人员行为审计、业务合作方管理；

运维部门：运维人员行为规范与管理、运维行为审计、运维第三方管理；

其它：第三方外包、人事、采购、审计等部门管理。

对于数据治理的角色与分工，需要明确关键部门内不同角色的职责，一般包括：

安全管理部门：政策制定者、检查与审计管理、技术导入者

业务部门：根据单位的业务职能划分

运维部门：运行维护、开发测试、生产支撑

4.3.2 数据的存储与分布梳理

敏感数据分布在哪里，是实现管控的关键。

只有清楚敏感数据分布在哪里，才能知道需要实现怎样的管控策略；比如，针对数据库这个层面，掌握数据分布在哪个库、什么样的库，才能知道对该库的运维人员实现怎样的管控措施；对该库的数据导出实现怎样的模糊化策略；对该库数据的存储实现怎样的加密要求。

4.3.3 数据的使用状况梳理

在清楚了数据的存储分布的基础上，还需要掌握数据被什么业务系统访问。只有明确了数据被什么业务系统访问，才能更准确地制定这些业务系统的工作人员对敏感数据访问的权限策略和管控措施。

大类	原有信息分类	包含的客户信息
业务支撑	BOSS	政企客户资料、个人客户资料、各类特殊名单、用户密码、详单、账单、客户消费信息、基本业务订购关系、增值业务（含数据业务）订购关系、增值业务信息、统计报表、渠道及合作伙伴资料、资源数据
	EDA	政企客户资料、个人客户资料、各类特殊名单、用户密码、详单、账单、客户消费信息、基本业务订购关系、增值业务（含数据业务）订购关系、增值业务信息、统计报表、渠道及合作伙伴资料、资源数据
	客户服务平台	可获取的信息：详单、客户资料
	网管系统	可获取的信息：位置信息
通信系统	短信网关	短信记录，短信内容
	ISAG	彩信记录，彩信内容
	HLR	客户当前位置信息、用户状态
	WAP 网关	客户上网记录、彩信记录
	端局	原始话单文件、位置信息
	关口局	原始话单文件
业务平台	ISMP-BMW	订购关系
	终端自注册平台	终端型号信息
	天翼 live	通讯记录
	协同通信平台	通讯记录
	基地平台	订购关系、行为

表 6　某运营商对敏感系统分布的梳理结果

以运营商行业上述梳理结果为例，这仅仅是一个数据梳理的基础，更重要的是要梳理出不同的业务系统对这些敏感信息访问的基本特征，如访问的时间、IP、访问的次数、操作行为类型、数据操作批量行为等，在这些基本特征的基础上，完成数据管控策略的制定。

4.4 数据的访问控制

针对数据使用的不同方面，需要完成对数据使用的原则和控制策略，一般包括如下方面：数据访问的账号和权限管理，相关的原则和控制内容包括：

（1）专人账号管理

（2）账号独立原则

（3）账号授权审批

（4）最小授权原则

（5）账号回收管理

（6）管理行为审计记录

（7）定期账号稽核

数据使用过程管理中，相关的原则和控制内容包括：

（1）业务需要访问原则

（2）批量操作审批原则

（3）高敏感访问审批原则

（4）批量操作和高敏感访问指定设备、地点原则

（5）访问过程审计记录

（6）开发测试访问模糊化原则

（7）访问行为定期稽核

数据共享（提取）管理，相关的原则和控制内容包括：

（1）最小共享和模糊化原则

（2）共享（提取）审批原则

（3）最小使用范围原则

（4）责任传递原则

（5）定期稽核

数据存储管理，相关的原则和控制内容包括：

（1）涉密数据存储的网络区隔

（2）敏感数据存储加密

（3）备份访问管理

（4）存储设备的移动管理

（5）存储设备的销毁管理

4.5 定期的稽核策略

定期的稽核是保证数据安全治理规范落地的关键，也是信息安全管理部门的重要职责，包括：

●合规性检查：确保数据安全使用政策被真实执行；

●操作监管与稽核；

●数据访问账号和权限的监管与稽核：

1）要具有账号和权限的报告

2）要具有账号和权限的变化报告

●业务单位和运维部门数据访问过程的合法性监管与稽核：

1）要定义异常访问行为特征

2）要对数据的访问行为具有完全的记录和分析

●风险分析与发现：

1）对日志进行大数据分析，发现潜在异常行为

2）对数据使用过程进行尝试攻击，进行数据安全性测试

因此建立健全数据安全治理过程管理的制度、流程、标准体系是非常必要的，后期才可以保障实行数据安全规划、计划、实施、运行、督查的全过程管控。对信息安全制度、标准进行滚动式修订，可以持续夯实自身数据安全标准化管理基础。

五. 数据安全治理技术支撑框架

5.1 数据安全治理的技术挑战

实施数据安全治理的组织，一般都具有较为发达和完善的信息化水平，数据资产庞大，涉及的数据使用方式多样化，数据使用角色繁杂，数据共享和分析的需求刚性，要满足数据有效使用的同时保证数据使用的安全性，需要极强的技术支撑。

数据安全治理面临数据状况梳理、敏感数据访问与管控、数据治理稽核三大挑战。

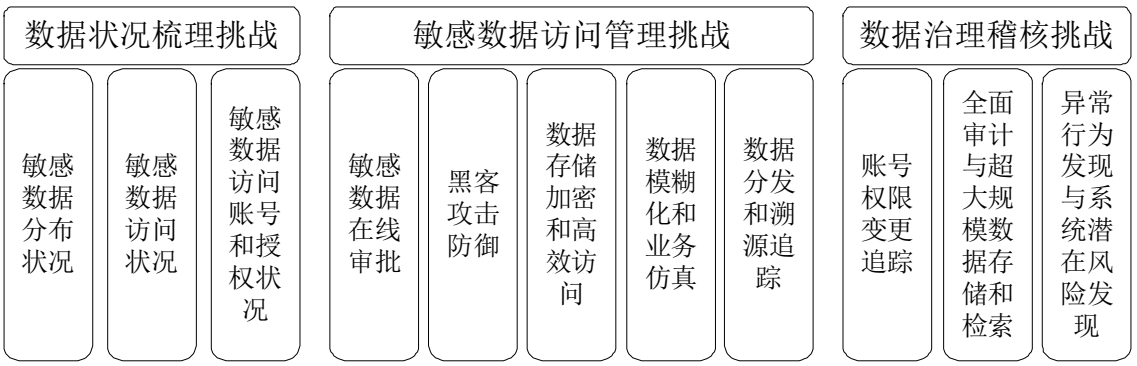


图 10　当前数据安全治理面临的挑战

5.1.1 数据安全状况梳理技术挑战

组织需要确定敏感性数据在系统内部的分布情况，其中的关键问题在于如何在成百上千的数据库和存储文件中明确敏感数据的分布；组织需要确定敏感性数据是如何被访问的，如何掌握敏感数据在被什么系统、什么用户以什么样的方式访问；组织需要迅速确定当前的账号和授权状况，清晰化、可视化、报表化的明确敏感数据在数据库和业务系统中的访问账号和授权状况，明确当前权控是否具备适当的基础。

5.1.2 数据访问管控技术挑战

在敏感数据访问和管控技术方面，细分至五个方面的挑战：

（1）如何将敏感数据访问的审批在执行环节有效落地

对于敏感数据的访问、对于批量数据的下载要进行审批制度，这是数据治理的关键；但工单的审批若是在执行环节无法有效控制，访问审批制度仅仅是空中楼阁。

（2）如何对突破权控管理的黑客技术进行防御

基于数据库的权限控制技术，在基于漏洞的攻击的基础上将很容易被突破。

（3）如何在保持高效的同时实现存储层的加密

基于文件层和硬盘层的加密将无法与数据库的权控体系结合，对运维人员无效；如何实现存储加密、权限控制和快速检索的整体解决，是这一问题的关键，只有这样的存储加密才能保证安全的同时数据剋用。

（4）如何实现保持业务逻辑后的数据脱敏

对于测试环境、开发环境和 BI 分析环境中的数据需要对敏感数据模糊化，但模糊化的数据保持与生产数据的高度仿真，是实现安全可用的基础。

（5）如何实现数据提取分发后的管控

数据的共享是数据的基本使用属性，但数据的复制是没有痕迹的；数据分发后如何保证数据不会被流转到失控的环境，或者被复制后可溯源，这是数据提取分发管理的关键。

5.1.3 数据安全的稽核和风险发现挑战

1、如何实现对账号和权限变化的追踪

定期地对账号和权限变化状况进行稽核，是保证对敏感数据的访问在既定策略和规范内的关键；但如何对成百上千个业务系统和数据库中的账号与权限的变化状况进行追踪是关键。

2、如何实现全面的日志审计

在新的网络安全法出台后全面的数据访问审计要求，日志存储要求 6 个月；在新的等保中要求，云的提供商和用户都必须实现全面的日志记录。全面审计工作对各种通讯协议、云平台的支撑，1000 亿数据以上的存储、检索与分析能力上，均形成挑战。全面的审计是检验数据安全治理中的策略是否在日常的执行中切实落地的关键。

3、如何快速实现对异常行为和潜在风险的发现与告警

数据治理中，有一个关键要素就是发现非正常的访问行为和系统中存在的潜在漏洞问题。如何对日常行为进行建模，在海量数据中快速发现异常行为和攻击行为避免系统面临大规模失控的关键。

5.2 数据安全治理的技术支撑

5.2.1 数据资产梳理的技术支撑

数据安全治理，始于数据资产梳理。数据资产梳理是数据库安全治理的基础，通过对数据资产的梳理，可以确定敏感数据在系统内部的分布、确定敏感数据是如何被访问的、确定当前的账号和授权的状况。根据本单位的数据价值和特征，梳理出本单位的核心数据资产，对其分级分类，在此基础之上针对数据的安全管理才能确定更加精细的措施。

数据资产梳理有效地解决企业对资产安全状况摸底及资产管理工作；改善以往传统方式下企业资产管理和梳理的工作模式，提高工作效率，保证了资产梳理工作质量。合规合理的梳理方案，能做到对风险预估和异常行为评测，很大程度上避免了核心数据遭破坏或泄露的安全事件。

（1）静态梳理技术

静态梳理是完成对敏感数据的存储分布状况的摸底，从而帮助安全管理人员掌握系统的数据资产分布情况。

静态梳理可以分为结构化数据梳理和非结构化数据梳理。

对于结构化数据的梳理，通过静态的扫描技术可以获得数据的以下基本信息：

A、通过端口扫描和特征发现，可以得到系统网段内存在的数据库列表，以及所分布的IP，从而获得数据库资产清单；

B、根据所定义的企业内不同敏感数据的特征，以及预先定义的这些数据的类别和级别，通过对表中的数据进行采样匹配，获得不同的列、表和库中的数据所对应的级别和类别；

对于非结构化数据，通过磁盘扫描技术，根据预先定义的数据特征，对于 CSV、HTML、XML、PDF、Word、Excel 和 PPT 等文档中的内容进行扫描，获得这些文件中所具有的信息的类别和级别。

无论是结构化还是非结构化，都要建立对应的敏感数据资产清单。

（2）动态梳理技术

动态梳理技术是基于对网络流量的扫描，实现对系统中的敏感数据的访问状况的梳理，包括：敏感数据的存储分布、敏感数据的系统访问状况、敏感数据的批量访问状况、敏感数据的访问风险。

通过动态梳理技术可以获得数据的以下基本信息：

哪些 IP（数据库主机）是数据的来源；

哪些 IP（业务系统或运维工具）是数据的主要访问者；

敏感数据是如何被业务系统访问的（时间、流量、操作类型、语句）；

敏感数据是如何被运维人员访问的（IP、用户、操作）；

动态梳理同样要分为对结构化数据访问网络流量的扫描，以及非结构化数据访问的网络

流量的扫描。结构化数据的网络流量，主要是对各种 RDBMS、NOSQL、MPP 数据库的通讯协议的流量监控；非结构化数据主要是对 Mail 协议、HTTP、FTP 等协议的监控和解析。

（3）数据状况的可视化呈现技术

通过可视化技术将静态资产和动态资产梳理技术梳理出的信息以可视化的形式呈现；比如敏感数据的访问热度、资产在组织内不同部门或业务系统内的分布、系统的账号和权限图、敏感数据的范围权限图。

（4）数据资产存储系统的安全现状评估

安全现状评估是将已定位、梳理的数据库资产进行全面检测评估，评估项包括：口令和账户、弱安全策略、权限宽泛、权限提升漏洞、日志、补丁升级等，评估是否存在安全漏洞。通过安全风险检查让数据资产管理员全面了解数据库资产运行环境是否存在安全风险。

通过安全现状评估能有效发现当前数据库系统的安全问题，对数据库的安全状况进行持续化监控，保持数据库的安全健康状态。

安全现状评估的价值：

（1）提升数据库使用安全系数：检测出数据库的 DBMS 漏洞、缺省配置、权限提升漏洞、缓冲区溢出、补丁未升级等问题。对检测出的问题进行有针对性的修复，整体提升数据库使用安全系数。

（2）降低数据库被黑客攻击风险：检测出数据库使用过程中由于人为疏忽造成的诸多安全隐患，例如：低安全配置、弱口令、高危程序代码、权限宽泛等。对上述安全隐患进行针对性处理后可有效降低黑客攻击风险。

（3）满足政策检测要求：在进行安全现状评估后，数据库管理人员可针对数据库漏洞、风险使用等方面的风险进行改进，满足相关政策对数据库安全使用的检测要求。

5.2.2 数据使用安全控制

数据在使用过程中，按照数据流动性以及使用需求划分，将会面临如下使用场景：

- 通过业务系统访问数据
- 在数据库运维时调整数据
- 开发测试时使用数据
- BI 分析时使用数据
- 面向外界分发数据
- 内部高权限人员使用数据

在数据使用的各个环节中，需要通过技术手段将各个场景下的安全风险有效规避：

图 11　数据使用安全控制示意图

5.2.2.1 业务系统数据访问安全管控

在业务系统提供服务的同时，其安全风险也随之暴露在系统中，攻击者可利用数据库的脆弱性发起攻击，达到破坏系统或者获取数据信息的目的。由此，需要针对业务访问过程进行严格控制。

- 通过虚拟补丁技术，对于漏洞攻击行为进行实时准确监测，一旦发现访问行为中包含漏洞攻击行为，实时进行拦截。
- 通过 SQL 注入防护技术，精确解析每一条到达数据库的 SQL 语句，并准确判断每一条语句是否带有注入特征，确保每一条到达数据库的语句都是合法的。

图 12　业务系统数据访问安全管控

综上所述，通过业务系统数据访问安全管控，实时、动态的监测数据库访问行为，一旦发现存在数据库攻击特性的行为，将精确拦截，确保业务系统数据访问安全性。

5.2.2.2 数据安全运维管控技术

数据在运维的过程中，重要数据的操作需要高度谨慎，一些细微的错误操作可能会导致数据库异常，并且由于接触数据的人群错综复杂，很容易发生数据运维过程中的恶意篡改或者批量导出。由此，数据库的运维过程安全性需要技术手段进行保障。

通过建立数据库运维行为流程化管理机制，对数据库运维行为提供事前审批、事中控制、事后审计、定期报表等功能，将审批、控制和追责有效结合，避免内部运维人员的恶意操作和误操作行为，确保数据库运维的安全性。

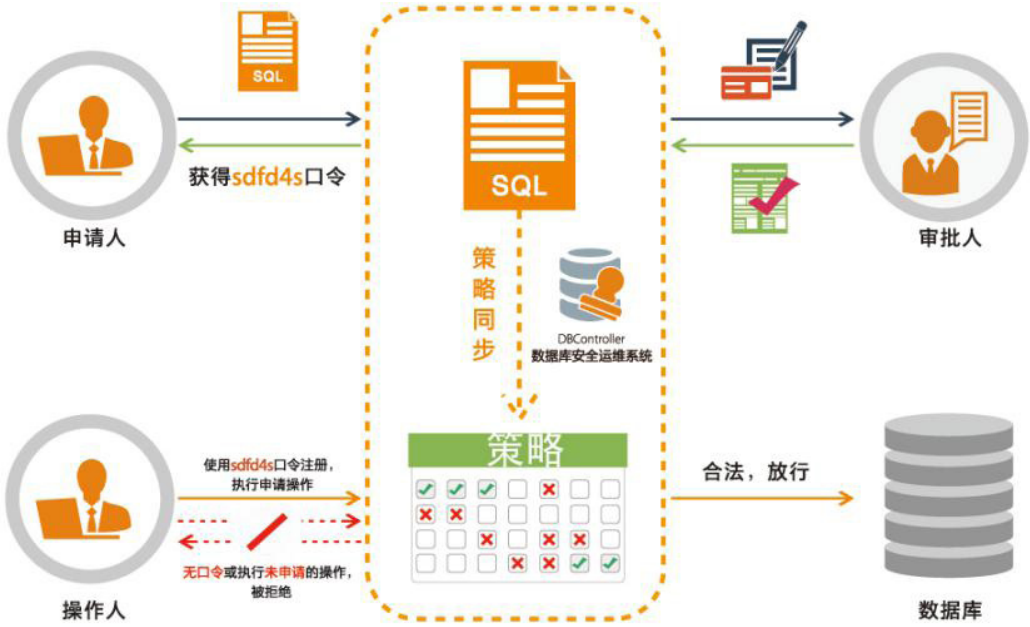


图 13　数据运维安全管控的技术原理

- 数据安全管控技术需要对内部运维人员的数据库操作请求进行智能分析，判断请求合理性及安全性，辅助决策。取代传统的“OA 或纸质申请”的审批模式，不仅提高工作效率，更能确保实际操作与原申请的一致性。
- 不仅需要为审批者提供对操作申请的风险评估，更能实时对申请与审批进行细粒度管控。通过语句特征及审计规则检测，对于疑似 SQL 注入、漏洞攻击等高危操作，即使审批通过，依然进行实时阻断；对于违反安全策略的风险操作，提供告警。同时，通过对操作申请与审批行为的实时监控，为安全管理人员同步提供可视化分析，辅助判断运维操作是否合理、安全。

5.2.2.3 开发测试环境数据安全使用

在单位内部的系统开发测试过程中，由于要高度模拟生产环境，因此很多情况下，需要使用生产环境中的生产数据进行系统开发测试。而生产数据一旦流转到开发测试环境，其数据的安全性则无法得到保障。由此，需要通过脱敏技术确保数据中的敏感信息被漂白，但又不影响开发测试人员对于数据的使用。

通过建立数据脱敏机制，对发放到开发测试环境的生产数据预先进行脱敏处理，确保经过脱敏后的数据不再带有敏感信息，且数据面向开发测试人员可用。

数据在脱敏时，为确保数据脱敏的可用性、灵活性，遵循“保证脱敏后数据可应用”规则的能力，需要实现以下六个方面的支持：

智能化，能够在复杂的数据库表与字段中，不依赖元数据中对表和字段的定义，根据数据特征自动识别敏感数据并进行有效脱敏。

可重复和不可重复性，提供重复脱敏相同数据的能力，在不同轮次的脱敏中，保证相同的隐私数据脱敏后的数据也是相同的，从而保证数据在增量环境下能够被有效的关联。也可以提供不可重复的脱敏能力，保证相同的数据在不同轮次的脱敏任务中产生的数据是不同的，从而防止逆向工程还原数据。

数据有效性，脱敏后的数据准确反应原始数据的业务属性和数据分布特征，从而保证数据在应用系统中的正常使用。

数据完整性，保证脱敏后数据的完整性，并且提供不改变原始数据尺寸，不包含无效信息的能力，防止敏感数据不符合目标数据的定义，造成无法顺利入库的情况。

数据关联性，严格保留原有数据库中数据的关系特征，支持时间序列脱敏后仍然能够保持原有的时间序列。

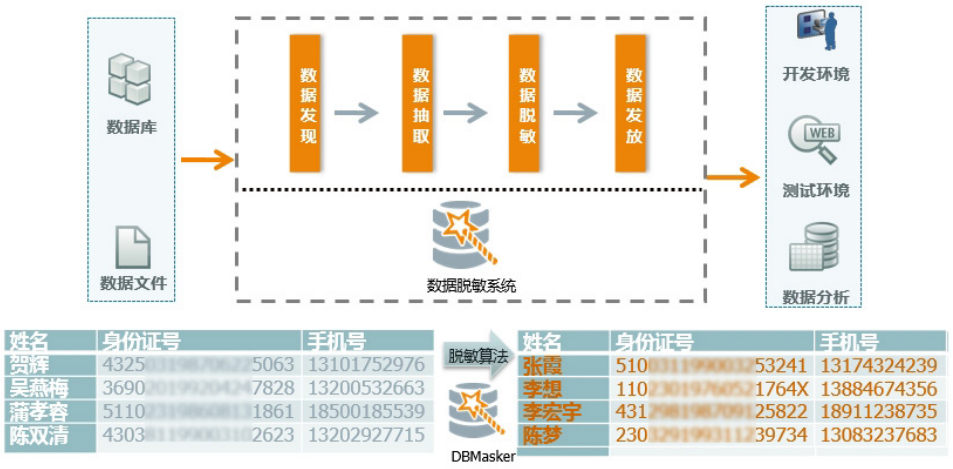


图 14　开发测试环境数据安全使用

脱敏技术有效保障脱敏后的数据可以满足原始数据相同的业务规则，是能够代表实际业务属性的虚构数据，能够使脱敏数据的使用者从体验上感觉数据是真实的，从而最终保证使用脱敏后的数据可以保证业务可靠运行。

BI 分析数据安全管控

面向 BI 分析场景，我们还是可以提供经过脱敏后的数据，用于遮盖数据中的敏感部分，但是当完成 BI 分析后，如需再对分析后的数据进行挖掘利用，则需将脱敏后的数据进行还原，否则无法了解 BI 分析后的数据结果的对应关系。

与此同时，在分析师访问业务系统获取数据时，由于不同的分析师按照自己的职责范围，应该获取自己份内的数据，但由于系统在数据访问过程中无法精确进行数据访问控制，存在越权访问数据行为。

- 由此，在 BI 分析场景下，可逆脱敏技术是必不可少的，它即可以保障顺利将数据脱敏，又可以保障完成 BI 分析后，脱敏数据可以还原成原始数据。
- 在分析师进行数据访问的同时，判断分析师的身份，根据分析师的身份返回不同程度遮盖的数据。

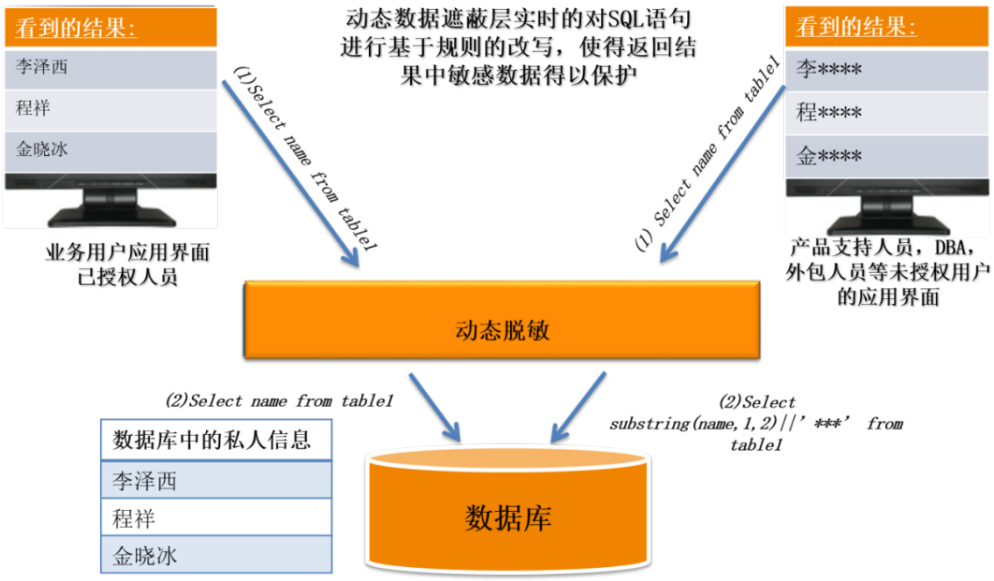


图 15　BI 分析数据安全管控

5.2.2.3 数据对外分发管控

开展业务时，数据需要对外共享，但是一旦数据对外分发后，安全保护责任的主体也应进行转移，数据共享中的接收方在接收到数据后，并没有对数据的安全保护起到应用的责任，因此，才引发了很多数据二次扩散的事件。由此，对于数据分发后的安全性需要通过技术手段监管起来。

通过建立数据分发水印机制，对于发布到外界的数据预先进行水印处理，在水印中植入数据接收者的相关信息，而植入的带水印的数据，具备如下特性：

- 安全性：嵌入在原始数据中的水印是不可除的，且能够提供完整的版权证据。数据水印不会因为数据的某种改动而导致水印信息丢失，能够保持完整性或仍能被准确鉴别。
- 透明性：在原始数据中嵌入水印标记信息不易被察觉，不影响原数据的可用性
- 溯源能力：从水印数据中溯源水印标记信息的能力。
- 低错误率：误判率低，误判分两种，一是数据无水印标记时，却检测到了水印存在；二是加了水印标记信息却没有检测出水印的存在。

一旦发现数据泄露，通过提取泄露的数据样本，对样本数据进行水印信息提取及分析，从而追溯数据泄密单位信息。

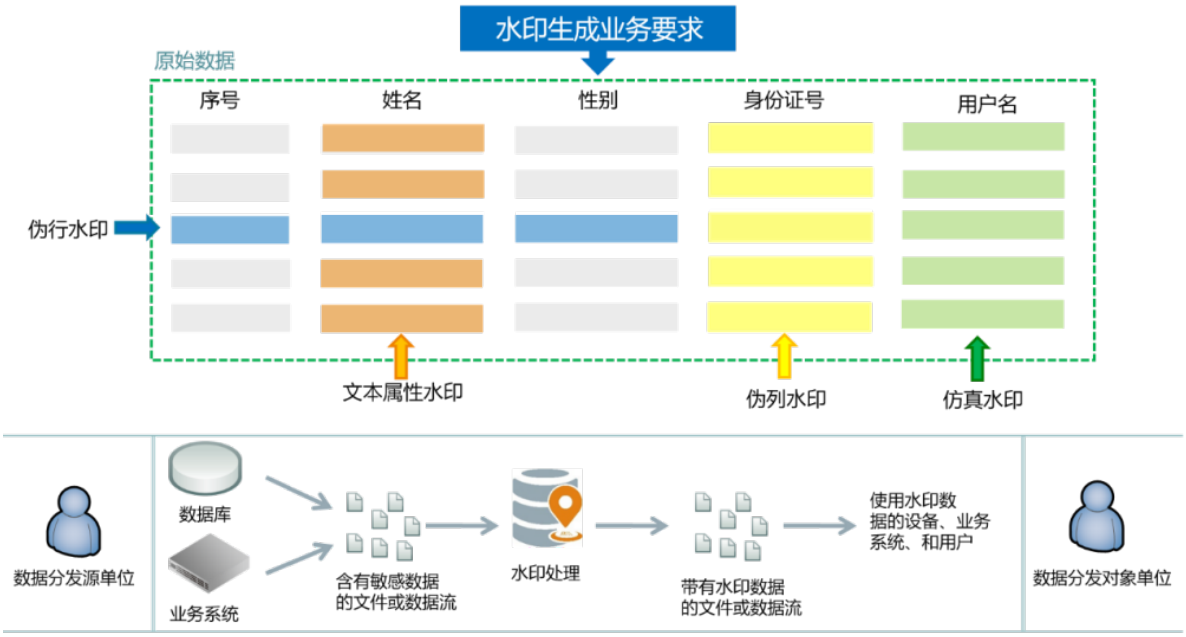


图 16　数据对外分发的安全管控

5.2.2.6 数据内部存储安全

数据在内部存储大多以明文方式，一旦数据被有意无意的带出内部环境，将面临泄密风险，另一方面，内部高权限用户对于数据的访问权限过高，同样存在数据被恶意利用的风险。

通过建立数据加密机制，将重要数据在数据库中进行加密方式存储，无论受到外部攻击导致“拖库”，还是内部人员恶意泄露数据文件，都无法对数据内容进行提取或破解。

使用我国密码管理机构认定的加密算法，也要使用国际先进的密码算法。对数据库指定列进行加密，保证敏感数据以密文形式存储，以实现存储层的安全加固。

透明的数据加密有两层含义：一是对应用系统透明，即用户或开发商无需对应用系统进行任何改造；二是对有密文访问权限的用户显示明文数据，且加、解密过程对用户完全透明。

增设数据安全管理员（Data Security Administrator，DSA）。DBA 和 DSA 相互独立，共同实现对敏感字段的强存取控制，实现责权一致。DBA 实现对普通字段一般性访问权限控制，DSA 实现对敏感字段的增、脱密处理和密文访问权限控制。该功能在数据加密存储的基础上，实现密文访问权限体系，对数据库用户进行强制访问控制，有效防止特权用户对敏感数据的非法访问。

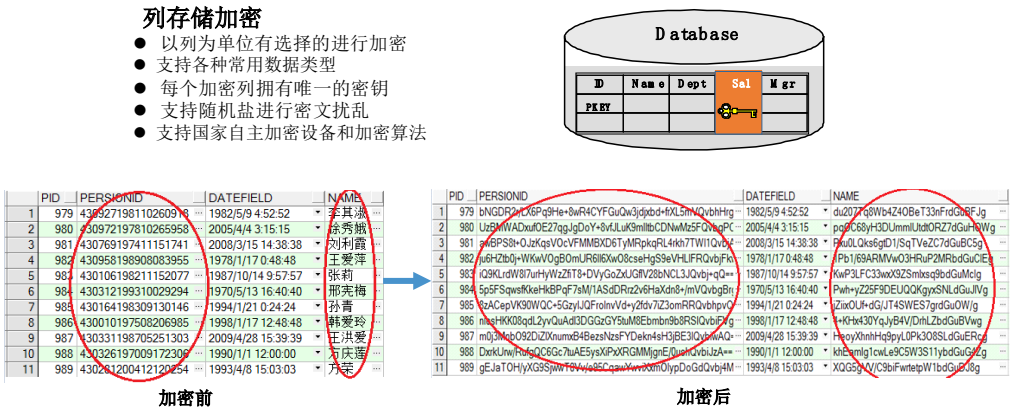


图 17　数据内部存储安全

5.2.3 数据安全审计与稽核

数据安全稽核是安全管理部门的重要职责，以此保障数据安全治理的策略和规范被有效执行和落地，以确保快速发现潜在的风险和行为。但数据稽核在大型企业或机构超大规模的数据流量、庞大的数据管理系统和业务系统数量面前，也面临着很大的技术挑战。

数据所面临的威胁与风险是动态变化的过程，入侵环节、入侵方式、入侵目标均随着时间不断演进。这也就要求我们的防护体系、治理思路不能墨守成规，更不能一成不变。所以数据安全治理的过程中我们始终要具备一项关键能力——完善的审计与稽核能力。通过审计与稽核的能力来帮助我们掌握威胁与风险的变化，明确我们的防护方向，进而调整我们的防护体系，优化防御策略，补足防御薄弱点，使防护体系具备动态适应能力，真正实现数据安全防护。

数据的安全审计和稽核机制由四个环节组成，分别是行为审计与分析、权限变化监控、异常行为分析、建立安全基线。

5.2.3.1 行为审计与分析

在数据安全治理的思路下，我们建设数据安全防护体系时必须具备审计能力。利用数据库协议分析技术将所有访问和使用数据的行为全部记录下来，包括账号、时间、IP、会话、操作、对象、耗时、结果等等内容。一套完善的审计机制能够为数据安全带来两个价值：

1、事中告警

数据的访问、使用、流转过程中一旦出现可能导致数据外泄、受损的恶意行为时，审计机制可以第一时间发出威胁告警，通知管理人员。管理人员在第一时间掌握威胁信息后，可以针对性的阻止该威胁，从而降低或避免损失。所以，审计机制必须具备告警能力，可以通过邮件、短信等方式发出告警通知。

为实现事中告警能力，审计系统需要能够有效识别风险威胁，需要具备下列技术：

●漏洞攻击检测技术：针对 CVE 公布的漏洞库，提供漏洞特征检测技术；

● SQL 注入监控技术：提供 SQL 注入特征库；

●口令攻击监控：针对指定周期内风险客户端 IP 和用户的频次性登录失败行为监控；

●高危访问监控技术：在指定时间周期内，根据不同的访问来源，如：IP 地址、数据库用户、MAC 地址、操作系统、主机名，以及应用关联的用户、IP 等元素设置访问策略；

●高危操作控制技术：针对不同访问来源，提供对数据库表、字段、函数、存储过程等对象的高危操作行为监控，并且根据关联表个数、执行时长、错误代码、关键字等元素进行限制；

●返回行超标监控技术：提供对敏感表的返回行数监控；

● SQL 例外规则：根据不同的访问来源，结合指定的非法 SQL 语句模板添加例外规则，以补充风险规则的不足，形成完善的审计策略。

2、事后溯源

数据的访问、使用过程出现信息安全事件之后，可以通过审计机制对该事件进行追踪溯源，确定事件发生的源头（谁做的？什么时间做的？什么地点做的？），还原事件的发生过程，分析事件造成的损失。不但能够对违规人员实现追责和定责，还为调整防御策略提供非常必要的参考。所以，审计机制必须具备丰富的检索能力，可以将全要素作为检索条件的查询功能，方便事后溯源定位。

一套完善的审计机制是基于敏感数据、策略、数据流转基线等多个维度的集合体，对数据的生产流转，数据操作进行监控、审计、分析，及时发现异常数据流向、异常数据操作行为，并进行告警，输出报告。

5.2.3.2 权限变化监控

账号和权限总是动态被维护的，在成千上万的数据账号和权限下，如何快速了解在已经完成的账号和权限基线上增加了哪些账号，账号的权限是否变化了，这些变化是否遵循了合规性保证。需要通过静态的扫描技术和可视化技术帮助信息安全管理部门完成这种账号和权限的变化稽核。

权限变化监控是指监控所有账号权限的变化情况，包括账号的增加和减少，权限的提高和降低，是数据安全稽核的重要一环。对权限变化进行监控，对抵御外部提权攻击，对抵御内部人员私自调整账号权限进行违规操作均是必不可少的关键能力。

权限变化监控能力的建立分为两个阶段，第一是权限梳理，第二是权限监控。

1、权限梳理

结合人工和静态扫描技术，对现有账号情况进行详细梳理，梳理结果形成账号和权限基线，该基线的调整必须遵循规章制度的合规性保障。通过可视化技术帮助管理人员直观掌握环境中所有账号及对应的权限情况。

2、权限监控

账号和权限基线一旦形成，即可通过扫描技术对所有账号及权限进行变化监控。监控结果与基线进行对比，一旦出现违规变化（未遵循规章制度的私自调整权限）会通过可视化技

术和告警技术确保管理人员第一时间可以得到通知。

5.2.3.3 异常行为分析

在安全稽核过程中，除了明显的数据攻击行为和违规的数据访问行为外，很多的数据入侵和非法访问是掩盖在合理的授权下的，这就需要通过一些数据分析技术，对异常性的行为进行发现和定义，这些行为往往从单个的个体来看是合法的。

对于异常行为，可以通过两种方式，一种是通过人工的分析完成异常行为的定义；一种是对日常行为进行动态的学习和建模，对于不符合日常建模的行为进行告警。

分类	异常描述	影响分析
异常的查询频率	一段时间内重复查询客户信息几百次	高
	一个号码一天内被查询 10 次以上，或一个月内被查询 100 次以上	中
	某些特殊号码被多次查询，例如吉祥号	中
帐号异常	长时间不登陆的帐号登陆使用，查询敏感信息	低
	同一个帐号被多个人员使用，同时登陆或登陆 IP 地址经常变化	中
异常的修改频率	一段时间内修改客户信息几百次	高
	单号码信息一天内被修改 10 次以上，或一个月被修改 100 次以上	中

表 7　几种异常行为定义例举

异常行为分析机制的建立对分析、寻找“好人中的坏人”非常关键，同时也是防御体系、防御策略调整的重要参考内容。

六 . 数据安全治理的发展展望

数据安全治理 , 作为一种系统性的围绕数据安全建设为核心的方法和框架体系 , 帮助具有中大型数据中心、数据向云端迁移的转型组织、数据高密度行业的政府单位或企业能够建立一个持续优化改进的 , 尽可能保障数据安全使用的数据安全体系。

在今天 , 国内以运营商、金融行业、部分政府客户为代表的高端用户群体当中 , 自发或自觉的在采用类似的方法论进行着数据安全体系建设 ; 但这种方法论还没有大规模地被发展采用。Gartner 预测 , 到 2021 年 , 将有超过 30% 的企业开始实施执行数据安全治理框架。到 2022 年，90% 的企业战略将明确数据作为关键企业资产，数据分析作为必不可少的能力。30% 的 CDO（首席数字官）将与 CFO（首席财务官）正式对组织的数据资产价值进行评估，以改善数据的管理和收益。超过 30% 的企业（目前不到 5%）将使用其数据资产的财务风险评估来对 IT、分析、安全和隐私的投资选择进行优先级排序。

在 2018 年，若干国内企业和重要行业都将推动相关数据安全管理规范的出台，这些规范都将以数据的分级分类为基础，对数据在行业内的安全使用提出要求，这些企业和行业将是数据安全治理的重要实践。

数据安全治理产业，大体可以分为大型数据中心用户、安全治理咨询服务商、技术产品供应商、技术方案提供商；当前在中国这样的产业链环境正在形成，通过这些产业链的构建，将为数据安全治理的落地提供保障。

每个企业的数字化业务都在经历数据在速度、规模、多样性和价值的快速增长机会，同时伴随着产生了大量具有财务影响的业务风险。由于越来越多来自数据收入和投资的机会，投资决策时却未考虑相关成本或负债。董事会层面的风险监管对于成功投资至关重要，以促使投资过程中加大对风险的评估。企业需要对导致业务结果的技术问题的风险评估。关于如何使用数据的投资决策可能导致的财务影响，在企业里很少进行讨论。因此，不评估机会成本，并导致过度乐观的财务预测。《一般数据保护条例》（GDPR）的巨大影响戏剧性地提高了企业对各种法规的关注（包括健康，信用卡和其他财务数据的各方面），以降低合规性风险。数据泄露，隐私执行，不合规甚至意外事件处理都可能以不同方式对业务产生财务影响。例如，被公开暴露出来的具有安全性或或隐私性问题的大量数据泄露，可能导致巨大的财务通知成本和罚款。然而，这些是一次性成本，可能会影响企业年度报告中的现金流，并可能导致短期资本化价值降低。虽然这会产生巨大的财务影响，但影响通常是短期的，除非企业需要借钱并改变长期投资。这些风险将减少短期和长期财务估值和数据货币化。

数据使用带来的财务影响，Gartner 最新通过信息经济学模型来评估，即财务数据风险评估（FinDRA）模型。信息经济学作为一个重要的工具，可以使安全和风险管理（SRM）领导者，首席信息安全官（CISO），首席数据官（CDO）和 CIO，根据收入机会评估每个数据集。信息经济学模型还允许他们对管理、存储、分析和保护数据的有形和无形成本进行评估。财务数据风险评估（FinDRA）模型如图所示：

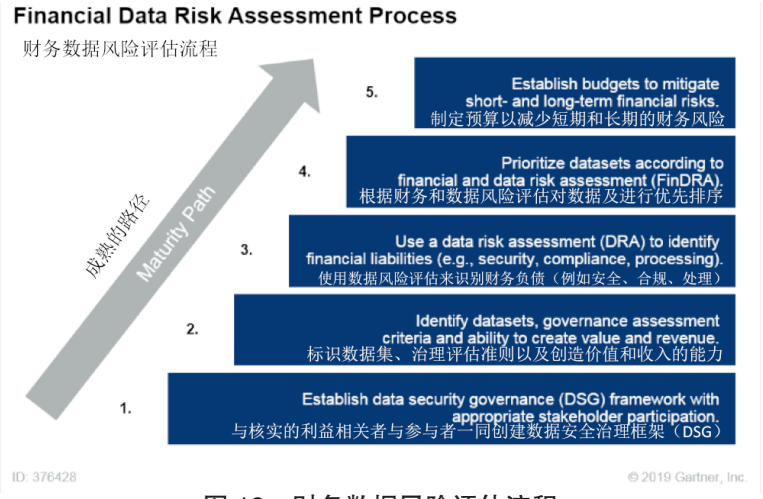


图 18　财务数据风险评估流程

这意味着需要仔细评估不同金融负债的业务风险，无论是数据货币化产生的短期还是长期影响。该研究将描述如何评估潜在负债的规模并根据影响确定优先级。需要注意的是，财务风险评估是更广泛的数字风险评估视图的一部分。

通过数据安全治理框架来识别业务风险，必须确定企业的业务风险，这些风险将会因以下事件而影响组织的财务绩效：

- 不合规（例如，隐私，税务，医疗保健或信用卡）
- 安全威胁（例如，恶意内幕，黑客，勒索软件或拒绝服务）
- 内部或外部审计流程
- 数据操作
- 数据完整性（例如，意外删除或修改）
- 意外披露
- 合并或收购业务前的尽职调查
- 规划数字创新计划，项目或技术投资

以数据安全治理（DSG）框架为基础，将这些事项作为数据风险评估（DRA）的一部分。这对选择新服务或 IT 硬件的投资决策具有关键影响。这是因为本地部署和通过公共云服务在新的存储和分析平台上传输数据会产生地理来源、跨境传输充分性、存储和数据访问相关的数据驻留等问题，随着与业务合作伙伴和其他生态系统共享数据，其他安全性，隐私，信任和道德问题也随之增加。

当前世界，特别是在中国，组织力求通过数字转型加速业务增速，摆脱数据规模激增但数据安全策略规则能力滞后的矛盾，数据安全治理必将在数据使用安全中发挥巨大作用，降低业务风险，推动组织 IT 治理变革。

附件 A 词汇列表

DSG： Data Security Governance，数据安全治理。Gartner 将其作为数据安全的原则与框架。

DGPC: Data Governance for Privacy, Confidentiality and Compliance 隐私、保护与合规性的数据治理。DGPC 由微软开发以帮助组织创建一个全面解决隐私、保护与合规这三个目标的数据治理计划。

DSMM： Data Security capability Maturity Model, 数据安全能力成熟度模型。组织对数据安全保障能力进行成熟度度量，从组织实践、流程、方法、水平的能力维度作为基准进行衡量，并设置提升目标的优先级，该模型包括三个方面：数据生命周期安全、安全关键能力、能力成熟等级。

GDPR： General Data Protection Regulation 欧盟通用数据保护条例。该条例将对全球欧盟居民个人数据的处理产生全球影响，并于 2018 年 5 月 25 日生效。

DCAP: Data-Centric Audit and Protection 以数据为中心的审计和保护。DCAP 能够集中监控用户和管理员与特定数据集相关的行为。基于数据安全治理原则，通过在非结构化，半结构化和结构化数据库或数据孤岛中应用数据安全策略和访问控制来实现。

DLP： Data Loss Prevention，数据泄露防护。基于内容检测和数据上下文分析，为数据丢失提供补救为核心功能的技术。

CASB： Cloud Access Security Broker 云接入安全代理。对通用的云应用存储、数据保护和企业授权的云应用服务进行治理并提供可视化的产品或服务，该技术需要确保采用增加大量的云服务以及传统企业内外用户对其进行访问。

IAM： Identity and Access Management 身份与访问管理。适用于使用访问控制引擎为多个用例中的目标应用程序提供集中式身份验证，单点登录，会话管理和授权实施的技术。通过建立一套全面的数字身份，实现组织信息资产统一的身份认证、授权和身份数据集中管理与审计。

UEBA: User and Entity Behavior Analytics，用户与实体行为分析。基于机器学习，对安全性的异常行为进行分析和检测。汇总和分析个人数据，构建个人和实体（IP 主机，应用程序，网络流量和数据存储库）标准概要和行为，通过对超出基线的异常行为打包分析，帮助组织发现潜在威胁，从事恶意行为进行分析。

附件 B　国际数据安全治理理论

2018 年 5 月，全球知名 IT 研究与咨询机构 Gartner 发布对数据安全治理（Data Security Governance）框架的最新研究结果，在此将其报告内容引入，以供参考：

Gartner 关于数据安全治理（DSG）的框架与观点

企业正在加速数字化转型，通过挖掘数据的价值抓住巨大的发展机遇。然而，企业面临的风险也在剧增，这些风险源于合规性、数据驻留问题以及安全威胁形势，因为数据需要流经本地数据中心或公有云平台中，随着数据与业务和其他数据生态系统共享，安全、隐私、信任和道德问题也随之增加。但是，目前的数据安全策略并未广泛应对这些商业风险。Gartner 认为，首席信息安全官（CISO）和负责数据安全和隐私的安全和风险管理（SRM）领导者必须致力于实施适合数据增长和扩散的数据安全治理（DSG）框架。

合适的 DSG 框架需要 CISO 团队、首席数据官（CDO）和数据保护官员（DPO）之间的新合作。由于数据保护和数据隐私性的相关性，CISO 和 DPO 团队之间已经形成合作关系。CISO 和 CDO 之间的合作将执行几项重要职能：

- 协调信息治理和信息安全治理
- 参照数据分类和数据生命周期管理的方法。
- 使用信息经济学（infonomics）制定相关预算和进行财务数据分析

DSG 框架提供了一个平衡的方法来定义如何通过数据保护和隐私声明来实现实际的安全性。每个数据集都不同，由于之前各个治理工作各自独立（见下图），业务风险要求 CDO 和 CISO 团队提供更高水平的交叉沟通和协作。数据支出分散在多个领导者的预算中，其中包括 CIO，CMO，CRO 和 DPO。

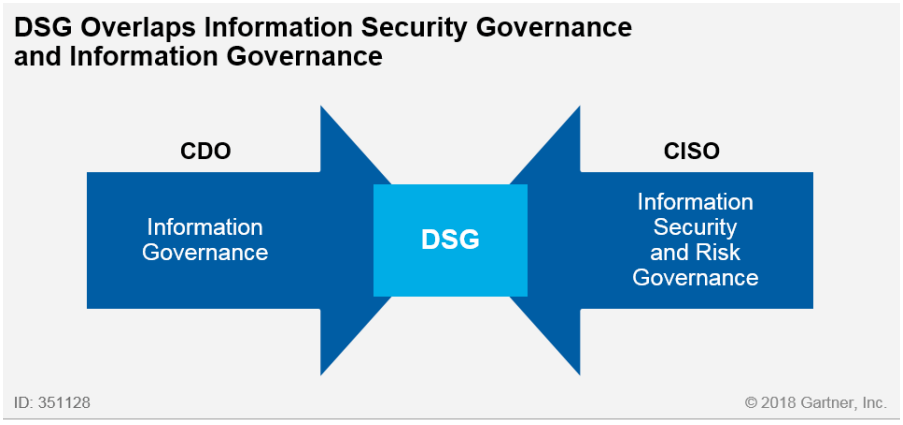


图 19　DSG 如何重叠信息安全治理和信息治理

使用 DSG 框架优先处理需要通过适当安全性进行缓解的业务风险

DSG 框架的构建对于每个数据集的流转和分析将创建八种不同的：隐私、机密性、完整性、可用性、道德和生命周期。

DSG 框架如下图所示，Gartner 的治理研究为相关角色和责任提供了完善的指导。确定问责原则也很重要，这必须记录在由首席执行官和董事会签署并得到明确支持的企业安全章程中。

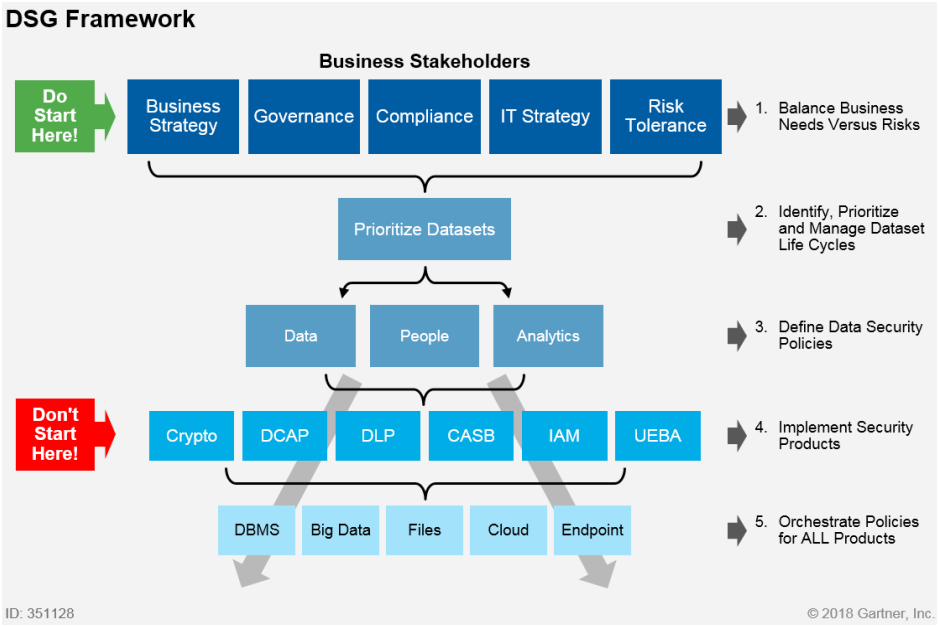


图 20　Gartner DSG 框架

许多 Gartner 客户开始提出有关实施特定安全产品的最佳实践的问题，或者特定产品如何合规，这是一个错误的开始。因此，上图中的注释强调“不要从这里开始”，因为每个产品选项都包含它提供的安全功能以及它实施的数据位置。没有单一产品能够降低安全风险。在 DSG 的实施中，Gartner 的主要观点如下：

- 与 CDO 和 DPO 合作，参照数据生命周期对数据进行发现和分类；
- 使用持续的适应性风险和信任评估体系（CARTA）对不同数据选择不同的安全策略，结合法律合规性，重点监控核心数据的访问权限和行为，及时响应、告警，并能够感知风险；
- 定期检查安全策略，尤其当安全风险发生变化。

Microsoft 提出的 DGPC 框架

由微软开发的隐私，保密和合规性（DGPC）框架的数据治理计划，是为了企业和组织能够以统一、跨学科的方式来实现以下三个目标，而非组织内不同部门独立解决这三个不同的问题：

1、传统的 IT 安全方法侧重于 IT 基础设施，通过边界安全与终端安全进行保护。重点应该加强对存储数据的保护，并随基础设施移动，加强保护。

2、隐私相关的保护措施必须超越与安全重叠的隐私保护措施，包括：重点获取、保护和执行客户对如何及何时收集、处理或第三方共享的行为保护措施；

3、数据安全和数据隐私合规责任需要通过一套统一的控制目标和控制行为，进行合理化处理，以满足合规。

DGPC 框架下的数据治理，需要 IT，人力资源，法律和财务部门以及商业团体和市场部门之间的合作 – 简而言之，涵盖任何在收集，处理，使用和管理个人身份信息（PII），知识产权财产，商业秘密和其他类型的机密信息。

需要指出的是，为安全性，隐私性，机密性和合规性而提议的数据治理方法并不需要修改或替换组织的现有信息安全管理系统或 IT 治理流程。相反，它通过指定可帮助组织更好地保护数据隐私和安全并满足合规性义务的其他角色，任务和技术工具来增强它们。

数据治理的商业案例

如果企业和组织已经拥有成功的 IT 治理流程，完善的控制框架和有效的信息安全管理系统以满足他们的安全需求和合规义务，他们为什么会希望采用另一个框架。有两个原因：

- 安全标准和控制框架倾向于主要保护整个 IT 基础架构，并将该基础架构中的成本投资与业务目标协调一致。换句话说，它们提供了数据安全“森林”的观点。DGPC 框架将重点放在数据安全的“树状结构”上，以识别和管理与特定数据流相关的安全和隐私风险需要保护的信息，包括个人信息，知识产权，商业秘密和市场数据。
- DGPC 框架创建了一个环境，可识别针对隐私信息的威胁，包括与安全威胁不重合的隐私威胁，例如违反客户选择和同意收集何种类型的个人信息以及如何使用，处理和共享。

DGPC 框架组件

DGPC 框架围绕三个核心能力领域组织：人员，流程和技术。

DGPC 框架与企业现有的 IT 管理和控制框架（如 COBIT）以及 ISO / IEC 27001/27002 和支付卡行业数据安全标准（PCI DSS）等安全标准协同工作。DGPC 框架围绕三个核心能力领域组织，涵盖人员，流程和技术三个部分：

人员

第一步是建立一个 DGPC 团队，由组织内的个人组成，并给予他们明确规定的角色和职责，为履行其所需职责提供充足的资源，并就整体数据治理目标提供明确的指导。

流程

有了合适的人参与 DGPC 的工作，组织就可以专注于定义流程。首先，检查各种权威性

文件（法律，法规，标准，公司政策和战略文件），明确必须满足的要求。其次，确定指导原则和政策，以产生适合这些要求的环境。最后，组织应该在特定数据流的场景下识别威胁数据安全，隐私和合规的风险所在，分析相关风险并确定适当的控制对象和行为。

技术

Microsoft 开发了一种技术方法来分析特定的数据流，并识别信息安全管理系统和控制框架的更广泛的保护措施可能无法解决的剩余流量特定风险。这种方法具体落到风险 / 差距分析矩阵模型中。该模型围绕三个要素构建：信息生命周期，四个技术领域以及组织的数据隐私和保密原则。

信息生命周期

为了识别安全风险并选择合适的技术措施和行为来保护机密数据，组织必须首先了解信息如何在整个系统中流动，以及信息如何在不同阶段被多个应用程序和人为了不同目的被访问和处理。

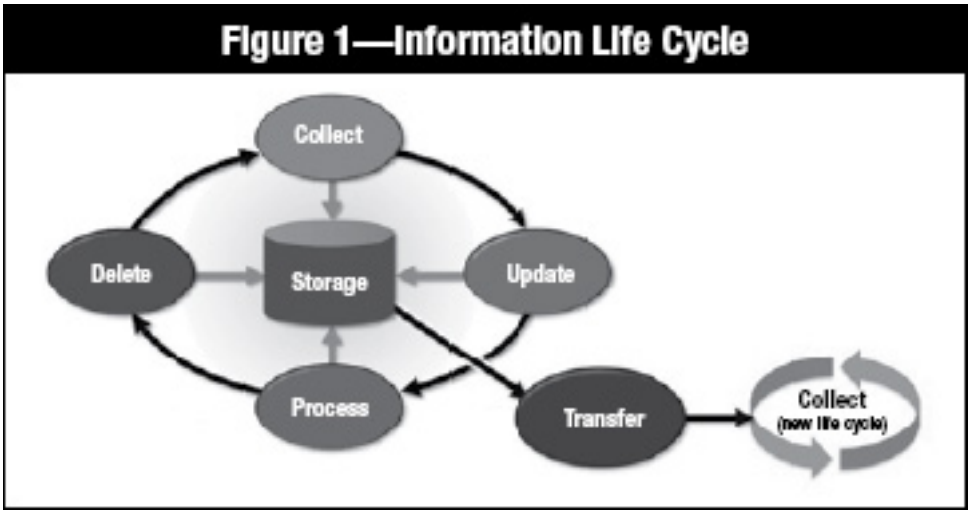


图 21　信息生命周期

四个技术领域

组织还需要系统评估保护其数据机密性，完整性和可用性的技术是否足以将风险降低到可接受的水平。以下技术领域为此任务提供了一个参考框架：

- 安全的基础架构：保护机密信息需要技术基础架构，可以保护计算机，存储设备，操作系统，应用程序和网络免受恶意软件，黑客入侵和内部人员窃取。
- 身份和访问控制：身份和访问管理技术有助于保护个人信息免受未经授权的访问，同时促进合法用户的可用性。这些技术包括认证机制，数据和资源访问控制，供应系统和用户账户管理。从合规角度来看，IAM 功能使组织能够准确地跟踪和执行整个企业的用户权限。
- 信息保护：机密数据需要持续保护，因为它们在组织内部和组织内共享。组织必须确

保其数据库、文档管理系统，文件服务器和实践在整个生命周期内正确分类和保护机密数据。

- 审计和报告：遵从性控制的系统管理，监控与自动化审计对验证系统和数据访问控制是否有效，这些对于识别可疑或不合规的行为十分有用。

数据隐私和保密原则

以下 4 项原则旨在帮助组织选择能够保护其机密数据资产的技术和行为，以指导风险管理和决策过程。

- 原则 1：在整个机密数据使用期限内遵守政策。这包括承诺按照适用的法规和条例处理所有数据，保护隐私并尊重客户的选择和同意，并允许个人在必要时审查和更正其信息。
- 原则 2：尽量减少未经授权的访问或滥用机密数据的风险。信息管理系统应提供合理的管理、技术和物理保障，以确保数据的机密性、完整性和可用性。
- 原则 3：尽量减少机密数据丢失的影响。信息保护系统应提供合理的保护措施，如加密，以确保遗失或被盗数据的机密性。应制定适当的数据泄露应对计划和升级路径，所有可能参与违规应对的员工都应接受培训。
- 原则 4：记录适用的控制措施并证明其有效性。为确保问责制，组织应遵守数据隐私和保密原则，应通过适当的监督、审计和控制措施的使用来加以验证。此外，组织应该有一个报告违规行为和明确定义的升级路径的流程。

风险 / 差距分析矩阵

该工具可帮助组织识别并解决现有保护工作的缺失：针对特定数据流中的隐私、机密和合规威胁的数据安全，该矩阵提供了数据现有和未来的保护技术、措施和行为，形成了统一视图。

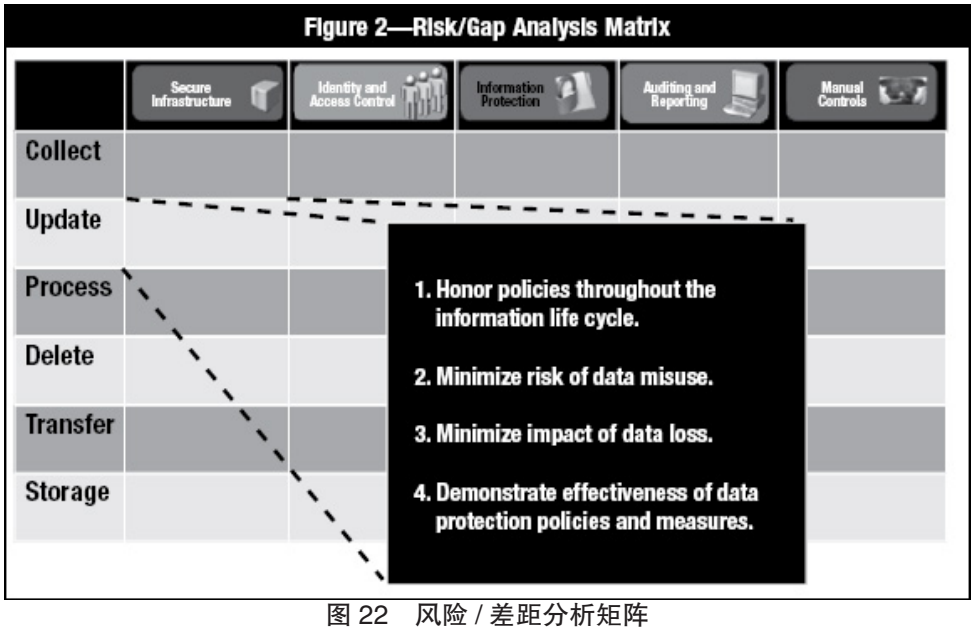


图 22　风险 / 差距分析矩阵

每一行描绘了信息生命周期中的一个阶段。矩阵中的前四列表示一个技术领域，而最右边的列表示控制行为，这些行为措施必须在信息生命周期的每个阶段满足四种数据隐私和保密原则的要求。

利用风险 / 差距分析矩阵评估风险

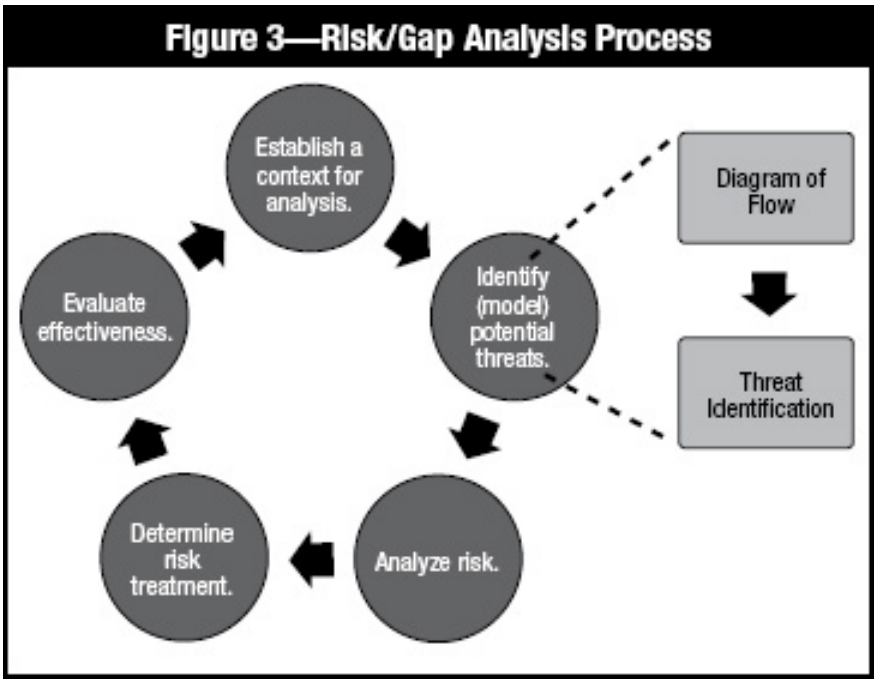


图 23　风险 / 差距分析过程

矩阵为组织提供了一个强大的风险评估和缓解工具。上图所示的分析过程和以下步骤可以帮助组织找出现有保护措施中的差距并进行调整措施：

步骤 1：建立风险分析

这涉及定义数据流的业务目的；需要了解如何使用数据以及涉及哪些业务系统；并确定业务流程中的隐私，安全和合规目的。

步骤 2：执行威胁建模

大多数威胁建模技术只关注安全威胁，威胁建模涉及两个阶段：

- 创建数据流的图表化呈现。这里有多种技术可用于图表构建。微软的产品团队和咨询服务机构通常使用数据流图（DFD），并添加“信任边界”。如上图所示，信任边界是用来分隔业务实体和 IT 基础架构领域（如网络或管理域）的边界。在这种情况下，客户将 PII 提供给应用服务器，应用服务器将其存储在由云提供商管理的服务器中。每个事务都记录在由管理与应用服务器同一主机的日志服务器中。每次机密数据需要跨越信任边界时，对于安全性、策略、流程或实施的要求可能会发生变化，因此将会在步骤 3 中识别出威胁。请注意，在图表步骤，模型通常代表系统和数据存储，而不是“传统”应用安全威胁建模中描述的单个进程。

●威胁列举是威胁图的系统分析，威胁不仅限于攻击者或技术威胁，还可以指代任何可能违反四项数据隐私和机密性原则的任何内容。组织应该使用这些原则来定义威胁类别，如图 4 所示，图 4 是将威胁枚举应用于图 5 所示数据流所产生的输出示例。这些类别的确切定义将取决于该组织的独特政策和适用的行业、地区和法律合规框架。

Figure 4—Collection and Update Stages in the Risk/Gap Analysis Process

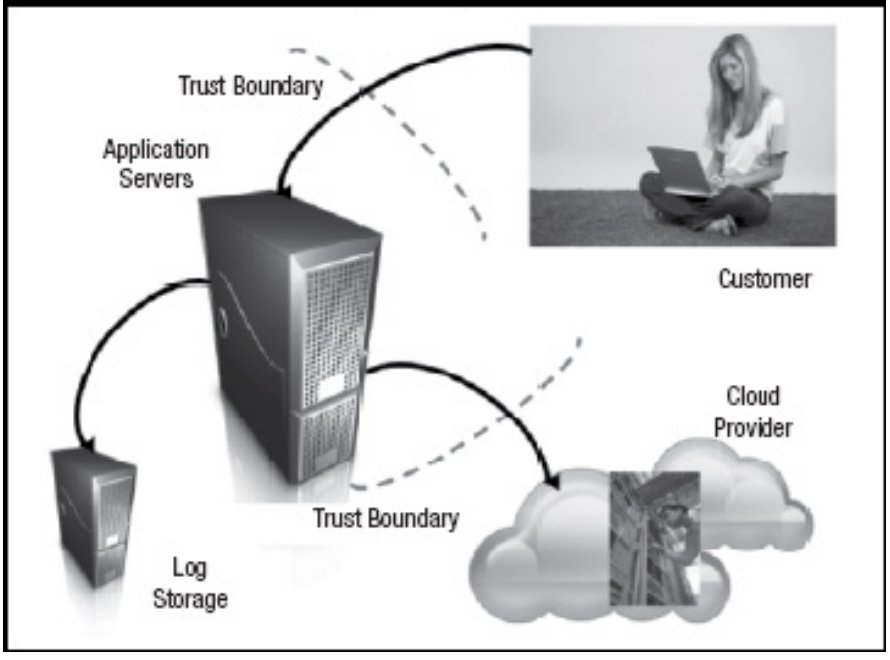


图 24　收集和更新风险 / 差距分析过程的阶段

Figure 5—Threat Identification

Threat Type	Specific Threat
Choice and consent	Options have to be displayed clearly in order to obtain appropriate consent.
Access and correction	Customer is not able to view/modify personal information.
Accountability	Customer PII is not properly classified.
Compliance	Compliance reports are not defined; escalation path to business owners is not specified.
Information protection	Customer information is sent in the clear, over an unauthenticated channel.
Data quality	Quality depends on customer; no threat is identified.

图 25　风险类别

以下是威胁列举示例，说明步骤 2 中描述的威胁类别的定义：

原则 1：在整个机密数据使用期间必须遵守法规政策。

- ●选择数据并经过客户授权后才能进行收集、使用和披露
  - – 避免数据收集、使用、披露和补救政策的通知不及时等问题
  - – 选择和提供个人信息收集和使用需要用户同意，语言或流程不明确或具有误导性可能是威胁之一。
- ●个人访问和修改
  - – 用户无法验证其个人信息的准确性。
- ●问责
  - – 缺乏客户授权及其他相关政策、法律和法规的管制和受控。

原则 2：尽量减少未经授权访问或滥用机密数据的风险。

- ●信息保护
  - – 避免因缺乏合理的管理，技术和物理保障措施，无法确保数据的机密性、完整性和可用性。
  - – 未经授权或不当的数据访问行为
- ●数据质量
  - – 无法验证数据的准确性、即时性和相关性
  - – 用户无法根据实际需要进行修改

原则 3：尽量减少机密数据丢失的影响。

- ●信息保护
  - – 没有足够的安全措施来确保数据丢失或被盗的风险
- ●问责制
  - – 缺乏数据泄露响应计划和升级路径
  - – 缺乏对所有机密数据的系统加密
  - – 无法通过适当的监控，审计和访问控制来确保遵守数据保护原则

原则 4：记录实施的安全控制措施并稽核其有效性。

- ●问责制
  - – 对计划，管控，流程或系统配置的文档不当进行问责
- ●合规性
  - – 无法通过现有的日志，报告和控制来验证或证明合规性
  - – 缺乏合规升级途径和流程
  - – 缺乏法律要求的违规通知计划和其他应对计划

识别这些威胁类型为组织评估其数据流量提供了一个基础，并考虑了当流量跨越安全边界时（例如生命周期不同阶段之间的转换期间），有关隐私性、机密性和合规性的要求和条

件可能会发生变化。

步骤 3：分析风险

大多数组织已经采取了一些措施来确保数据安全性和隐私性，正如其现有控制框架和信息安全管理系统所指定的那样。为了完成这一步骤，组织应首先统计现有的保护控制、技术和行为。然后，对于风险 / 差距分析矩阵中的每个单元格，确定哪些控制措施、技术和活动支持遵守四项隐私和保密原则。当矩阵的相应单元格中已识别现有保护措施未解决的威胁，并评估了相关风险时，此步骤即告结束。

步骤 4：确定缓解措施

在矩阵的适当单元格中，组织应列出使各项风险达到可接受水平所需的额外控制措施、技术和活动，然后评估每项风险的成本 / 收益。当组织决定是否以及如何降低，转移每个确定的风险时，这一步骤就结束了。

步骤 5：评估缓解措施的有效性

如果存在不可接受的风险，组织应审查前面步骤的结果并重新启动整个评估周期（图 6）。

Figure 6—Identified Mitigation Measures

	Secure Infrastructure	Identity and Access Control	Information Protection	Auditing and Reporting	Manual Controls
Collect/ Update	*Servers are on regular OS and App. Patch cycle, and up to date in malware signatures.* *Incoming data are correctly classified and tagged as per customer choice and consent.*	**All transactions to take place on authenticated communications.**	*Choices are displayed and consent is obtained as per MPSD guide.* *Transaction log data are encrypted in transit and at rest.* **All material customer transactions arrive over encrypted communication channel.**	*All material transactions are to be logged as per logging framework.* *Communications channel and log servers are monitored. Failover process to local log servers in processor facilities is up and running.* **Alerts and alert recipients are defined and operational.** **Access and use reports, along with recipients and delivery schedules, are defined.**	**The escalation path for issues is defined.**

图 26　评估缓解措施

附件 C　数据安全治理实践

电信数据安全治理实践

电信运营商行业逐步进入大数据时代，由于该行业集中了很多个人隐私信息，导致用户在对数据进行应用同时，会受到各种内外部风险的影响，导致信息的泄露或恶意的篡改，对公民、社会、甚至国家安全造成一定的影响。因此，亟需加强对基于大数据环境下的电信运营商客户信息安全保护进行数据安全治理工作，减少个人信息泄露或修改问题的出现，满足国家法律法规要求，保障客户隐私权益。

C.1.1 运营商数据安全现状与挑战

1、大数据新技术带来客户信息安全挑战。大数据平台数据量大、数据类型多样、大数据平台组件设计独立等，导致大数据的采集、存储、处理、应用、传输等环节均存在更大的风险和威胁。在大数据安全管理层面，存在缺乏客户信息衡量标准，安全管理职责不明确等风险，特别是在运营商大数据对外业务合作过程中，留存等诸多的安全风险。在安全运营层面，也存在着供应链、业务设计、软件开发、权限管理、运维管理、合作方引入、系统退服等安全风险。

2、客户信息的分类分级较难。客户信息包括用户身份和鉴权信息、用户数据及服务内容信息、用户服务相关信息等三大类，而在这三类信息中，又包含了身份标识、基本资料、鉴权信息、使用数据、消费信息等诸多不同类型的数据。这就导致在实际工作落地中，电信运营商往往很难进行全量的识别，致使对这些客户信息进行管理时，无法进行全部监控，因而不能在第一时间发现风险。当前网络中都应用了加密等先进技术，一定程度上加强了客户敏感信息的管理，但这种单一的方式，往往还存在一些漏洞，使敏感信息依然存在安全隐患。

3、数据大集中导致风险集中爆发。随着近些年来，目标明确、精准打击的高级持续性威胁攻击行为带来越来越大的风险，电信运营商受到了越来越多更加隐蔽、更加深度的威胁。目前大数据平台、云计算环境尚处于起步阶段，基于新环境下的数据安全防护手段和措施仍然欠缺，同时由于大数据环境存在宝贵的海量数据资产，因此更容易成为不法分子的目标，带来大数据安全难题。

C.1.2 运营商数据安全对策

1、加强对大数据环境下客户信息保护的研究。为了使客户信息得到保护，电信运营商

必须要加强对大数据环境下客户信息保护的要求工作，深入探索大数据安全，开展大数据安全保障体系规划，同步推进大数据安全防护手段建设，保障大数据环境下安全可管可控。在治理大数据客户信息安全的过程中，需要从安全策略、安全管理、安全运营、安全技术、合规评测、服务支撑等层面，建立大数据客户信息安全管理总体方针，加强内部和第三方合作管理过程把控，强化数据安全运营和业务安全运营的过程要求，夯实对大数据平台系统的安全技术防护手段，定期开展大数据客户信息安全评估工作，强化大数据客户信息安全治理过程。

2、强化电信运营商对客户敏感信息的识别和分类、分级。当前阶段电信运营商的发展当中，存在着客户敏感信息识别难的问题，使电信运营商无法有效的对客户敏感信息进行针对性保管。因此，必须要改善这一现象。首先，以现有的管理平台为基础进行研究，建立能够自动识别、分类、标识客户信息的功能。其次，要根据客户信息的实际情况，制定出合理的识别标准，并且，在每一类标准当中，详细的阐述具体的管理方法。标准制定完成后，通过编程的方式将其融入到管理平台中。只有这样才能够在客户大量的信息中，有效的分析出敏感信息，并科学管理这些信息。

3、增强数据安全治理的建设。大数据背景下，电信运营商客户信息常常受到数据安全的威胁，想要增强客户信息的安全性，必须要增强数据安全治理体系的建设。首先，需要继续加强传统网络安全手段的建设，通过数据梳理、数据库防火墙、数据库审计、数据脱敏等基础数据安全设备构筑防护能力。其次，针对大数据的特殊环境进行研究，解决虚拟化、大数据共享、非关系型数据库安全等新型问题，作为传统网络防御手段的有效补充。最后，需要遵循国家针对大数据下安全标准，制定适合本行业科学、合理的标准，为大数据安全打下良好基础。

目前电信运营商数据安全治理具体实践内容参照如下：

C.1.3 电信数据安全治理具体实践

C.1.3.1 建立组织

构建大数据安全保障组

一、大数据安全保障工作组职责

1、负责制定大数据信息安全策略，明确信息安全目标。

2、组织相关平台负责人定期召开信息安全会议。

3、负责客户数据安全突发事件应急方案实施和大数据信息系统日常安全运行管理的组织协调及决策工作。

4、研究决定客户数据安全工作的重大事项。

二、大数据安全保障工作组责任

1、承担信息安全管理领导小组的具体工作，协助在大数据安全事务上的决策。

2、负责大数据安全管理体系的建立、实施和日常运行，起草信息安全政策，确定信息安全管理标准，督促各信息安全执行单位对于信息安全政策、措施的实施。

3、负责定期召开信息安全管理工作会议，定期总结运行情况以及安全事件记录，并向信息安全管理小组领导汇报。

4、负责制定大数据安全政策行为标准，并对违反信息安全政策的人员和事件进行确认和处罚。

5、负责调查大数据安全事件，并维护、总结安全事件记录报告。

C.1.3.2 建立总则

1、明确规范所保护的数据

针对最重要的政企客户信息和个人客户信息。

2、明确规范的目的

为了加强客户信息安全管理，规范客户信息访问的流程和用户访问权限以及规范承载客户信息的环境，降低客户信息被违法使用和传播的风险，特制定本规范。

3、明确规范所要解决的风险

客户信息安全面临的风险和威胁主要包括：因为权限管理与控制不当，导致客户信息被随意处置；因为流程设计与管理不当，导致客户信息被不当获取；因为安全管控措施落实不到位，导致客户信息被窃取等。

4、规范管理的对象

适用于客户信息的使用人员、运维人员、开发测试人员、管理人员和安全审计人员。

C.1.3.3 梳理职责

1、涉及客户信息的业务管理部职责

- 负责规范本部门访问客户信息的业务人员岗位角色及其职责；
- 负责主管的业务系统的客户敏感信息安全保护，建立落实管理制度和实施细则；
- 负责业务层面客户信息安全的日常管理和审计工作；
- 负责受理客户信息泄密事件的投诉、上报；
- 制订对业务合作伙伴的信息泄露的惩罚措施及具体实施；
- 协助完成客户信息泄密现象的市场调查；
- 协助进行客户信息泄密事件的查处。

2、人力资源部职责

- 组织有关员工签订保密承诺书；
- 及时发布人员岗位变动、离职的信息给帐号管理部门；
- 参与对客户信息泄密人员的查处。

C.1.3.4 数据分类分级

全面摸底，进行数据资产梳理、敏感数据发现及梳理、数据资产分级、用户及敏感资产权限梳理。

数据分级分类的原因：只有对数据进行有效分类，才能够避免一刀切的控制方式，在数据的安全管理上采用更加精细的措施，使数据在共享使用和安全使用之间获得平衡。

数据分级分类的原则：

分类：依据数据的来源、内容和用途对数据进行分类；

分级：按照数据的价值、内容的敏感程度、影响和分发范围不同对数据进行敏感级别划分。

数据分级分类内容：

信息类别	信息项	第三方价值	事故影响	分级定义
客户基本资料	政企客户资料	牟取暴利	造成政企客户流失，损失巨大	机密数据
	个人客户资料	价值较大	造成客户损失，损失大	敏感数据
	各类特殊名单	牟取暴利	造成投诉，损失大	敏感数据
身份鉴权信息	用户密码	牟取暴利	造成客户损失，损失巨大	机密数据
客户通信信息	详单	价值较大	造成投诉，损失大	敏感数据
	账单	价值一般	损失一般	普通数据
	客户当前位置信息	价值较大	损失一般	敏感数据
	客户消费信息	价值一般	损失一般	普通数据
	订购信息	价值低	无明显损失	普通数据
	增值业务订购关系	价值低	无明显损失	普通数据
	增值业务信息	牟取暴利	造成客户损失，损失巨大	敏感数据
客户通信内容信息	客户通信内容记录	牟取暴利	客户私密信息泄露，损失巨大	机密数据
	移动上网内容及记录	价值低	损失一般	普通数据
	增值业务客户行为记录	价值低	客户私密信息泄露，损失大	敏感数据
	领航平台交互信息	牟取暴利	损失一般	敏感数据

表 8　分类分级示意图

C.1.3.5 定义岗位角色与权限

角色 1：运营系统支撑

1）岗位包含举例：业务系统管理、系统运营支撑等细项岗位；

2）岗位说明：该类岗位角色主要指各省业务部门负责系统管理及支撑的岗位。

3）权限要求：该角色人员负责部门系统帐号、口令的管理，配合业支部门进行相应系统的开发、运营和维护，可以查看相应权限所涉及的客户敏感信息；仅具有查询权限，不应授予增加、删除、修改、批量导入与导出、批量开通与取消、批量下载等针对客户敏感信息的操作权限。

角色 2：开发测试

1）岗位包含举例：架构管理、系统设计、应用开发、应用测试、项目建设管理等；

2）岗位说明：该类岗位主要包括各省公司负责涉及客户敏感信息的系统的设计、研发、测试以及项目建设管理人员。

3）权限要求：开发测试人员原则上不能接触生产系统数据；开发测试人员仅具有测试系统的操作权限，开发测试系统需要涉及到客户敏感数据信息的内容，原则上使用过期数据

或是模糊化处理之后的数据。

C.1.3.6 建立账号与授权管理机制

1、业务账号管理

2、运维账号管理

1）系统运维支撑部门应指定专人（系统帐号管理员）负责运维帐号和权限的管理工作，制定岗位角色和权限的匹配规范，提供岗位角色和权限对应的矩阵列表，确保职责不相容。

2）运维人员应向上一级主管提出帐号权限申请，系统帐号管理员应按照权限最小化原则分配运维人员的帐号权限。

3）系统帐号管理人员要定期对系统帐号使用情况、权限、口令等进行检查稽核，确认帐号、权限的有效性，并对存在的问题进行整改。

3、第三方账号管理

C.1.3.7 建立客户敏感信息操作规范

1、业务人员对客户敏感信息操作的管理

1）涉及客户敏感信息的批量操作（批量查询、批量导入导出、批量为客户开通、取消或变更业务等），必须遵循相应的审批流程，通过业务管理部门审核；

2）业务人员因业务受理、投诉处理等情况下需要查询或获取客户信息时，应遵循如下要求：

a. 涉及客户普通资料的查询，服务营销人员要获得客户的同意，并且按照正常的鉴权流程通过身份认证。鉴权一般采取有效证件或服务密码验证，并保留业务受理单据。

b. 涉及客户通话详单、政企客户详细资料等客户敏感信息的查询，客户接触人员只能在响应客户请求时，并且客户自身按照正常流程通过身份鉴权的情况下，协助客户查询；禁止客户接触人员擅自进行查询；查询需保留业务受理单据。

c. 除客户接触外的业务人员，因投诉处理、营销策划、经营分析等工作需要查询和提取客户敏感信息的，业务管理部门应建立明确的操作审批流程，定期进行严密的事后稽核与审查。

d. 对敏感数据的批量操作，需要在指定地点、指定设备上进行操作，相关设备必须进行严格管控，对于该设备的打印、拷贝、邮件、文档共享、通讯工具等均需进行严格管控，防止数据泄露。

2、运维人员对客户敏感信息操作的管理

1）运维支撑部门需制定并维护业务系统层角色权限矩阵，明确生产运营、运行维护、开发测试等岗位对客户敏感信息的访问权限。

2）运维支撑人员因统计取数、批量业务操作对客户敏感信息查询、变更操作时必须有业务管理部门的相关公文，并经过部门领导审批。

3）运维支撑人员因应用优化、业务验证测试需要查询、修改客户敏感信息数据，只能利用测试号码进行各项测试，不得使用客户号码。

4）运维支撑人员因系统维护进行客户敏感信息的数据迁移（数据导入、导出、备份）必须填写操作申请，并经过部门主管审批。

5）严禁运维支撑人员向开发测试环境导出客户敏感信息，对需导出的信息必须经过申请审批，并进行模糊化处理。

6）对敏感数据的批量操作，需要在指定地点、指定设备上进行操作，相关设备必须进行严格管控，对于该设备的打印、拷贝、邮件、文档共享、通讯工具等均需进行严格管控，防止数据泄露。

3、数据抽取管理

1）各省、市公司数据需求部门由指定人员担任数据分析员，负责该部门的数据提取需求。

2）为确保数据安全，数据管理员不得将取数结果交付给非需求人员。非数据管理员不接收取数申请，也不得将提取数据直接发给相关需求人员。

3）数据分析员应对所提需求所涉及的客户信息进行审核并对需求内容作详细描述，数据管理员有责任进行复核并尽量减少客户敏感信息的提取。

4）数据提取部门不得将数据提取结果直接发给需求人员，数据提取结果必须为受控文档，并在指定平台上进行编辑和处理，不得存放在指定平台外的任何主机上。

5）受控文档是指采用加密、授权、数字水印、数字签名等技术手段对文档进行安全保护后的文档。

6）数据提取的检查稽核必须由专人负责，检查稽核人员应每月对日常数据提取情况进行检查稽核。

7）公检法等司法机关为满足司法取证等需要而查询客户信息时，应提交正式介绍信并进行留存，由相关主管领导批准后，方可提交业务支撑部门查询取数。

C.1.3.8 落实客户信息安全日常审查

1）安全检查主要分为操作稽核、合规性检查、日志审计、例行安全检查与风险评估。

2）信息安全管理责任部门针对安全检查过程中发现的突出问题，牵头协调各部门提出改进方案，并要求相关部门落实解决，并对改进措施落实情况进行跟踪检查。

3）操作稽核是对操作日志与工单等原始凭证进行比对，分析查找违规行为。

4） 合规性检查重点是依据本管理规范要求进行检查，检查相关要求的落地情况。

5）日志审计，对所有日志按关键功能、关键角色、关键帐号、关键参数，进行审计检查。及时发现异常时间登录、异常 IP 登录、异常的帐号增加和权限变更、客户信息增删改查、批量操作等敏感操作。

6）例行安全检查是指运维支撑部门对所负责维护的系统进行的常规性安全检查，包括

漏洞扫描、基线检查等。

7）风险评估侧重通过白客渗透测试技术，发现深层次安全问题，如缓冲区溢出等编程漏洞、业务流程漏洞、通信协议中存在的漏洞和弱口令等等。风险评估以各系统的运维支撑部门自评估为主、信息安全管理责任部门抽查相结合的方式进行。

C.1.3.9 落实客户信息系统的技术管控

根据现有体系，构建了大数据安全管控平台，提升对大数据安全管控技术能力。实现对大数据的安全状况摸底、数据使用管控，数据治理稽核等三方面管理。

安全状况摸底：旨在提升大数据平台自我免疫能力，并对数据进行分级分类管理和权限管理。

数据使用管控：对数据生命周期的分级分类、风险评估、业务访问、运维访问、测试开发、数据外发、数据存储等层面，提供技术资产梳理、风险评估扫描、数据防护、数据脱敏、数据水印、数据运维管控、数据加密、访问审计等方面技术融合。

数据治理稽核：通过审计、大数据分析、监测预警等技术，动态监测安全变化、事件变化、权限变化、策略变化，出现问题应急处置，构建大数据安全基线。

通过建立大数据安全管控平台，开展预防、发现、预警和协调处置等工作，维护电信运营商大数据安全，保障基础重要信息系统的安全运行。

C.1.4 实践总结

综上所述，电信数据安全治理实践，较为完备的覆盖了数据安全治理的各个领域，实现了数据的分级分类；制定了对不同组织和角色人员的数据安全职责和管理流程；明确了异常行为特征和重要风险行为的具体化管理要求；突破了传统防外的思维，实现了基于业务角度出发的业务侧、运维侧和第三方的综合管理，具有较高的可操作性。

教育部数据安全治理实践

教育部为全面加强网络安全，推进教育信息化引入了数据治理理念，但是鉴于教育行业数据敏感、业务特殊、系统繁杂等特性，在数据治理过程中同样面临着严峻的考验。

教育部数据安全治理现状与挑战

教育部业务种类众多，信息化系统涉及数百个应用系统和数据库做支撑。这对存在海量数据资产的教育部来说，如何发现有价值的数据，做到全量的盘点和梳理，对存在的敏感数据使用情况进行管理和管控来说，变得尤为困难。这些不足直接导致了现阶段教育部信息化建设无法正确决策后续数据安全建设方向和防控策略。目前，教育部数据安全主要存在如下

不足：

（1）教育部在涉及数据安全防护中对数据的使用、流动、敏感数据范围和分布都缺少全面的掌控，这就造成教育部以往对数据安全手段是采取“完全封闭”的态度和措施。

（2）教育部对数据保护的主要防护手段，依靠传统的网络防火墙、入侵防御等网络安全产品进行防护，而这些传统的安全防护体系，对数据库这个层面的防护力度还不完善。

教育部数据安全治理具体实践

教育部将数据安全治理工作合理划分为四步骤：

（1）全面梳理教育部各系统的敏感数据资产；

（2）制定教育行业的数据安全管理规范；

（3）选择教育行业的数据安全治理技术；

（4）开展教育行业的数据安全落地稽核。

梳理敏感数据的资产

教育部拥有着庞大且错纵复杂的业务系统，进行资产梳理的目的是：扫描检测数据资产，梳理数据库分布情况，通过扫描发现敏感数据，并对资产的访问热度做出分析，协助教育部完成数据等级分类，合理规范使用教育数据资产。

此阶段数据梳理主要工作内容如下：

1. 数据资产梳理，主要包括：数据库、表、字段；
2. 针对敏感数据的分布情况梳理、访问情况梳理、授权情况梳理；
3. 当前环境下数据安全措施、产品、工具的梳理；
4. 评估当前环境下数据安全风险；

制定数据安全治理规范

数据的安全始于数据资产梳理，资产梳理是数据安全治理的第一步建设。完成梳理后需要按照教育部领导及技术专家的指示，贯彻教育部办公厅关于印发《教育部机关及直属事业单位教育数据管理办法》的通知，并依据资产梳理过程中的成果，建立了《教育数据安全管理规范》。

确立符合行业需求的数据治理技术

基于数据梳理的成果，将学籍数据、教师、校舍、学生资助数据作为海量数据重中之重，作为教育部第一阶段数据治理重点关注的对象。

在治理过程中，将数据表中涉及的“姓名”、“身份证号”、“地址”作为条件，分级别建立数据治理方案：

1. 数据表同时含有三个因素，级别★★★，采用数据加密保护手段；
2. 数据表同时含有其中两个因素，级别★★，建议采用数据脱敏保护手段；
3. 数据表只含有其中一个因素，级别★，建议采用数据运维管控保护手段；
4. 其中针对数据脱敏功能，选择了两种数据脱敏保护手段：

静态脱敏：对于教育部生产重要数据，在开发、测试环境使用进行数据演练和测试时候采用静态仿真脱敏方式。

动态脱敏：教育部领导定期检查系统报表信息，领导对系统查看要求实时性检查，对人员敏感信息进行遮蔽处理，防止数据泄露。

数据安全落地稽核

数据治理稽核目的是监督数据安全落实情况，针对数据在使用访问过程中潜在风险进行预警，利用数据库审计和数据态势感知技术做好数据的安全稽核与风险预警。将监控的所有节点实时上传至监控统一平台，平台系统监测节点状态，业务流向；将分析发现的可疑威胁源与高风险事件，进行持续跟踪分析，并结合历史告警事件进行关联分析，挖掘隐藏的真正威胁。

实践总结

数据安全治理是一项复杂的系统工程、教育部通过数据安全治理实践成果，提升了信息化综合管理的水平。同时，对推进政务信息资源整合和数据共享，提升政府信息资源再配置、再利用有着深远意义。

市政务云数据治理实践

2017 年以来，青岛市先后制发了《青岛市人民政府关于促进大数据发展的实施意见》、《青岛市大数据、云计算服务产业发展行动计划》，旨在建设与城市发展目标相适应并具有较强影响力的“大数据集散服务中心、研发创新中心、应用引领中心和产业集聚高地”，形成“三中心一高地”大数据发展目标。在推进政务云平台的同时，引入“数据治理”理念推进政务云平台合规化发展。

市政务云面临的挑战

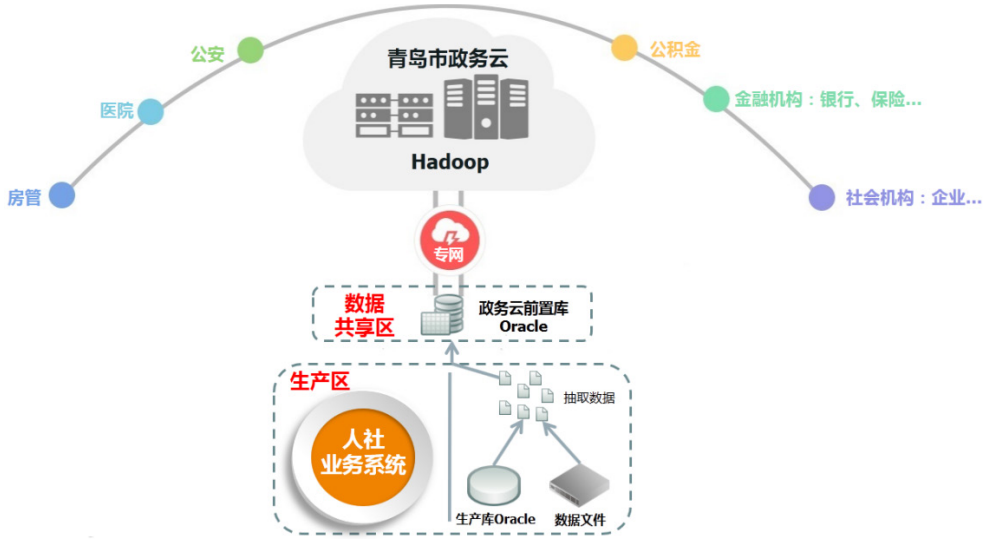


图 27　市政务云平台架构图

市政务云平台的建设目标是将市政府下属各委、办、局的数据共享到大数据与云计算平台，从而进行数据共享、数据互通和数据统一存储。因此，市政务云平台面临如下挑战：

个人信息泄露风险：由于需要将生产库数据定期同步给政务云平台，如果不经数据脱敏直接上传，数据的安全性将不受管控。因此，需要将共享给政务云的个人隐私信息进行数据脱敏处理。

敏感数据多、脱敏难度大：生产库大量数据表都涉及十几个字段要求脱敏，并且其中涉及的组织机构代码和身份证号需要在脱敏的同时保证数据的仿真度，因此工作难度极大。

合规性要求多：政务数据共享不仅要满足国家层面的《网络安全法》、《等级保护》等法律法规要求，并且需要满足地方级《青岛市人民政府关于促进大数据发展的实施意见》、《青岛市大数据、云计算服务产业发展行动计划》等全市性规划文件要求。

市政务云数据治理具体实践

数据治理过程中，采用了数据特征学习以及 SQL 语句处理技术。

基于敏感特征发现数据库敏感数据

1. 设置敏感样例数据：识别获取数据库中的样例数据，通过对包含个人敏感信息的数据类型（字符、数值等）和数据内容进行敏感数据识别。

2. 发现敏感数据：个人敏感数据的识别由动态敏感数据识别引擎完成，动态敏感数据识别引擎采用规则、特征库以及 SQL 语句处理，对包含个人敏感信息的数据进行识别、特征提取从而进行智能发现。

基于通讯协议脱敏

自动识别语句中个人数据：可对政务云应用程序执行的 SQL 语句进行自动识别，通过敏感信息特征库发现语句中包含的个人敏感信息。

根据个人字段自动改写语句：根据 SQL 语句语义，查找需要脱敏处理的个人字段进行脱敏函数替换，从而对 SQL 语句进行改写。

动态脱敏个人敏感数据：改写完毕，将修改后的语句提交到前置库执行，前置库将脱敏后的结果返回给政务云平台，此时政务云平台获取的数据均是脱敏后的数据。

实践总结

本次数据治理从实际的安全需求出发，并依据市政务云安全需求进行安全设计、实施、建设。从整体上、全过程、全周期、动态的为市政务云平台提供安全保障，符合政务大数据局对信息系统机密性、完整性、可用性、可审查性等安全性要求，并提升政务数据交换的安全等级。

国家电网数据安全治理实践

国家电网公司在 2019 年两会期间提出要全力打造“三型两网 世界一流”的企业，随着泛在电力物联网的建设，国家电网信息化建设必然打破传统的数据孤岛，转而走向共享、开放。因此，国家电网大数据将呈现日益活跃的“流动”趋势，在“流动”中发挥价值。必然驱动数据的有序流动、合理利用和安全分享。

但是，在数据“流动”的过程中，存在诸多隐患问题：对个体而言，特别关心数据的隐私泄露问题；对主管部门来说，则关心数据是否“健康”，也即数据是否真实、完整、可信，关心数据使用过程中等是否会被批量泄露和篡改。数据安全治理，已经成为了国家电网业务部门与安全部门共同的核心关切点。

国家电网数据安全治理面临挑战

随着国家电网公司智能电网技术的深化应用和“三集五大”管理体系的全面建设，信息系统已全面融入公司生产经营管理业务的各个方面，积累了大量的结构化数据、非结构化数据、海量历史准实时数据和地理信息数据。数据的安全性已经迫在眉睫：

图 28　国网数据安全挑战

数据繁多复杂：随着国家电网公司“业务贯通 数据共享”的发展思路逐渐深入落实，国网公司各单位的数据体量越来越大，并且数据的种类越来越多，作为数据的管理部门很难清晰地、系统地认识当前的数据现状，无法为数据的安全管理提出有效且可行的措施保障。因此，无论在安全层面还是在管理层面都给国网公司提出了巨大挑战。

数据集中存储风险：当前国家电网公司的数据呈集中化存储趋势，而在数据的存储层当前基本没有有效的保护措施，在数据库中重要敏感的数据都是以明文的方式存储。那么一旦黑客通过攻击手段形成“脱库”或者后台运维人员通过权限滥用将数据文件拷走，都将直接

形成数据的全部泄露。

第三方服务风险：国家电网公司的业务系统繁多，系统的运维压力巨大，因此国网公司众多业务系统的运行维护大多交由第三方服务商。而第三方服务商本身在安全管理方面普遍偏弱，但第三方服务商却掌管着系统中重要数据的访问权限，那么由于利益的驱使，则存在数据被三方服务商误用、滥用甚至泄露的风险。

共享与分发风险：随着“业务贯通 数据共享”的发展思路逐渐深入落实，国家电网公司会将大量的业务数据、个人隐私数据进行部门间共享以及面向外部机构的数据分发，那么如何平衡数据共享、分发与数据安全之间的利与弊，是国家电网公司进行数据安全治理工作的核心环节。

新技术风险：随着国家电网全业务统一数据中心以及大数据中心的建立，更多的大数据技术已经得到应用，而 Hadoop 体系中的数据存储组件，如 HBase、Hive、Mongodb 这些 NoSQL 数据库，其自身的安全性就相对薄弱，因此针对 NoSQL 数据库这类新技术的安全管理也是国网公司面临的挑战之一。

政策性要求：国家电网公司作为国内重要的能源企业，自身也要遵循国家层面、行业层面、监管层面、公司层面各项关于数据安全的政策法规。

国家电网数据安全治理具体实践

建立数据安全治理组织保障体系

首先，国家电网在数据安全治理的组织保障上开始入手，形成了“三级垂直组织管理保障”体系。

第一级，国家电网总部安全部门牵头，负责制定数据安全总体方针、重大政策和重大事项，并提出了“谁主管谁负责，谁运行谁负责，谁使用谁负责，管业务必须管安全”的总体原则。

第二级，省公司牵头，以总部的数据安全方针为指引结合本省公司的数据安全现状，制定数据安全治理可落地的技术与管理办法，建立具体的数据安全治理运营体系。

第三级，省公司业务部门牵头，负责具体的技术与管理措施的落地。

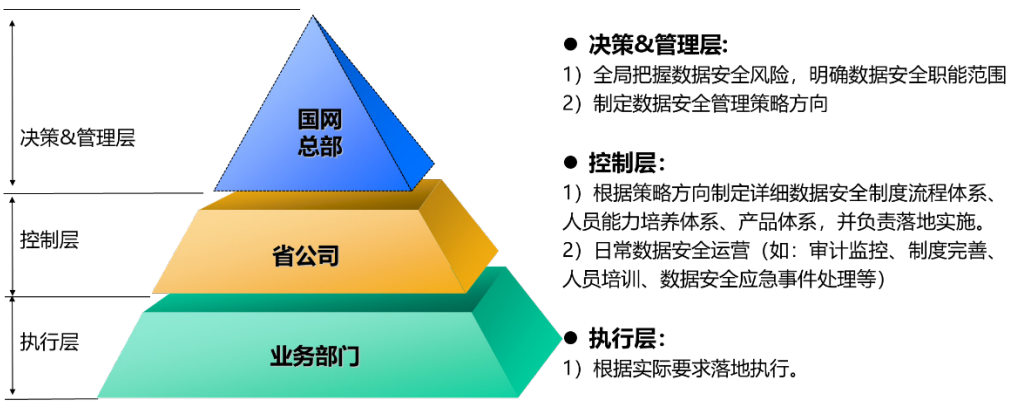


图 29　国家电网数据安全治理组织保障体系

建立数据安全治理管理保障体系

其次，国家电网在数据安全治理的制度保障上持续跟进，建立了一系列数据安全相关的管理制度：

《关于加强对外提供数据规范管理的指导意见》

重点提出了数据在面向国家电网外部单位提供数据时的流程规范以及提供数据应采取具体技术措施的细则；

《国家电网客服服务中心数据导出实施细则》

重点提出了客服中心导出敏感数据并提供给外部单位时的业务流程以及应遵循的管理要求；

《国家电网公司关于进一步加强数据安全工作的通知》国家电网信通【2017】65 号

重点提出了国家电网公司在全生命周期过程中应采取的技术措施以及管理办法；

《国网营销部关于加强营销专业网络与信息安全管理的工作意见》 营销综【2017】4 号

重点提出了国网营销系统应提供加密、脱敏、访问控制等管控措施以及具体要求。

《营销专业客户敏感信息脱敏规范》营销综【2017】65 号

重点提出了国网营销系统的脱敏要求，具体到营销系统客户敏感信息 6 大类 23 子项数据类型的划分依据以及具体的脱敏方法及规则要求。

建立数据安全治理技术保障体系

定期进行数据安全督查 发掘数据安全隐患

国家电网各省公司安全督查相关部门定期对公司内部各信息系统、数据库系统进行安全督查，通过专业的检查工具对数据库系统的安全漏洞以及安全配置基线进行安全检查，并将检查结果通报被检单位。被检单位将根据检查结果进行安全漏洞的修复以及安全配置调整，并接受复查。

构建主动数据防护机制 抵御非法数据窃取

根据业务部门以及安全部门需求调研，明确其业务开展必须的数据访问权限，形成《数据访问权限矩阵》通过对重要数据建立增强级访问控制，针对业务访问、运维访问环节实施精准防护，针对不同角色用户在访问数据对象时进行不同力度的安全防护，并细化到数据表、字段级。

业务数据访问管控 敏感数据细粒度防护

针对国家电网营销系统，国网营销部发文（营销综【2017】65 号）要求针对前台业务人员访问以及运维人员访问营销系统客户敏感数据进行脱敏防护。通过对业务人员数据以及客户敏感数据梳理，将业务人员分为不同等级以及不同的角色，按照“数据访问最小化原则”，在不影响业务正常开展的前提下，最大化实施客户敏感数据脱敏。

强化数据操作行为审计 落实数据访问稽核

国家电网公司全面推广实施数据库审计，针对核心业务系统的数据库操作行为进行精准记录的同时，进行了数据库审计深化应用，推广并实施了数据库审计典设，针对敏感表操作、攻击行为检测、违规操作检测、异常登录检测等典型场景进行了细化风险分析，达到了实时洞悉数据库安全风险的目标。

实践总结

国家电网公司近年来持续进行数据安全治理工作，从组织保障、制度保障、技术保障三方面持续加强并深化，通过在实践过程中发现不足并弥补不足。随着坚强智能电网深入应用以及泛在电力物联网的建设，对于国家电网公司而言是机遇亦是挑战。但可以肯定的是，数据的安全问题将愈加凸显，而彻底贯彻数据安全治理工作思路势必将国家电网公司整体的数据安全水平提升到一个新的台阶。

附件 D　数据安全生态环境

全球数据安全现状

2018 年 5 月，Verizon 发布“数据泄露调查报告”（DBIR），对包括 65 个国家的数据泄露样本进行统计和分析结果如下：

安全事件：近一年内全球范围内共发生 53,308 次安全事件，2,216 次数据泄露。

犯罪目的：76% 的数据泄露事件以金钱为目的。勒索软件在恶意软件中居首，占比 39%。

威胁来源：几乎四分之三（73%）的网络攻击来自外部人员，超过四分之一（28%）涉及内部人员的窃取，由于很难发现犯罪迹象，这部分内部泄露行为更加难以防范。

安全意识：有 4% 的人会点击网络钓鱼攻击；有 68% 的漏洞需要数月甚至更长时间才能发现。

各行业发生的安全事件及数据泄露事件占比：

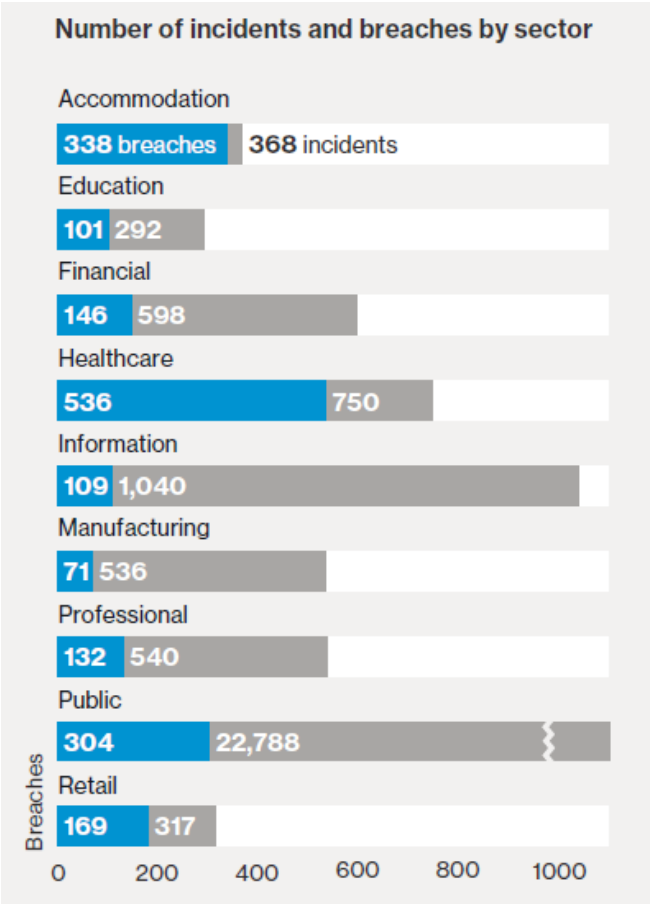


图 30　安全时间及数据泄露占比

安全风险：94%的安全事件和 90%被证实的数据泄露事件来源于这九类安全问题：

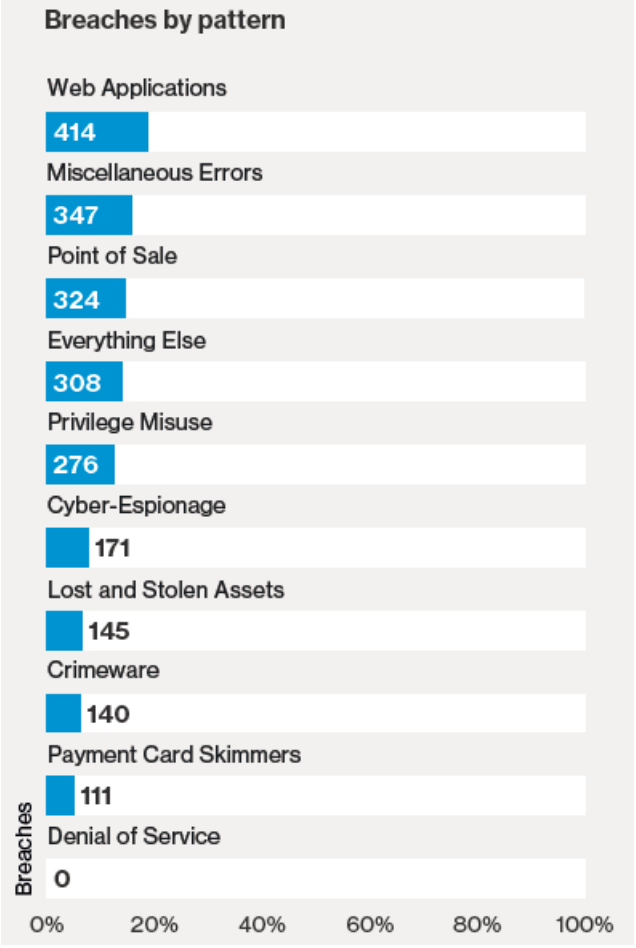


图 31　主要安全问题占比

国内外重要数据安全事件列举

万豪集团 5 亿用户数据或外泄

事件描述

2018 年 11 月，万豪官方微博公开发布声明，称“2018 年 9 月 10 日及之前喜达屋旗下酒店预定数据库中的宾客信息曾在未授权的情况下被访问”。12 月 8 日，万豪国际收到一条内部安全工具发出的告警，经调查 “自 2014 年起，即存在第三方对喜达屋网络未经授权的访问”。这意味着，近几年预定该酒店的最多约 5 亿名用户的信息或被泄露。此次外泄的数据包括姓名、电话号码、电子邮件、护照号码、SPG 俱乐部帐号、支付卡号和支付卡有效期等。

事件分析

本次泄露事件早在 2014 年就开始。潜伏了约 4 年才被发现。提升威胁监测能力，尽早发现潜藏的未知威胁，缩短发现入侵的时间差（dwell time），是攻防对抗中的关键。

台积电遭勒索病毒 3 天损失 17.6 亿元

事件描述

2018 年 8 月 2 日傍晚，全球芯片头号代工厂台积电（TSMC）遭遇勒索病毒 Wannacry 入侵，并于当晚 10 点左右快速扩散至三大重要生产基地，生产线全数停摆。后官网发布声明，称入侵事件起因为新机台在安装软件的过程中操作失误，病毒在新机台连接到台积电内部电脑网路时发生了病毒扩散，并预计在关键的 60 小时“排毒行动”后有望全数排除电脑病毒。

因比预期慢了约一天，对台积电营收的影响也比预期要大，预计约造成 87 亿元新台币（约合人民币 17.6 亿元）损失。同时，股价受勒索病毒影响，短时间内蒸发 78 亿。

事件分析

本次勒索病毒等网络入侵是有一台新加入网络的电脑开始。短短几个小时之内勒索病毒就扩散至整个内网环境。最终导致生产线全面瘫痪。接入新机器尤其在安装新软件之后一定要做安全检测和安全加固。否则可能就是 87 亿的经济损失。

华住旗下酒店 5 亿条信息泄露

事件描述

2018 年 8 月，媒体爆料华住旗下连锁酒店开房数据在暗网被明码标价公开售卖，包括华住旗下汉庭、桔子、全季、宜必思、诺富特、海友等酒店。被泄露的数据为华住官网注册资料、酒店入住登记身份信息和酒店开房记录，内容包括姓名、手机号、邮箱、身份证号码等，共计 140G 约 5 亿条信息。

经业内人士对出售者提供的测试数据进行验证后，确认真实性非常高。此事可能成为国内近几年规模最大且最严重的信息泄露事件。

事件分析

拖取 140G 数据是以天或周为单位的一个过程。大量数据的长时间持续窃取是黑产灰产链条中必不可少的环节，多数利用免杀或合法用户非法访问来实现。通过数据安全治理，构建业务访问规则，监测越界行为是治本之道。

Exactis 或泄露 2.3 亿人隐私数据

事件描述

2018 年 6 月，安全研究员 Vinny Troia 梳理数据库时发现，来自数据代理商 Exactis 的包含 3.4 亿条记录的数据库暴露在可公开访问的服务器上。这 2TB 大的数据库几乎囊括了所有美国公民，且包含非常详细的个人信息。除电话号码、家庭住址、电子邮箱等外，每条记录还包含超过 400 种各类具体特征，比如是否吸烟、宗教信仰、有无宠物等。

虽然数据库中不包含财务信息或身份证号，不能直接用来进行身份盗窃，但其所含个人

信息的深度，能为其他形式的社会工程欺诈提供帮助。

事件分析

本例是标准的低级配置失误导致。公司采集完数据后，并未对数据进行妥善处理。未加任何防护的放在互联网上。以至于不用任何技术就可以轻易获得其中的内容。责任心和安全管理同样也是数据安全的重要组成部分。

Aadhaar 中 11 亿公民信息遭泄露

事件描述

2018 年 1 月，印度国家身份认证系统 Aadhaar 被曝遭网络攻击，数据被明码标价出售。论坛报业集团（Tribune News Service）记者证实，支付 500 卢比（约 48 元人民币）后，可输入任何 Aadhaar 号码检索相关信息，包括姓名、住址、照片、电话号码和邮箱地址等。

Aadhaar 是世界上最庞大最复杂的生物身份识别系统（UID），截止至 2017 年 2 月已采集印度 11.2 亿人的生物识别数据（包括照片、指纹及虹膜等），并提供独一无二的身份证明编号。同时，Aadhaar 号码与银行账户、手机号码、保险账户等进行了绑定。

事件分析

安全已经成为国家的硬实力之一。黑客早已是有组织有计划的团体作战。而且现今数据安全已经上升到国家层面。数据安全早已不是个人的安全问题，而是国家的安全问题。现在的安全问题绝不能向以前一样 “头疼医头，脚痛医脚”，而是应该从整个安全架构体系出发构建整体的安全治理方案，来对抗敌对黑客的入侵行为。

国泰航空 940 万乘客信息遭泄露

事件描述

国泰航空 2018 年 10 月 24 日发布公告：发现公司及其全资子公司港龙航空有限公司的部分乘客资料曾被未获授权取览。公司知悉大约九百四十万位乘客的资料曾被不当取览。受到未获授权取览的个人资料包括乘客姓名、国籍、出生日期、电话号码、电邮及实际地址、护照号码、身份证号码、飞行常客计划会员号码、顾客服务备注及过往的飞行记录资料。此外，有 403 张已逾期的信用卡号码曾被不当取览。另有 27 张无安全码的信用卡号码曾被不当取览。

事件分析

信息安全已上升到国家战略层面，民航信息安全同样不可忽视。国泰航空 3 月份已经发现系统遭到入侵，但 5 月份依旧存在数据被非法取览。国泰航空响应含糊，无论 3 月份的发现还是 5 月份的发现都未报案或向香港私隐专员公署和受影响用户通报。企业在发展的同时，更要关注自身的安全。保护用户的数据安全，既是企业的责任，更是企业的义务。

驱动人生木马 2 小时感染十万电脑

事件描述

2018 年 12 月 14 日一款通过“驱动人生”升级通道的木马突然爆发，仅 2 小时内就攻击用户电脑 10 万多台。值得注意的是，因为这款木马病毒会利用高危漏洞在企业内网呈蠕虫式传播，并进一步下载云控木马，对企业信息安全威胁巨大。

事件分析

这是一起标准的供应链攻击。驱动人生系列软件的升级服务器地址被劫持成攻击者的 CC 服务器。用户正常升级驱动人生就会导致下载木马。木马会收集用户个人信息，并同时进行挖矿。此外还会尝试暴力破解 sqlserver 密码，控制用户数据。攻击往往来自于信任的渠道。提高整体的安全能力，才是安全之道。

AI 安防企业泄露 680 万条个人数据

事件描述

2019 年 2 月中旬，有网络安全研究人士发现，提供人脸检测和人群分析服务的中国科技公司 SenseNets(深网视界) 的人脸识别数据库缺乏密码保护，导致大规模的数据泄露。据称，该数据库包含了超过 256 万用户的记录，包括身份证号码、地址、出生日期、照片、工作单位，能够识别用户身份的位置信息等高度敏感的隐私信息。

事件分析

企业在发展时，如果只注重业务，而不注重安全。很容易在发展过程中遭遇滑铁卢事件。届时失去的不光是业务，失去的将是市场和客户的信任。深网视界的例子就是一则经典的独角兽企业被安全打垮的例子。向前一小步，安全一大步。

Mongodb、CouchDB、Hadoop 等非关系数据库勒索事件

事件描述

随着云的迅猛发展云上数据库越来越流行。一起针对云上非关系型数据库的攻击悄然而至。三个黑客团伙劫持了 MongoDB 逾 26000 多台服务器，其中规模最大的一组超过 22000 台。短短几天后黑客组织 NODATA4U 又勒索了 115 台 Hadoop。

事件分析

非关系型数据库部署之后除了要做性能优化等工作之外一定要开启自身的安全参数。大部分非关系型数据库默认是不开启身份验证功能的。导致黑客一旦获取非关系型数据库的 ip 和端口就能以最高权限登陆数据库，转移数据实施勒索。所以最后一定不要忘记至少开启安全参数，保护您的数据安全。

云上 mysql 数据库勒索事件

事件描述

随着云的发展，大量部署的不光是非关系型数据库。还有 Mysql 数据库。于是黑客的手也向着 mysql 数据库伸出。2018 年初黑客利用自动化脚本，利用弱口令、漏洞等方式攻破大量云上 mysql 数据库从而获得百万级的数据，并实施勒索。

事件分析

云给企业带来了便利，但同时也改变了软件部署环境。新环境必然会有新的安全挑战。如何让数据库这种内网产品快速适应云上环境，解决潜在安全问题。既是数据库厂商需要思考的问题更是数据运营者需要思考的问题。必须抛弃数据库固若金汤的幻想，踏下心来一步一步以数据库为核心构建安全防护体系。

Oracle Rushql 勒索病毒

事件描述

2016 年开始中国发生多起针对 Oracle 数据库的勒索病毒案例。该病毒捆绑在被感染的绿色版 / 破解版 PS/SLQ developer 安装程序上，一旦用户连接到数据库，就会立即执行“Afterconnet.sql”中的代码，在用户的数据库中创建多个存储过程和触发器，并判断数据库创建时间是否大于 1200 天。如果大于 1200 天，重启数据库后会触发病毒触发器，加密并删除 sys.tab$，导致用户无法访问数据库中所有的数据库对象集合（schema），提示“你的数据库已经被 SQL RUSH Team 锁死，请发送 5 个比特币到这个地址……”的勒索信息，并设置定时任务，如果在期限内不交赎金，就删除所有的表。该病毒在感染 Oracle 数据库后不会立即触发，具有较长的潜伏期。

事件分析

本 Oracle 数据库勒索病毒，追根溯源是由于用户缺乏软件安全意识、下载了破解版 PL/SQL 导致。希望大家能提高安全意识，具体建议如下：采用正版软件，规避未知风险。检查数据库工具的使用情况，避免使用来历不明的工具产品；加强数据库的权限管控、生产环境和测试环境隔离，严格管控开发和运维工具；定期进行产品安全风险评估，将风险评估工作规范化，例行化。

Facebook 数据泄露事件

事件描述

2018 年 3 月 17 日，据美国纽约时报和英国观察者报 (英国卫报的周日版) 联合曝光，Facebook 上超过 5000 万用户信息数据被一家名为“剑桥分析”(Cambridge Analytica) 的公司泄露，用于在 2016 年美国总统大选中针对目标受众推送广告，从而影响大选结果，此事在

世界范围内引发了轩然大波。

而 Facebook 这 5000 万用户数据是什么概念，接近 Facebook 美国活跃用户总数的三分之一，美国选民人数的四分之一。

事件分析

这次超大规模的数据泄露事件的根本原因就在于 Facebook 作为数据的采集和拥有者，在数据安全管理方面存在漏洞，主要表现在两方面，一是：欠缺对第三方获取用户数据目的的必要审查；二是，对第三方使用用户数据缺乏有效监控。

Wannacry 蠕虫勒索软件事件

事件描述

2017 年 5 月 12 日晚，Wannacry 勒索软件袭击了全球，至少有上百个国家和上千个企业及组织受到了该勒索软件的影响。

图 32　Wannacry 勒索攻击现场截图

该勒索软件被认为是一种蠕虫病毒的变种（也被称为“Wanna Decrypt0r”、“Wanna Cryptor”或“ Wcry”），勒索病毒结合了蠕虫的方式进行传播，传播方式采用了 NSA 被泄露出来的 MS17-010 漏洞。一旦电脑感染了 Wannacry 病毒，电脑中的数据就会被加密，并且会在被加密文件上添加“WCRY”的扩展名，从而造成电脑无法使用。之后勒索人会要求受害者支付一定的比特币后才能解锁文件。

事件分析

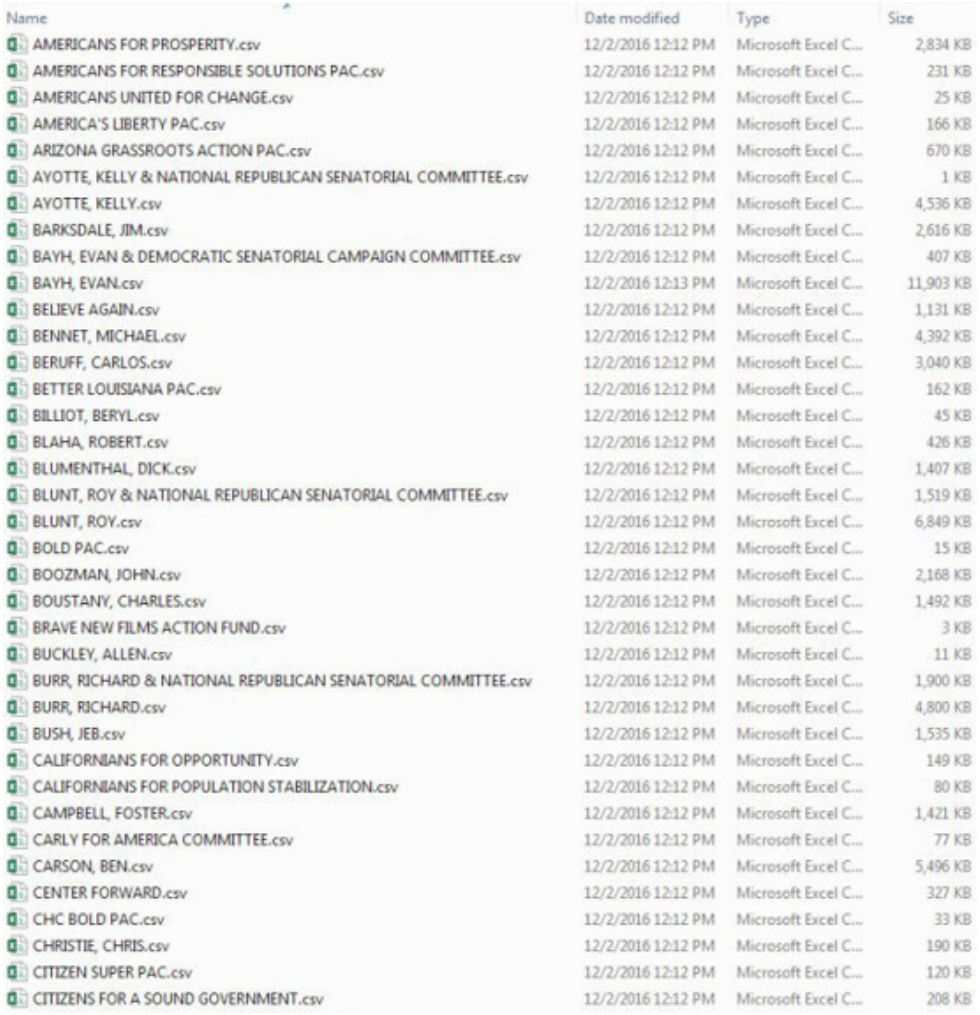
在 NSA 泄露的文件中，Wannacry 传播方式的漏洞利用代码被称为“EternalBlue”，所以也有的报道称此次攻击为“永恒之蓝”。其中 ETERNALBLUE 模块是 SMB 漏洞利用程序，

可以攻击开放了 445 端口的 Windows 机器，实现远程命令执行。 蠕虫软件正是利用 SMB 服务器漏洞，通过 2008 R2 渗透到未打补丁的 Windows XP 版本计算机中，实现大规模迅速传播。

美国 2 亿选民个人资料泄露事件

事件描述

2017 年 6 月爆出美国共和党签订的营销公司在一个可公开访问的亚马逊服务器上存储内部文件，导致超过 1.98 亿美国公民的个人数据泄露 ，这些数据包含大约 61% 的美国公民大量个人信息，除了家庭地址，出生日期和电话号码之外，这些记录还包括政治团体采用的先进情绪分析系统来预测个人选民如何处理热门政治话题，如枪支所有权、干细胞研究和堕胎权，以及宗教信仰和种族问题等，安全专家们认为这是美国历史上规模最大的选民信息泄露事件。



Name	Date modified	Type	Size
AMERICANS FOR PROSPERITY.csv	12/2/2016 12:12 PM	Microsoft Excel C...	2,834 KB
AMERICANS FOR RESPONSIBLE SOLUTIONS PAC.csv	12/2/2016 12:12 PM	Microsoft Excel C...	231 KB
AMERICANS UNITED FOR CHANGE.csv	12/2/2016 12:12 PM	Microsoft Excel C...	25 KB
AMERICA'S LIBERTY PAC.csv	12/2/2016 12:12 PM	Microsoft Excel C...	166 KB
ARIZONA GRASSROOTS ACTION PAC.csv	12/2/2016 12:12 PM	Microsoft Excel C...	670 KB
AYOTTE, KELLY & NATIONAL REPUBLICAN SENATORIAL COMMITTEE.csv	12/2/2016 12:12 PM	Microsoft Excel C...	1 KB
AYOTTE, KELLY.csv	12/2/2016 12:12 PM	Microsoft Excel C...	4,536 KB
BARKSDALE, JIM.csv	12/2/2016 12:12 PM	Microsoft Excel C...	2,616 KB
BAYH, EVAN & DEMOCRATIC SENATORIAL CAMPAIGN COMMITTEE.csv	12/2/2016 12:12 PM	Microsoft Excel C...	407 KB
BAYH, EVAN.csv	12/2/2016 12:13 PM	Microsoft Excel C...	11,903 KB
BELIEVE AGAIN.csv	12/2/2016 12:12 PM	Microsoft Excel C...	1,131 KB
BENNET, MICHAEL.csv	12/2/2016 12:12 PM	Microsoft Excel C...	4,392 KB
BERUFF, CARLOS.csv	12/2/2016 12:12 PM	Microsoft Excel C...	3,040 KB
BETTER LOUISIANA PAC.csv	12/2/2016 12:12 PM	Microsoft Excel C...	162 KB
BILLIOT, BERYL.csv	12/2/2016 12:12 PM	Microsoft Excel C...	45 KB
BLAHA, ROBERT.csv	12/2/2016 12:12 PM	Microsoft Excel C...	426 KB
BLUMENTHAL, DICK.csv	12/2/2016 12:12 PM	Microsoft Excel C...	1,407 KB
BLUNT, ROY & NATIONAL REPUBLICAN SENATORIAL COMMITTEE.csv	12/2/2016 12:12 PM	Microsoft Excel C...	1,519 KB
BLUNT, ROY.csv	12/2/2016 12:12 PM	Microsoft Excel C...	6,849 KB
BOLD PAC.csv	12/2/2016 12:12 PM	Microsoft Excel C...	15 KB
BOOZMAN, JOHN.csv	12/2/2016 12:12 PM	Microsoft Excel C...	2,168 KB
BOUSTANY, CHARLES.csv	12/2/2016 12:12 PM	Microsoft Excel C...	1,492 KB
BRAVE NEW FILMS ACTION FUND.csv	12/2/2016 12:12 PM	Microsoft Excel C...	3 KB
BUCKLEY, ALLEN.csv	12/2/2016 12:12 PM	Microsoft Excel C...	11 KB
BURR, RICHARD & NATIONAL REPUBLICAN SENATORIAL COMMITTEE.csv	12/2/2016 12:12 PM	Microsoft Excel C...	1,900 KB
BURR, RICHARD.csv	12/2/2016 12:12 PM	Microsoft Excel C...	4,800 KB
BUSH, JEB.csv	12/2/2016 12:12 PM	Microsoft Excel C...	1,535 KB
CALIFORNIANS FOR OPPORTUNITY.csv	12/2/2016 12:12 PM	Microsoft Excel C...	149 KB
CALIFORNIANS FOR POPULATION STABILIZATION.csv	12/2/2016 12:12 PM	Microsoft Excel C...	80 KB
CAMPBELL, FOSTER.csv	12/2/2016 12:12 PM	Microsoft Excel C...	1,421 KB
CARLY FOR AMERICA COMMITTEE.csv	12/2/2016 12:12 PM	Microsoft Excel C...	77 KB
CARSON, BEN.csv	12/2/2016 12:12 PM	Microsoft Excel C...	5,496 KB
CENTER FORWARD.csv	12/2/2016 12:12 PM	Microsoft Excel C...	327 KB
CHC BOLD PAC.csv	12/2/2016 12:12 PM	Microsoft Excel C...	33 KB
CHRISTIE, CHRIS.csv	12/2/2016 12:12 PM	Microsoft Excel C...	190 KB
CITIZEN SUPER PAC.csv	12/2/2016 12:12 PM	Microsoft Excel C...	120 KB
CITIZENS FOR A SOUND GOVERNMENT.csv	12/2/2016 12:12 PM	Microsoft Excel C...	208 KB

图 33　被泄露的选民信息数据库文件

事件分析

造成如此严重的信息泄露事件，是因为受雇于共和党的一家网络数据供应商 Deep Root

Analytics 将这些数据存储在了可公开访问的亚马逊云服务器上，并且没有设置密码，任何人都可以访问。这突显出组织机构在使用云存储的时候，如果缺乏必要的安全策略和配置，会存在很大的风险。

瑞士最大电信运营商信息泄露事件 80 万用户数据被盗

事件描述

“瑞士资讯”2018 年 2 月 7 日报道，瑞士最大的电信运营商 Swisscom 日前宣布，有 80 万用户的数据信息在 2017 年秋季被盗取。瑞士电信在一份公告中称，被窃取的主要包括姓名、地址、电话号码、出生日期等。而密码、通话内容和账务数据等信息因采取了更严密的保护措施未被泄露。

事件分析

本次泄露事件并非由于外部黑客攻击，而是被一个销售合作公司窃取了相关信息。这一泄露事件的原因同样是因为作为数据的采集和拥有者在数据安全管理方面存在漏洞，致使第三方合作机构轻易的获取到了用户数据，从而造成了数据泄露。

美国征信巨头 Equifax 数据泄露事件

事件描述

2017 年 9 月，美国三大老牌征信机构 Equifax 被爆出泄露了 1.43 亿用户信用记录，被泄露的信息中包括名称、社会保障号、出生日期、地址，以及一些驾驶执照号码等。除此之外还有 20 多万名美国消费者的消费详情和 18.2 万人的争议性文件可能遭到泄露。同时 Equifax 在英国和加拿大的一些顾客信息也受到影响。

事件分析

在本次泄露事件中，黑客是利用了已经在 3 月份披露并公布修复方案的 Apache Struts（CVE–2017–5638）漏洞发起的攻击。

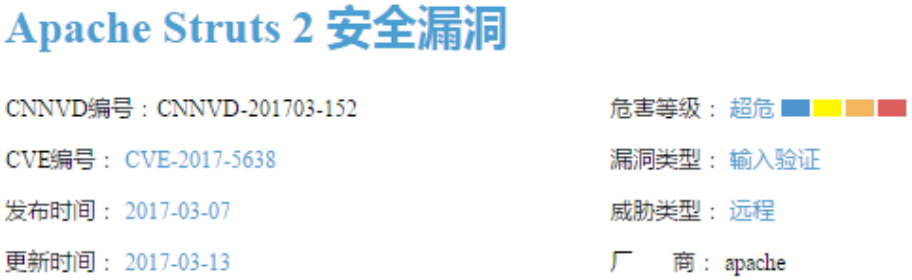


图 34　CNNVD 公布的 Apache Struts 漏洞信息

在漏洞披露的时候评分为最高分 10 分，Apache 随后发布 Struts 2.3.32 和 2.5.10.1 版本。但 Equifax 在漏洞出现的两个月内都没有修复，导致 5 月份黑客利用这个漏洞进行攻击，敏

感数据泄露。除了 Apache 的漏洞，黑客还使用了一些其他手段绕过 WAF 等网络端安全防御。

优酷上亿条用户账户信息在暗网 2000 元售卖

事件描述

2017 年 4 月 17 日，外媒 Hackread 爆料，一个名为 CosmicDark 的供应商在暗网售卖优酷的数据库，该出售的数据库包括了 100759591 条优酷用户账户信息。据 hackread 报道，该数据库在 2016 年泄露，今年暴露在互联网上，目前不清楚数据库是如何被盗走的，CosmicDark 将该数据库售卖价格定为 300 美元，折合人民币 2000 余元。这么算下来，5 万人的个人信息才值 1 块钱。

事件分析

优酷信息泄露事件，源于存储用户信息的数据库被整库盗窃。目前数据库应用和维护环境有了很大的变化，传统安全解决方案存在诸多安全隐患，数据库安全问题越来越引起国家安全部门的重视，拖库、撞库等传统的黑客攻击手段，需要使用专门的数据库访问控制手段，结合精细的策略配置，实现安全防护。

58 同城简历信息泄露事件

事件描述

2017 年 3 月，多家新闻网站曝出“58 同城陷数据泄露：700 元可采集网站全国简历信息”的新闻报道，指出目前淘宝等电商平台大量出售 58 同城简历数据，并出售爬虫软件，能够采集 58 同城全国简历数据，以及 58 本地商户信息、汽车过户联系人信息、保洁公司信息、租房联系人信息等多类信息。

自 2016 年初开始，关于 58 同城的爬虫软件和相关技术讨论不断涌现，如今已成规模。利用这些工具，一天可采集到的数据量达 10 万条。

据中国电子商务研究中心 (100EC.CN) 监测数据显示，58 同城月独立用户近 3 亿，此次全国范围内的简历数据泄露事件涉及了大量用户的个人信息，影响十分严重。

事件分析

由于 58 同城网站存在弱加密等设计缺陷，导致攻击者可通过访问该网站的某些数据查询接口，经过简单的解密还原，获取并关联用户关键信息，进而获取用户简历的全部信息。

简而言之，攻击者获取简历全部信息可通过以下三个步骤：

1、攻击者通过某移动端接口获取部分简历信息（求职方向、年龄、期望月薪、工作经验、居住地、学历、用户 ID、更新简历时间等内容）和简历 ID；

2、攻击者使用简历 ID 通过另一个接口获取用户的真实姓名；

3、攻击者使用用户 ID 通过另一个网站页面获取用户的电话号码。

通过用户 ID 和对应简历 ID 将三部分信息关联，攻击者就可以获得最完整的用户简历

信息。

“其实这几个漏洞任何一个都算不上是高危漏洞，甚至可以算是正常的接口功能。但是结合在一起就会造成严重的数据泄露事件。”

医疗卫生系统被入侵 7 亿公民信息泄露

事件描述

2017 年 9 月据《法制日报》报道，王某辉于 2016 年 2 月入侵某部委的医疗服务信息系统，将该系统数据库内的部分公民个人信息导出，并进行贩卖。库某于 2016 年 9 月侵入某省扶贫网站，窃取了该系统内数个高级管理员的账号和密码，并下载系统内大量公民个人信息数据进行贩卖。随后，库某将其中一个账号和密码转卖给陈某亮，其下载大量公民个人信息后，又将该数据以及帐号和密码贩卖给了台湾等地的诈骗团伙。

事件分析

本次事件中造成数据泄露的主要原因看似是不法分子对信息系统外部攻击引发的，但实际上这与一些单位的信息系统存在系统漏洞密不可分。所以我们在打击外部攻击行为的同时也要做好自身信息系统的安全防护工作。建议系统提供方、信息采集方要加强信息的安全存储，以及相关系统的安全防护、检测等工作，避免使用的系统存在漏洞，增加信息泄露的风险。

香港宽带公司数据库被黑：38 万名客户信息泄露

事件描述

香港宽带有限公司在 2018 年 4 月份公布，集团一个已停用的数据库服务器遭身份不明者入侵，该数据库涉及 2012 年至今约 38 万条固网电话及 IDD 服务客户申请人记录，包括其个人资料及约 4.3 万条信用卡数据，受影响数据占整体客户记录的 11%。

这些截至 2012 年的数据包括姓名、电邮地址、通讯地址、电话号码、身份证号码及约 4.3 万条信用卡资料。

事件分析

该泄露事件的主要原因有两个，一是：外部黑客的攻击行为；二是，公司对数据资产的安全性没有足够的重视，对于存储用户信息的数据库没有做到有效的安全防护，为非法窃取数据者提供便利。

网络安全法第一案——国内高校数据泄密被处罚

事件描述

2017 年 9 月 28 日下午，安徽省淮阳市网络与信息安全信息通报中心（市公安局网安支队）接到国家网络与信息安全信息通报中心通报：淮南职业技术学院系统存在高危漏洞，系统存储的 4000 余名学生身份信息已经造成泄露。

市公安局网安支队经过现场调查和勘验取证工作，并依法对网络中心系统管理员和操作维护人员进行询问。市公安局网安支队依法传唤学院分管网络信息安全工作的院长和网络中心主任及相关工作人员进行调查，确认该学校因未落实网络安全等级保护制度造成数据泄露，依法对淮南职业技术学院处以立即整改和行政警告的处罚措施。对泄露的学生身份信息流向，市公安局正在依法调查中。

事件分析

经核实，淮南职业技术学院招生信息管理系统存在越权漏洞，后台登录密码弱口令，学院未落实网络安全管理制度，未建立网络安全防护技术措施，网络日志留存少于六个月，未采取数据分类、重要数据备份和加密措施，致使系统存储的 4353 名学生的身份信息泄露。这样的安全隐患普遍存在于教育行业的信息系统中，被黑客利用攻击只是时间问题。对于此类安全隐患，应当从日常的漏洞检查做起，及时进行数据安全加固。另一方面，作为高校网安法第一案，此案件的判罚具有指导意义，同时也警示各行业及部门应尽快落实法律要求的安全防护建设。

数据泄露成本分析

目前越来越多的企业和组织开始量化数据资产，关注数据泄露的成本化，并对数据丢失或被篡改可能导致的后果进行量化分析，这在评估数据保护方面的预算投入时，会成为关键的评估依据和数据支撑。

数据泄露或被篡改等安全事件对企业和组织带来的损失将是多方面的，这其中包括可量化的经济损失，如监管罚款，盈利受损，企业审计失败造成的资产负债，以及不可量化的品牌和业务影响，如组织公信力受损、客户投诉带来的经营状况下降，更重要的是，全球多国正在践行数据保护法规化，这让数据泄露案件按量入刑有法可依。以下为国内外具有代表性的数据保护相关法律对数据泄露案件的量刑，以及权威咨询机构的数据泄露成本分析报告等材料。

国内相关法律的判罚标准

网络安全法

【第六十四条】规定网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

两高对侵犯公民个人信息刑事案件的解释

2015 年 11 月 1 日起施行的《刑法修正案（九）》对个人信息犯罪的法律条款作出修改完善以来，案件数量显著增长。2015 年 11 月至 2016 年 12 月，全国法院新收侵犯公民个人信息刑事案件 495 件，审结 464 件，生效判决人数 697 人。

2017 年 5 月，最高人民法院、最高人民检察院联合发布《关于侵犯公民个人信息刑事案件适用法律若干问题的解释》，对侵犯公民个人信息犯罪的定罪量刑标准和有关法律适用问题作了全面、系统的规定，共十三条。明确非法获取、出售或者提供公民个人信息，违法所得 5000 元以上即可入罪，造成被害人死亡、重伤、精神失常或者被绑架等严重后果的，依照刑法规定，处 3 年以上 7 年以下有期徒刑，并处罚金。对于行踪轨迹信息、通信内容、征信信息、财产信息，非法获取、出售或者提供 50 条以上即算“情节严重”；对于住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息，标准则是 500 条以上；对于其他公民个人信息，标准为 5000 条以上。

该司法解释已于 2017 年 6 月 1 日起正式施行。

全球性的数据保护法规化

2016 年 4 月 27 日，欧洲议会通过了《一般数据保护条例》（简称“GDPR”）法律条例并将在 2018 年 5 月 25 日生效。非欧盟成员国的公司（包括免费服务）只要满足下列两个条件之一：

（1）为了向欧盟境内可识别的自然人提供商品和服务而收集、处理他们的信息。

（2）为了监控欧盟境内可识别的自然人的活动而收集、处理他们的信息。

该公司就受到 GDPR 的管辖，即无论公司总部在哪，无论数据存储和使用地点在哪，只要与身处欧盟的企业有生意往来，或者监视欧盟公民的行为，就必须遵从 GDPR。这个条例将对中国企业与欧盟国家的信息服务中所涉及的数据收集、使用、处理和分析等产生重大影响。

2018 年 5 月 25 日 GDPR 实施，就会出现两级制裁制度。如果没有通过，企业面临的罚款标准为：一般违规行政罚款的上限是 1000 万欧元或该企业上一财年全球年度营业总额的 2%（以较高者为准）；严重违规行政罚款的上限是 2000 万欧元或该企业上一财年全球年度营业总额的 4%（以较高者为准）。

GDPR 的制约和惩罚力度给中国企业敲响了警钟，将迫使涉及对外业务的中国企业在提供产品和服务时，首先需要确保客户的数据安全保护措施是否经得起挑战。

权威机构对数据泄露成本的研究结果

《2017 年全球数据泄露成本研究》报告中，IBM Security 和 Ponemon Institute 两家研究机构针对 419 家公司进行调研，合计数据泄露总成本达到 362 万美元。每条包含敏感和机密信息的丢失或被盗记录的平均成本达到 141 美元。对比往年，2017 年企业和组织数据泄露的规模较以往更大，平均规模增长了 1.8%。

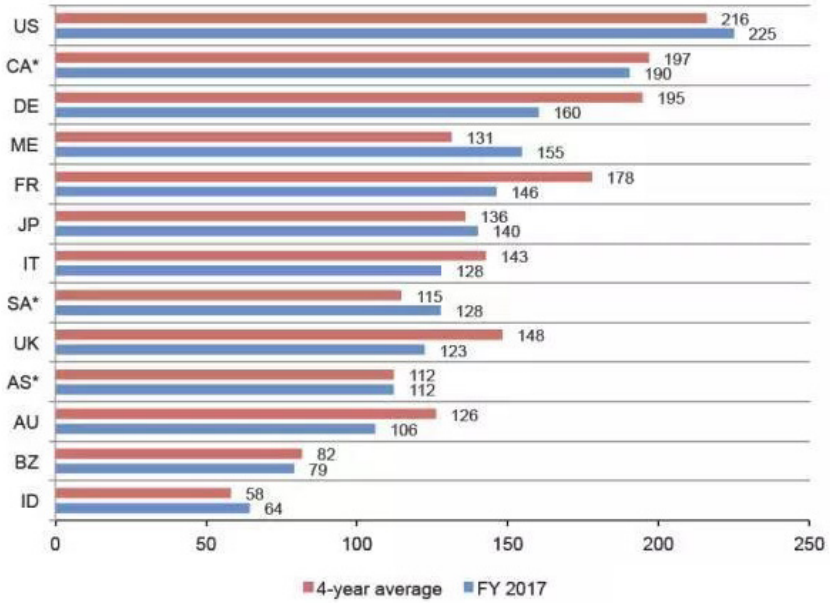


图 35　全球各国数据泄露成本总览

外泄规模的大小以及丢失或被盗记录的数量

调研结果显示，数据泄露事件将导致客户信任度下降、企业也需要投入大量成本进行取证调查，挽回数据，以及相关客户的联系及法律成本。通过成本分析揭示了数据泄露的平均总成本与事件的大小之间的关系：少于 10,000 个损失记录事件的平均总成本 190 万美元，超过 50,000 记录的事件平均总成本是 630 万美元。因此，丢失的记录越多，数据泄露的成本就越高。对于这一情况，报告中提到数据分类存储计划对于了解敏感和机密信息至关重要。

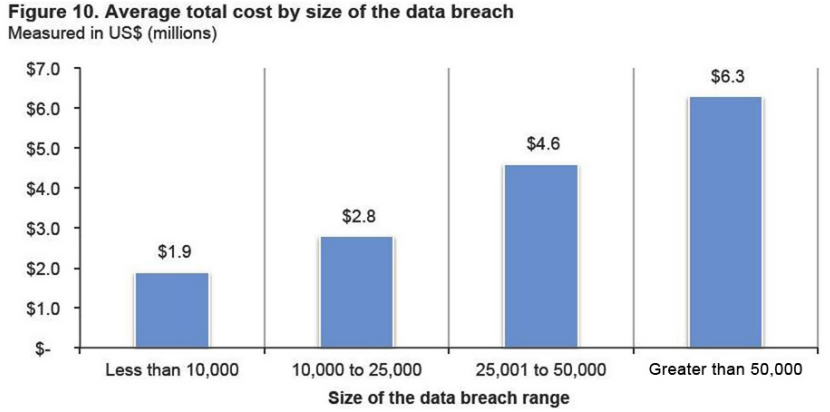


图 36　数据泄露的平均总成本与 419 个组织的事件大小之间的关系

哪些行业的数据泄露更为昂贵

每个丢失或被盗记录的数据泄露的全球平均成本为 141 美元。然而，医疗保健机构的平均成本为 380 美元，金融服务平均成本为 245 美元。行业的数据特性，全球共通，医疗及金融行业的数据更多涉及公众个人隐私及资产信息，数据量庞大；另一方面，从业务角度来看，这两个行业与其他行业的数据集中、共享需求更为明显，从中国国情来看，这两个行业除了互相业务交叉，还会与政府、社保、工商、税务财政等诸多行业发生数据共享，在数据使用和流转的过程中，节点更多，一旦单点发生安全事件，可能牵连出跨行业的极大规模数据泄露，由此产生的恶劣社会影响难以估计。

附件 E　数据安全成熟度模型

数据安全能力成熟度模型的模型架构由以下三方面构成（如下图所示）：

1、数据生命周期安全：围绕数据生命周期，提炼出大数据环境下，以数据为中心，针对数据生命周期各阶段建立的相关数据安全过程域体系。

2、安全能力维度：明确组织机构在各数据安全领域所需要具备的能力维度：制度流程、人员能力、组织建设和技术工具四个关键能力的维度。

3、能力成熟度等级：基于统一的分级标准，细化组织机构在各数据安全过程域的 5 个级别的能力成熟度分级要求。

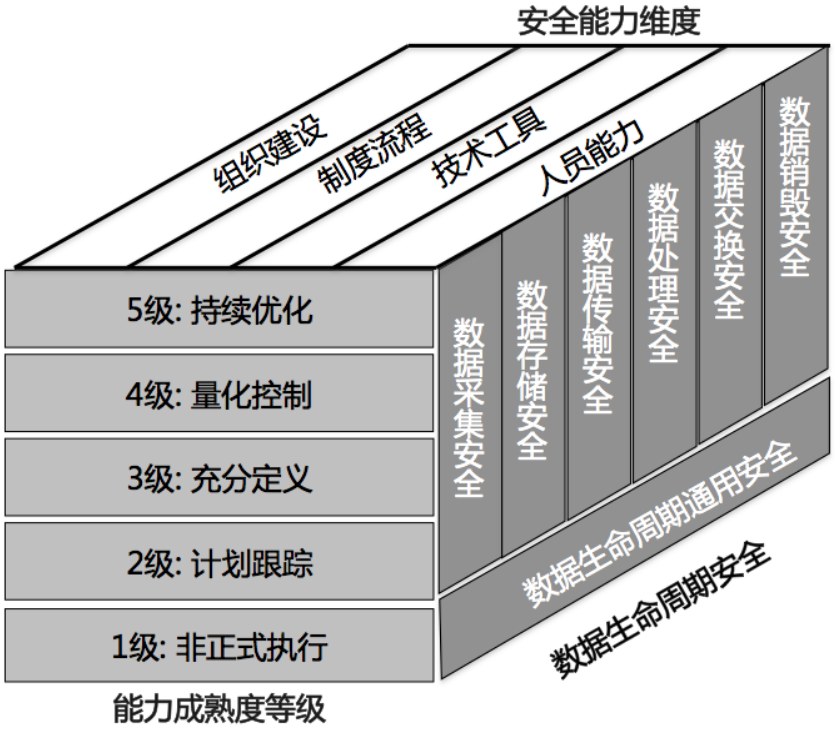


图 37　数据安全能力成熟度模型架构

通过对模型的应用可以帮助组织机构了解其整体的数据安全风险，有针对性制定解决方案；建立组织内部整体的数据安全管理体系；明确自身的数据安全管理水平并确定后期建设的方向。

1、数据生命周期安全维度

数据生命周期基于大数据环境下数据在组织业务中的流转情况，定义了数据的六个生命周期阶段，如图 28 所示，各阶段的定义如下：

数据产生：指新的数据产生或现有数据内容发生显著改变或更新的阶段；

数据存储：指非动态数据以任何数字格式进行物理存储的阶段；

数据使用：指组织在内部针对动态数据进行的一系列活动的组合；

数据传输：指数据在组织内部从一个实体通过网络流动到另一个实体的过程；

数据共享：指数据经由组织与外部组织及个人产生交互的阶段；

数据销毁：指利用物理或者技术手段使数据永久或临时性的不可用的过程。

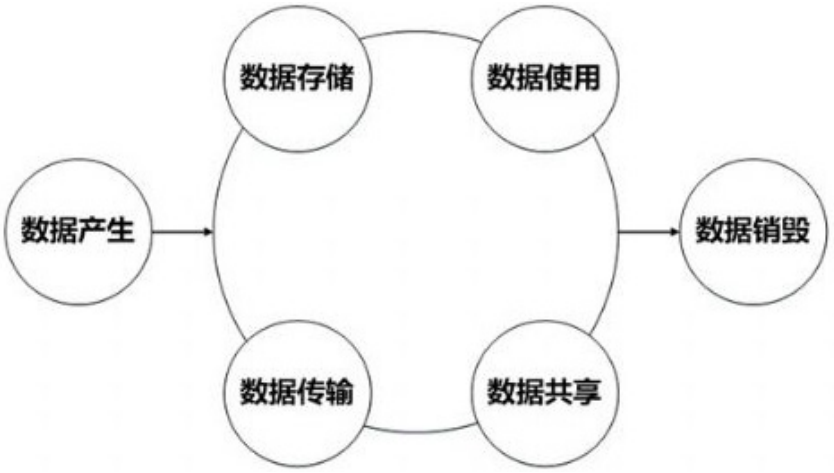


图 38　组织数据生命周期的六个阶段

安全过程域体系覆盖数据生命周期的六个阶段，包含数据生命周期通用安全的过程域和数据生命周期各阶段安全的过程域，如图 39 所示。

图 39　数据安全过程域体系

2、安全能力维度

组织建设

从承担数据安全工作的组织机构建设应具备的能力出发，从以下方面进行能力的级别区分：

1）数据安全组织架构对组织业务的适用性；

2）数据安全组织机构承担的工作职责的明确性；

3）数据安全组织机构运作、沟通协调的有效性。

制度流程

从组织机构在数据安全层面的制度流程建设，以及制度流程的执行情况出发，从以下方面进行能力的级别区分：

1）数据生命周期关键控制节点授权审批流程的明确性；

2）相关流程制度的制定、发布、修订的规范性；

3）安全要求及流程落地执行的一致性和有效性。

技术工具

从组织机构用于开展数据安全工作的安全技术、应用系统和自动化工具出发，从以下方面进行能力的级别区分：

1）数据安全技术在数据全生命周期过程中的利用情况，针对数据全生命周期安全风险的检测及响应能力；

2）利用技术工具对数据安全工作的自动化和持续支持能力，对数据安全制度流程的固化执行能力。

人员能力

从组织机构承担数据安全工作的人员应具备的能力出发，从以下方面进行能力的级别区分：

1）数据安全人员所具备的数据安全技能是否能够满足复合型能力要求（对数据相关业务的理解力以及专业安全能力）；

2）数据安全人员的数据安全意识以及关键数据安全岗位员工的数据安全能力的培养。

3、成熟度等级维度

组织机构的数据安全能力成熟度模型分为五个成熟度等级，一级是非正式执行级，二级是计划跟踪级，三级是充分定义级，四级是量化控制级，五级是持续改进级。能力级别从一级至五级逐级提高，标志着组织机构的数据安全保障能力的成熟度不断提升。每个级别规定了对应的公共特征和通用实践。对成熟度等级的描述如表 1 所示：

成熟度等级	详述	特征
等级 1: 非正式执行	· 执行基本实践：组织机构在数据安全过程域未有效的执行相关工作，仅在部分业务场景中 / 项目执行过程中根据临时的需求执行了相关工作，却未形成成熟的机制保证相关工作的持续有效进行，执行相关工作的人员能力也未得到有效的保障。所执行的过程可称为“非正式过程”。	随机、无序、被动的执行安全过程，依赖于个人，经验无法复制。
等级 2: 计划跟踪	· 规划执行：对安全过程进行规划，提前分配资源和责任。 · 规范化执行：对安全过程进行控制，使用过程执行计划、执行基于标准和程序的过程，对数据安全过程实施配置管理。 · 验证执行：确认过程按照预定的方式执行，验证执行过程与可应用的计划是一致的，对数据安全过程进行审计。 · 跟踪执行：控制数据安全项目的进展，通过可测量的计划跟踪过程执行，当过程实践与计划产生重大偏离时采取修正行动。	在项目级别主动实现了安全过程的计划与执行，没有形成体系化。

成熟度等级	详述	特征
等级 3: 充分定义	· 定义标准过程：组织机构对标准过程进行制度化，为组织机构定义标准化的过程文档，为满足特定用途对标准过程进行裁剪。 · 执行已定义的过程：充分定义的过程可重复执行，使用已定义的过程，针对有缺陷的过程结果和安全实践的核查，使用过程执行的结果数据。 · 协调安全实践：对业务系统和组织活动的协调，确定业务系统内、各业务系统之间、组织机构外部活动的协调机制。	在组织级别实现了安全过程的规范定义与执行。
等级 4: 量化控制	· 建立可测的安全目标：为组织机构的数据安全建立可测量目标。 · 客观地管理执行：确定过程能力的量化测量并使用量化测量来管理安全过程，以量化测量作为修正行动的基础。	建立了量化目标，安全过程可进行度量与预测。
等级 5: 持续优化	· 改进组织能力：在整个组织机构范围内标准过程的使用进行比较，寻找改进标准过程的机会，分析对标准过程的可能变更。 · 改进过程有效性：制定处于连续受控改进状态下的标准过程，提出消除标准过程产生缺陷的原因和持续改进的标准过程。	根据组织的整体目标，不断改进和优化安全过程。

表 9　成熟度等级描述

附件 F　数据安全治理重要相关技术

F.1 DCAP 技术

DCAP（Data Centric Audit and Protection）是以数据为中心的审计与安全防护技术的统称，这些技术能够集中监控和管理用户与特定数据集相关的行为。一些安全企业正在开发机器学习或行为分析能力，通过行为监控和智能分析提供更高层次的洞察力。这种技术基于数据安全治理（DSG）的原则，将数据安全策略中的控制要求在非结构化，半结构化和结构化数据库或数据孤岛进行实现。

F.1.1 核心功能

- **数据分类和发现** 大多产品都附带符合相关政策的内置字典或搜索算法，如 PCI，HIPAA 或 GDPR。但是，不同产品的搜索能力有所不同，例如速度和准确性。在特定 DBMS，文件类型，Hadoop 或云平台搜索的能力将因厂商而异。如果打算将产品与 DBMS 一起使用，需要搜索到列 / 表元数据或字段。此外，需要检查是否可以在数据库中的二进制大对象（BLOB）或字符大对象（CLOB）中搜索数据。一些产品只能在非结构化文件中进行搜索，并通过将元数据附加到每个文件进行标记。
- **数据安全策略管理** 需要提供统一管理控制台的能力，可以控制所有数据存储仓库的安全策略。大多数产品会分拆这些功能，用户需要分别购买不同的产品，但同时也需要通过单一的软件或管理控制台进行统一管理。将角色和责任在数据安全治理过程中统一起来的功能非常重要。策略的应用通常基于通过第三方产品（如（AD）或 LDAP）进行身份验证（用户身份和业务角色）。策略管理人员定义对特定数据的访问策略，甚至需要授予多个用户组访问多个数据单元的多对多的能力。如果应用程序通过使用连接池来提供更高效的数据访问帐户，那么在应用程序的级别识别业务用户的就是很重要的能力要求。有时可以通过与 Kerberos 等身份验证协议与应用程序进行通信，但并不是所有应用程序都提供此功能。其他产品可能会使用应用层的代理程序来收集用户身份，从应用程序工具中关联日志，或者使用代理技术拦截和分析来自应用程序或 Web 服务器的网络通讯。以应用层为中心的工具将不具有数据层用户访问权限的视图。应该注意，还有其他控制措施来解决这个问题，例如额外的代理监控代理软件或数据层的加密软件。
- **监控用户权限和数据访问行为** 制订安全策略来管理和监视所有可访问特定数据集的

应用用户和管理权限。监控 AD 成员资格的变化或个别权限的更改是非常重要的，以确保它们符合业务角色、数据类型或数据存储位置相关的要求。检测数据修改、权限提升和更改安全警报的功能，对于检测潜在的恶意内部人员或外部黑客活动以及满足合规性，但是并不是所有的产品都在存储层运行，并且它们可能无法评估数据库管理员，系统管理员或开发人员等特权用户的能力。因此，产品能够拦截各种管理员在数据和应用层的访问也很重要。产品需要在服务器峰值加载或网络通信拥挤时持续运行。如果在基础架构高度负载的情况下需要进行密集监控，则必须考虑网络架构和产品的能力要求。否则，可能导致延迟或在极端情况下不能监视某些行为。

- **审计和报表** 随着数据分析要求的不断增长，对报表功能的需求也将增长。在各种监管环境中的审计员需要有能力在历史日志的基础上对用户的行为进行洞察，这可能需要至少一个月的可访问数据。合规性还将需要各种监控功能的审计跟踪，例如异常用户行为，数据更改，违反政策或更改权限。在发生违规或安全事件的情况下，重要的是能够进行审计日志分析来追溯所有行为，包括数据访问、修改或权限更改。
- **行为分析，警报和阻断** 基于预先选择的监控条件创建安全警报的能力至关重要，这可能导致不同级别的警报范围从政策违规到访问数据的可疑行为。警报机制，包括控制台显示器的告警、对关键安全人员、数据所有者或业务人员的自动消息传递。也可以启用其他功能，例如自动阻断访问或删除行为。极端的反应可能包括在大规模数据下载情况下关闭访问。未来的产品甚至能够通过一些关联分析来检测异常行为。分析历史访问趋势的能力将提供越来越重要的洞察力以检测不适当的行为。产品的不同之处在于管理控制台界面的易用性，可以管理和报告安全警报，以及不同数据存储平台内的报告的粒度。例如：关于数据库审计行为，需要在可以检测的命令数量与软件 / 硬件处理能力以及结果集进行分析的能力之间进行权衡。如果服务器或网络通信已经严重加载，并且本地监视代理程序处理大量日志的能力受到限制，则可能会发生这种情况。可以根据数据内容和组成员资格或权限阻止数据访问。当控制台通过具有下发的策略管理或不同监视功能的代理或软件来监督多个数据对象时，可能会有不同的检测结果。
- **数据保护** 一些供应商通过加密，令牌化或数据脱敏提供独立的数据保护工具，而其他厂商不提供这些工具，这样用户需要独立购买相关产品。在这两种情况下，这些防护产品可能不会集成到单个管理控制台中，并且需要与数据安全策略的仔细协调。选择这些工具需要仔细评估每种可能提供的威胁和风险。例如，实现透明的数据库加密可以防止系统管理员的访问，但数据库管理员仍然可以访问。通过数据库服务器上的代理应用数据动态脱敏，并通过 AD 链接，可以用于防止数据库管理员访问。然而，存储时数据不受保护；它仍然可以由系统管理员访问。加密或令牌化字段可以保护正在活动或存储的数据元素，但必须注意这不会影响应用程序的操作。

F.1.2 相关技术

当前的 Gartner 对 DCAP 的研究覆盖四个细分市场：数据库审计和保护（DAP）；数据访问管理（DAG）；云访问安全代理（CASB）；和数据保护（DP），其中包括加密，令牌化和数据脱敏（DM）。不同的进化轨迹，意味着不同的产品在其产品路线图中具有不同的目标和基本功能。虽然没有一款产品完全符合 DCAP 的要求，但这些产品在每种类别中都在完成跨数据处理对象的兼容能力：

● **DAP** 这些产品已经开发了多年，用于实施数据安全策略，数据分类和发现，特权访问管理，数据活动监控或行为分析，审计和数据保护。以前，专注于 RDBMS 和数据仓库，某些产品开始兼容 Hadoop 和非结构化文件共享以及 DBaaS。

● **DAG** 这是 有时被称为以文件为中心的审计和保护（FCAP）。通常，这些产品专注于实施文件数据的安全访问策略，数据分类和发现，以及文件存储库和目录服务（如 SharePoint）的活动监视和审计。这些产品与身份和访问管理（IAM）密切相关。一些产品也开始包含云 SaaS 应用的功能。

● **CASB** 在 SaaS 应用程序或云存储环境（如 Microsoft Office 365，Salesforce，ServiceNow，Box 和 Dropbox）中保护数据的能力正在通过多种产品快速增长。这些产品具备跨越 DCAP，数据丢失防护（DLP）和用户实体行为分析（UEBA）等能力的数据安全控制。CASB 正在不断发展数据分类和发现，访问控制，活动监控，审计和阻断，改写，加密，标记化和隔离等方面的不同组合。这些产品通常是独立的，一些 CASB 可以从企业 DLP 产品导入策略，但它们的管理并不与内部部署 DLP 集成。

● **DP** 这些产品传统上侧重于通过多个数据仓库（RDBMS，数据仓库，非结构化大数据和一些基于云的企业文件同步和共享 [EFSS] 工具）的加密，标记化或遮蔽来保护数据。但是，通过添加实时警报，活动监控和审计功能，几项产品已经创新发展。DAP 和 DAG 产品可以提供对文件或数据库中所有数据的访问的监视和审计，但这些 DP 产品通常只关注敏感数据类型。

产品可以使用各种技术通过应用层和 / 或数据层进行连接。通过需要应用层代理，接口或与特权管理工具的集成，穿透隐藏了身份标识的连接池，从而对来自应用层的个人访问进行控制。

F.2 脱敏技术

数据脱敏（DM）是一种技术，旨在通过向用户提供高度仿真的数据，而不是真实和敏感的数据，同时保持其执行业务流程的能力，从而防止滥用敏感数据。

DM 与加密或标记化不一样，数据脱敏通常是数据进行了单向转换的不可逆过程。令牌化和格式保存加密（FPE）是被设计成基于授权控制的可逆替代算法，但如果密钥没有被正

确管理，则这种可逆性会增加重新识别和隐私侵犯的风险。

F.2.1 核心功能：

- 数据和关系发现
- 数据脱敏规则定义
- 数据脱敏操作和管理
- 报告合规性

F.2.1.1 数据和关系发现

相同的敏感数据类型可能存在于同一数据库的多个表以及整个企业中的其他数据库中。如果需要脱敏，则应将其应用于所有所需表和数据库中的所有数据实例。正确保持这些关系对于存储脱敏数据的数据库和使用脱敏数据的应用程序是至关重要的。

手动的脱敏过程耗时且容易出错。自动化的脱敏数据和数据关系发现过程至关重要，作为此过程的一部分，对脱敏元数据的自动采集大大改善了脱敏规则定义过程。

自动数据和关系发现通常使用不同方法的组合实现：

- 通过数据库中的元数据提供的主外键关系进行分析相关的表和列是一种基本手段。然而，一些应用程序将这些关系保存在应用程序逻辑中，通过这种方法将无法发现这些关系。
- 分析事务日志，应用程序代码和应用程序执行的实时监控可以提供对应用程序级别定义的关系的洞察。
- 分析存储库中的实际数据还可以识别以前不知道包含敏感数据的列，一些供应商可以通过在多个表中查找和关联相同的数据值来找到隐藏的关系。那些发现的关系通常会经过手动审查和完成，以弥补差距。

随着模式更改，新数据源或应用程序的更改或脱敏的数据量的变化，保持对最新环境的同步和兼容很重要，这可能会影响脱敏解决方案的性能和有效性。数据和关系发现也可以用于捕获这些变化并支持脱敏操作的生命周期。

F.2.1.2 数据脱敏规则定义

应在一个“中央仪表盘”中定义数据脱敏规则，以便跨多个交叉引用的数据库实现这些规则的全面应用。这确保了脱敏的一致性，以及节省时间和资源。与对每个数据库分别定义和应用脱敏规则相比，这种方法也是更为有效的，以此确保在相互引用的数据库中的被脱敏的数据的一致性。

通过模板来实现对特定数据脱敏策略的统一的制定，将极大地帮助用户对数据采用了正

确而一致的脱敏方法。提供用户设置脱敏策略的规则向导已经变得很常见。不幸的是，即使有规则向导可用，用户通常也不能确定应该脱敏什么数据，或应该采用什么规则来确保安全性和遵守法规。客户应该寻找提供模板和预定义规则的供应商，这些规则通常映射到自己的应用领域和合规性问题，以加速他们的项目，并从这些模板的现有部分中获益。产品自带的规则通常需要定制，并能提高满足合规要求的机会。根据设定的规则，预测脱敏效果或评估脱敏数据再识别风险的能力也是非常需要的。

F.2.1.3 数据脱敏操作与管理

数据脱敏产品应提供工具来管理脱敏数据的完整生命周期：

- 部署脱敏规则
- 计划或触发脱敏作业
- 监控 SDM（静态脱敏）或 DDM（动态脱敏）操作的性能

在解决方案架构（服务器，设备，插件，代理等）的不同组件中部署脱敏规则的功能可以显著减少管理工作量，并保持实时的变化同步从而提高解决方案的可靠性。所有这些组件的工作状态也应该是可见的，并且在发生故障时产生警报，以防止安全漏洞或其他业务操作的负面影响。

脱敏工作调度和管理是可调用，提供对外开放的 API 或服务也是很重要的。

监控解决方案的性能，对于检测可能影响脱敏作业耗时的数据规模或访问方法，以及脱敏耗时的趋势也很重要，或者监控 DDM（动态脱敏）中高于用户预期的长时间滞后响应的行为。

合规报告

数据脱敏工具应能够对敏感数据，数据依赖关系和应用脱敏技术等信息形成报告。此外，他们应该能够跨多个数据源跟踪和报告脱敏的数据。

报告可以检测到无意中发生的错误，发现未被脱敏的易受攻击的数据以及在各种数据库中发现交叉引用的数据。它还将反映对于特定数据不够安全的脱敏技术。报告增加了企业的审计准备，并且证明了所有适用的政策是由内部或外部要求（如 PCI DSS，HIPAA 或 GDPR）所驱动的。报告可视化脱敏结果，使开发人员 / 测试人员和审核员更加透明。

F.2.2 主要技术

- 静态数据脱敏
- 动态数据脱敏
- 非结构化和半结构化数据改写（USR）

F2.2.1 静态数据脱敏（SDM）

SDM 用于对开发或测试中的数据集而不是生产中的数据集。数据在使用之前被脱敏，因此数据在存储和随后的使用或传播过程中受到保护。它最经常实现为手动启动，按计划或由应用程序驱动的批处理。脱敏行为也可以是数据复制或复制虚拟化层的一部分，从而导致目标环境中的静态数据集被脱敏。

SDM 还可用于创建与真实数据一起使用的脱敏数据副本，以动态管理对不同用户组的数据库视图的访问。结果类似于 DDM，但是当需要访问脱敏后的大数据集时，比起 DDM 性能影响大大降低 le（以增加的存储空间为代价），因为数据已经被脱敏过了。这种方法主要适用于分析和大数据环境，因为不是所有的应用程序都可以支持创建额外的视图和结构来存储被脱敏的数据。

SDM 是一个相对成熟的市场，与测试数据管理和数据管理市场密切相关。SDM 主要用于在以下情况下保护数据：

- 应用程序开发和测试 – 在用户需要代表性数据但不需要查看真实数据的开发和测试环境中保护数据并减少合规范围
- 数据发布和共享 – 生成身份识别数据，供各方交换或出版
- 商业智能（BI）和分析 – 保护业务分析应用或用户所需的数据库，仓库和大数据环境中的数据，其中一些或所有用户需要被阻止查看真实数据

F2.2.2 动态数据脱敏（DDM）

DDM 在应用程序或个人根据授权访问数据时，实时进行脱敏操作。原始敏感数据驻留在存储库中，并且在应用程序访问时按策略授权进行数据提供。没有权限访问敏感信息的用户和应用程序提供了脱敏数据。DDM 不会更改底层存储库中的数据。

DDM 操作可以在不同的应用层进行。大多数商业解决方案在本地（例如，关系数据库管理系统 [RDBMS] 内核的一部分）或者通过代理（作为数据库和应用程序之间的代理），或者在应用程序服务器级别脱敏数据，作为一个插件，或通过在不同层级的 API。其他实现形式也存在，例如，在展现层或消息传递层。数据的访问权限所依赖的访问者身份和上下文信息，对于不同的目标应用程序体系结构而有所不同。一些解决方案将应用程序主机或终端设备也作为上下文，但脱敏动作依然是通过代理或类似代理的服务执行脱敏。

这些解决方案的每种都需要对客户环境进行不同程度和类型的更改，以实现与现有数据安全层（例如加密）的兼容性。而且，即使不需要代码更改的解决方案，也将对受保护系统的应用程序生命周期管理产生影响。

DDM 主要用于在以下情况下保护数据：

- 业务应用程序 – 对于业务应用程序访问生的产数据库和仓库中的数据，对于某些用

户需要防止其查看真实数据。

● BI 和分析 – 对于在业务分析环境下，存储在数据库、数据仓库中的大量数据，需要防止某些用户看到真正的数据。

DDM 还可用于应用程序开发和测试环境，其中某些授权户需要查看真实数据或环境特性（例如，刷新频率要求）会阻止 SDM 的有效使用。

F.2.2.3 非结构化和半结构化数据改写

组织可以使用数据改写技术保护敏感的非结构化（PDF，Excel 文件，文本文件，日志文件等）和半结构化（XML，JSON 等）内容。数据脱敏供应商对数据改写的需求不如关系数据平台和数据平台的 SDM 和 DDM 需求强劲，但许多厂商都有能力：

●存储在 RDBMS，大型数据平台或文件系统中的结构化和半结构化数据

●通过日志文件或服务中的应用程序来处理敏感数据的扩散

支持的文件格式通常限于 PDF，Microsoft Office 文件和纯文本格式，例如 CSV，XML，JSON 和各种日志文件。脱敏供应商支持的非结构化数据改写用例通常具有明确的系统和数据所有权结构。具有复杂数据所有权和使用模式的共享存储库中的非结构化数据的数据改写可能难以用 DM 产品实现。

F.3 DLP 技术

DLP 是一款内容识别安全技术，可解决敏感企业信息的三大关键问题：

1、敏感企业信息存储在何处？

2、敏感企业信息使用情况如何？

3、如何保护敏感企业信息，以防丢失和被窃？

无论处于下列哪种状况，DLP 均可让组织保护客户数据、公司信息、知识财产及敏感信息：网络 DLP 产品通过电子邮件、Web 邮件或其他 Internet 协议保护网络传输中的数据；终端 DLP 产品通过 USB/CD/DVD 保护数据离开终端或存储在终端时的安全；存储设备 DLP 产品保护存储在共享服务器及数据库中的数据。

DLP 软件由智能安全平台管理应用及八项组件组成：

● Network Monitor（网络监控 DLP）

● Network Prevent for E–mail（邮件防护 DLP）

● Network Prevent for WEB（网络防护 DLP）

● Endpoint Prevent（终端防护 DLP）

● File Storage Insight（文件存储洞察 DLP）

● Database Insight（数据库洞察 DLP）

- Business Interface System（商用接口服务器）
- Workflow Management System（工作流管理系统）

虽然这八项组件都可以单独部署或组合部署，但它们始终需要与 (Security Intelligence Platform) 智能安全平台管理应用程序一起实现。Security Intelligence Platform 是所有产品模块的中央管理应用程序，用于自动运行数据安全策略。在平台中，可创建用于自动检测和保护敏感数据数据防泄漏策略、控制策略、工作流程及审计信息，生成报告并配置以访问角色为基础的访问权限和系统管理。

F.3.1 关键技术

Network Monitor

Network Monitor 常驻于网络出口点，可监控网络数据。所涵盖的协议包括电子邮件 (SMTP)、Web (HTTP)、即时消息 (IM)、文件传输 (FTP)，以及通过任何端口进行的所有其他 TCP 会话。

Network Prevent for E-mail

Network Prevent for E-mail 常驻于企业邮件服务器后，可监控和禁止 / 修改企业邮件中的敏感信息。包含邮件的发件人、标题、内容和附件。

Network Prevent for WEB

Network Prevent for WEB 部署于网络出口点，可监控和组织网络数据的修改行为。所涵盖的协议包括电子邮件 (SMTP)、Web 和安全 Web (HTTP/HTTPs) 以及文件传输 (FTP)。

Endpoint Prevent

Endpoint Prevent 部署于员工的笔记本电脑及台式机计算机，可监控下载到内部硬盘的数据，并监控和禁止复制到 USB 设备、智能移动设备及 CD/DVD 的数据。

Endpoint DLP 可在终端进行网络层面的安全控制，比如禁止敏感信息邮件外发，禁止 QQ 发送敏感信息内容等。 对于文档，Endpoint DLP 可以进行权限授权、加密控制、标定密级等安全控制，保证数据更高的安全等级。Endpoint DLP 可以对终端计算机进行端口、磁盘和外设设备（如 U 盘）的安全管控，如全磁盘加密、可信介质管理等功能。

对于敏感文件的发现，Endpoint DLP 可以提供终端数据快速扫描的功能，可供管理员对于每个员工存储的敏感信息数据数量和位置进行查询，以便采取相关步骤。

File Storage Insight

File Storage Insight 可对文件共享服务器上的文件进行扫描，且不需要在服务器上安装 agent 程序，对于扫描出的机密数据文档进行事件通知和告警，以便采取相关步骤。

Database Insight

Database Insight 可对数据库表或字段进行扫描，且不需要在服务器上安装 agent 程序，

对于扫描出的非法数据表存储敏感数据的情况进行事件通知和告警管理员，以便采取相关步骤。

Business Interface System

Business Interface System 商用接口服务器通过 Web Service 方式向第三方系统提供一系列的服务能力，比如加密、解密、授权、外发文件制作、数据敏感信息检测、审批工作流托管等功能，以便和用户侧的 OA、ERP、PDM、SAP 等系统进行对接，更深入的和客户业务系统结合，提供一体化的服务。

Workflow Management System

Workflow Management System 工作流管理系统，当客户需要将敏感文档进行脱敏、解密、外发、权限变更时，工作流管理系统提供了流程审批的功能，其中提供会签、多级审批等场景设置，并且可分别设置不同部门的审批管理员，所有提交的审批和相关文件都将被存储备份保存可被审计，同时提供多种查询方式。

F.3.2 产品组成

下图是 DLP 产品的部署位置，以及不同的 DLP 产品在企业 IT 架构中的部署位置。“网络 DLP”产品部署于 DMZ 中，而其他产品则部署于企业 LAN 端 或数据中心。除了“终端 DLP”产品以外，所有其他产品都是以服务器为基础。

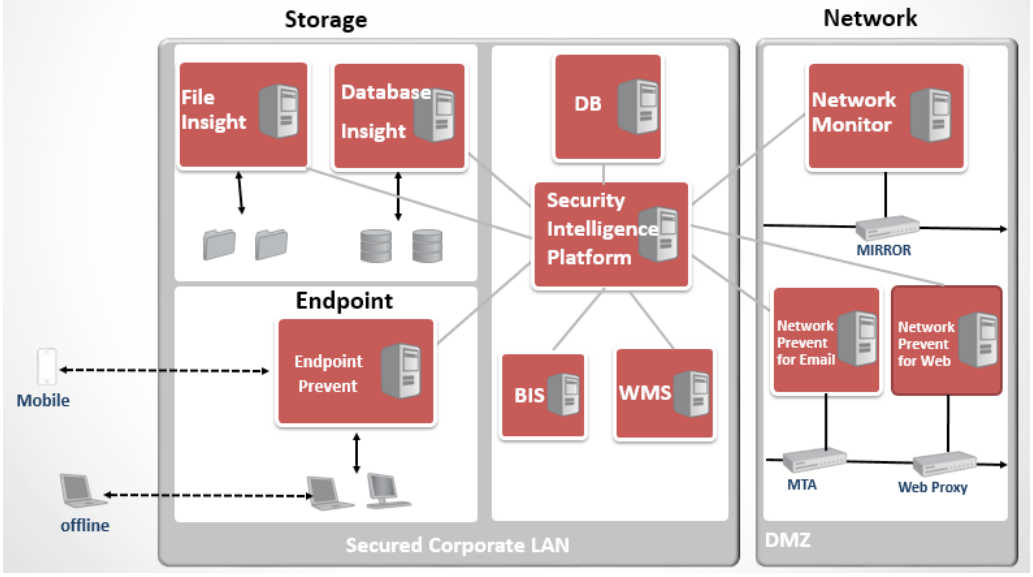


图 40　DLP 在 IT 架构中的部署位置

F.4 CASB 技术

CASB 作为部署在客户和云服务商之间的安全控制点。通过嵌入身份认证、设备识别、

单点登录、异常监控、加密等企业安全策略，来监控和防护企业用户对云上资源的连接访问。CASB 技术有两种工作模式，一种是 Proxy 模式另一种是 API 模式，Proxy 模式下，CASB 要处理企业上传到云应用的全部流量，重要数据采用加密等安全策略处理后再上传到云服务商。API 模式中，企业数据直接传给云服务商，CASB 通过利用云应用的 API，对用户进行访问控制以及执行企业的安全策略。

CASB 即 Cloud Access Security Broker 在 2012 年由 Gartner 提出，并连续多年被 Gartner 列为年度十大信息安全技术。CASB 是部署在云服务商与企业客户之间，在企业访问和使用云计算资源的过程中加入必要的安全策略，包括身份认证、单点登录、权限控制、加密、令牌化、恶意软件检测 / 预防、日志审计等多种类型的安全策略。CASB 作为一项新兴技术发展迅速，成为企业对其用户使用的众多云应用及服务的控制点。

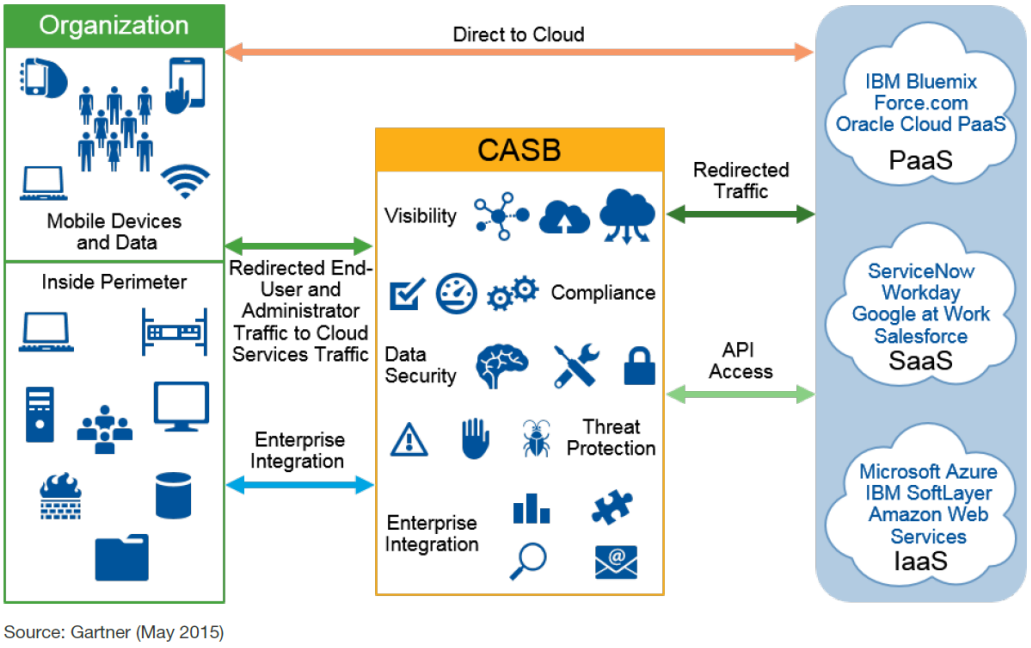


图 41　CASB 工作逻辑图

从 Gartner 给出的 CASB 逻辑图可以看出，CASB 作为部署在客户和云服务商之间的安全控制点。通过嵌入身份认证、设备识别、单点登录、异常监控、加密等企业安全策略，来监控和防护企业用户对云上资源的连接访问。

F.4.1 核心功能：

- 可见性：目前 SaaS 和很多其他的公有云服务缺乏企业级的活动监控，CASB 可以提供对企业内使用云服务的数据、使用人员、客户端设备以及使用情况，提供集中化视图，对异常行为进行检测、阻断和记录，可以识别哪些云应用被哪些员工使用了，从而避免了 Shadow IT 的存在。
- 合规性：企业 IT 系统往云上迁移后，仍然能满足外部法律以及内部标准等合规性要求，

并对云服务商进行信任评级、提供内容监控、审计日志等功能。CASB 的特性可以很好地弥补许多云应用以及基础设施的合规缺口，不论访问云服务的用户与设备是在网络边界的内部或者外部。

- 数据安全：企业想要掌控自己的数据，不管这些数据存储和处理是在终端用户的设备上还是在云服务商服务器，CASB 可以实现结合人员、设备、内容和应用多个维度，提供 DLP、Encryption、Tokenization 等多种类型的数据安全保护，防止云端数据泄露。CASB 可以提供基于上下文，感知业务的安全策略下发。
- 威胁防护： CASB 可以提供云服务商基础设施威胁防护之外的一些关乎企业用户自身的特定威胁，诸如账户劫持问题。CASB 可以帮助企业对进出云上的数据、用户访问云服务资源行为进行监控，及时发现威胁并且做出防御。

F.4.2 工作模式

Proxy 模式

在 Proxy 模式中，CASB 串联入用户端与云服务端，对用户端上传到云服务端的上行流量做预处理，对云服务端下载到用户端的下行流量做后处理。CASB 在用户端与服务端之间既扮演正向代理又扮演反向代理来完成工作。CASB 服务商有公有部署，也有私有部署，还有一少部分二者都支持。

API 模式

在 API 模式中，用户端数据直接传给云服务商，CASB 并不处理所有流量，用户赋予 CASB 访问云服务的权限，CASB 通过利用云应用的 API，控制和定义企业安全策略，来监控各种层级云服务管理员以及终端用户对云计算资源的访问情况。

从上述信息中可以看出，由于云服务的大量使用，用户在使用应用进行数据处理时，不论是用户还是数据，都不一定处于受严格保护的企业内部。因此 CASB 所提供的产品功能也就有别于大家常见的传统安全产品，比如 Web 应用防火墙（WAF）、上网行为管理、下一代防火墙（NGFW），甚至是数据库加密 / 审计产品。CASB 产品的设计理念来源于保护对象的变化：在云端，虽然数据是用户的，但是处理和存储数据的系统并不归用户所有，因此难以保证用户能够持续拥有数据的主权。CASB 能够面对多个云服务提供统一的策略和数据安全治理规则，并提供对用户和设备、敏感数据使用情况、用户行为的细粒度可见性和控制能力。

F.5 IAM 技术

IAM 是一套全面建立和维护数字身份，提供有效安全的 IT 资源访问的业务流程和管理手段，实现组织信息资产统一的身份认证、授权和身份数据集中管理与审计。身份和访问管

理是一套业务处理流程，也是一个用于创建、维护和使用数字身份的支持基础结构。

可信计算是一种能从可信硬件、可信软件、可信网络和可信应用等诸多方面保障系统安全的技术。身份认证是确保平台安全可信的有效方法。平台可以通过提供自己的有效身份信息证明自己是被信任的终端实体。

身份识别与访问管理（Identity and Access Management，IAM），几乎是所有 IT 服务设计与实施过程中最基础的信息安全问题。用户身份及他们对于应用及数据的访问级别在业务领域处于核心位置。因而，必须对其实施高效管理。当前，由于所部署的应用和资源日益增长，同时，面对企业内外部的用户数量与日俱增，身份管理任务倍加繁重，机构有必要建立一套全面的维护数字身份的机制，有效、安全地提供 IT 资源访问的业务流程和管理手段，从而实现组织信息资产统一的身份认证、授权和身份数据集中管理与审计。主流 IAM 均采用 PKI 数字签名方式设计身份认证协议。在基于数字签名的身份认证协议中，用户拥有一对公私钥对，私钥用于对消息进行签名，公钥传输给对方进行签名验证，以保证使用者的安全性、完整性和不可抵赖性。然而，再具体实现的技术上，主要分为两方认证与第三方认证机制。

F.5.1 基于两方认证的 IAM

伴随机构 IT 系统复杂度上升，用户单点登录即可使用所有相互信任的应用系统已经成为移动互联网时代各机构 IAM 管理的主流。基于两方认证的单点登录 (Single Sign On，SSO) 成为流行的企业业务整合的解决方案。

（1）基于 cookies 实现 SSO。CAS(Central Authentication Service) 是 Yale 大学发起的一个开源项目，是最简单实效的 SSO 选择。从结构体系看，CAS 包含两部分：CAS Server 与 CAS Client。CAS Server 负责完成对用户的认证工作，会处理用户名 / 密码等凭证 (Credentials)；CAS Client 负责部署在客户端，原则上，CAS Client 的部署意味着，当有对本地 Web 应用的受保护资源的访问请求，并且需要对请求方进行身份认证时，Web 应用不再接受任何的用户名密码等类似的 Credentials，而是重定向到 CAS Server 进行认证。目前，CAS 协议支持非常多的客户端应用，包括 Java、.Net、ISAPI、Php、Perl、uPortal、Acegi、Ruby、VBScript 等。

CAS 基础协议旨在完成一个很简单的认证任务，即通过用户打开浏览器，直接访问应用服务时重定向到 CAS Server 进行认证，CAS Client 和 CAS Server 相互核实 Service Ticket 核实后，告知用户 Service Ticket 对应确凿身份，CAS Client 才会对当前 Request 的用户进行服务。以 Filter 方式过滤从客户端过来的每一个请求，CAS Client 会重定向用户请求到 CAS Server 发送基于 http 或 https 请求，以证明用户的可信度。CAS Server 校验用户提供的正确凭证作为认证依据后，产生缓存、并返回随机的 Service Ticket，且重定向用户到 CAS Client 以确保认证的不可伪造性。

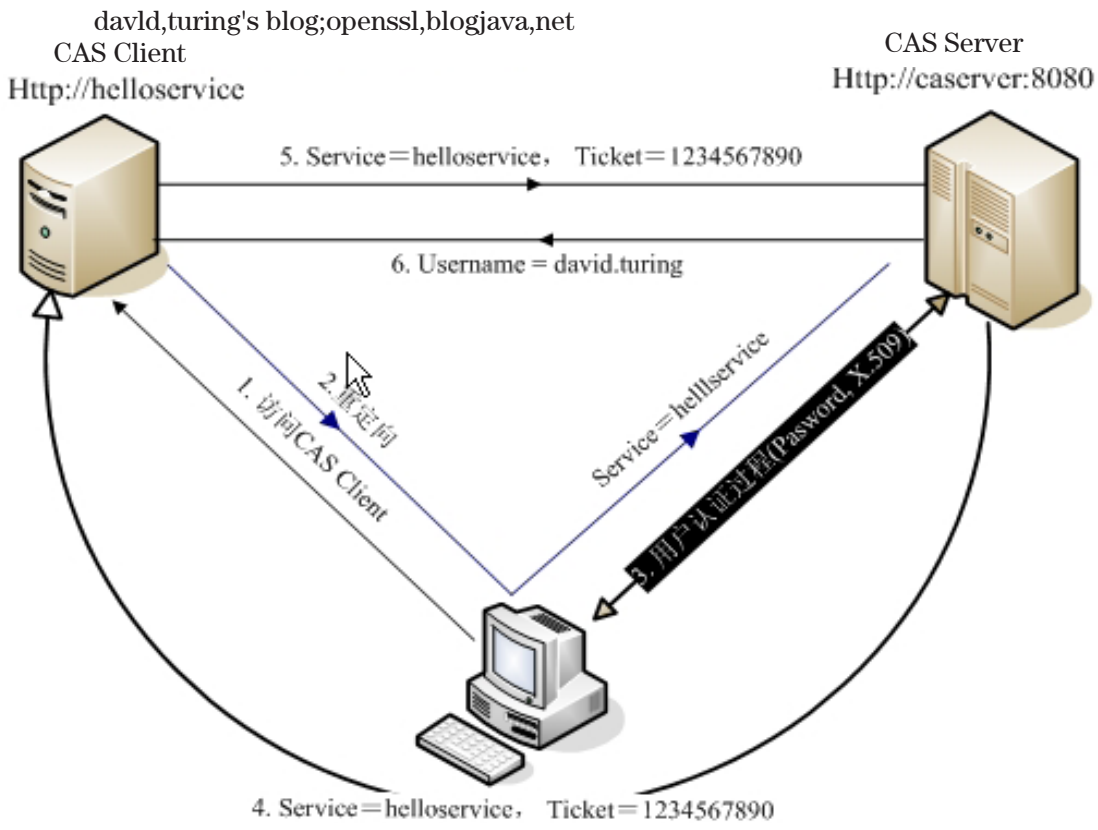


图 42　CAS 的基础模式

1（2）Broker-based（基于经纪人），例如 Kerberos 等；这种技术的特点就是，有一个集中的认证和用户帐号管理的服务器。Kerberos 协议使用中央数据库管理用户身份数据，经纪人被用于请求验证电子身份数据，并利用 Session Key 证明身份后加密传输所有会话，以确保隐私和数据完整性。不过由于不使用非对称密钥算法，因此在抗抵赖性上具有缺陷。

F.5.2 基于第三方独立 CA 的 IAM

（1）安全断言标记语言（Security Assertion Markup Language，SAML）实现基于 XML 的标准并在不同的安全域 (security domain) 之间交换认证和授权数据的协议。SAML 为了在两个拥有共享用户的站点间建立安全可靠的信任关系，SAML 依靠双向 SSL 加密信道完善安全标准，保护源站点和目标站点之间通信的安全。

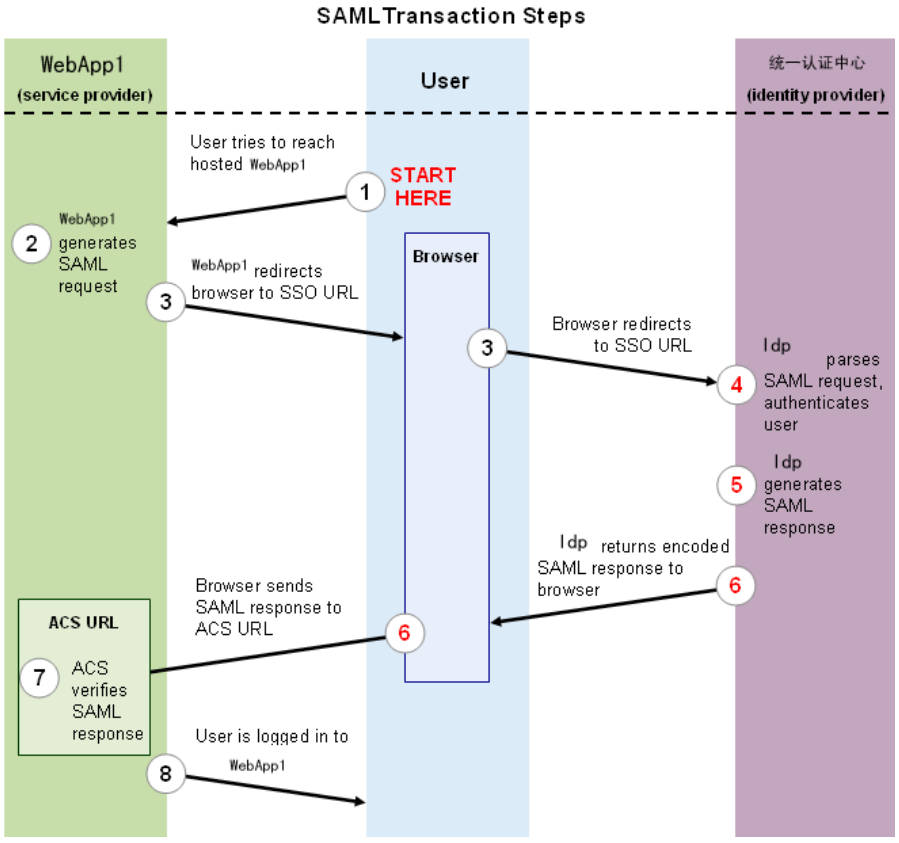


图 43　SAML 的通讯步骤

（2）可信计算组织 (Trusted Computing Group,TCG) 规范 1.1 版本采用基于可信第三方平台身份认证机制，如图所示。

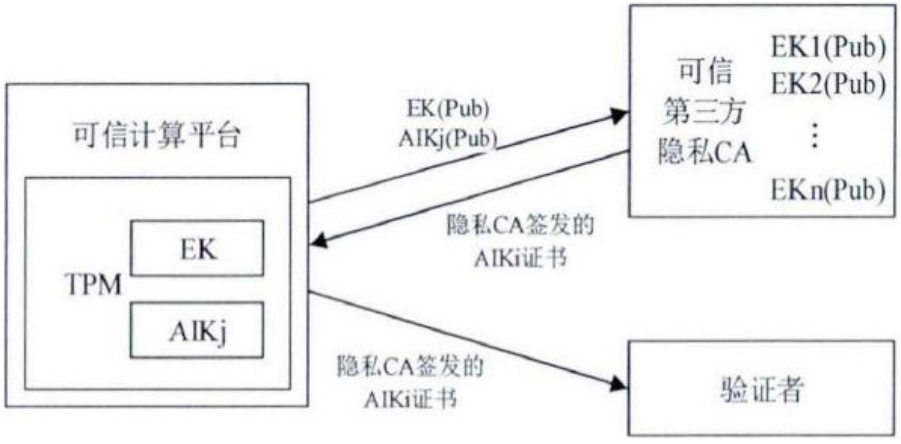


图 44　身份认证机制

该机制中引入可信第三方隐私 CA 保护平台身份信息不被泄露。该方案中，证明者将身份信息发送给可信第三方平台，由可信第三方对证明者的信息进行验证，如果证明者的身份信息有效，则可信第三方为其颁发数字证书。证明者在请求服务时，使用数字证书中的私钥

对身份信息签名，并将数字证书和签名信息一起发送给验证者，验证者使用收到的数字证书和签名信息验证证明者身份的有效性，并根据验证结果给出响应信息。

综上，在 IAM 中，单点登录 (SSO) 结合包括密码、令牌、X.509 证书、智能卡、定制表单和生物识别等技术的强认证管理，进行基于 webservice 的统一策略的集中式授权和审计，才能够适应地监控、管理、维护与审计环境下的企业应用。认证机构 CA 作为 PKI 体系中的公正服务方，保证了 PKI 体系中被验证的数据是基于哈希值的数字签名、公钥在数学上的正确性和签名私钥的合法性。

F.6 UEBA

User and Entity Behavior Analytics（UEBA 用户行为分析）是一个解决方案，它通过分析来构建用户和对象（包括主机，应用程序，网络流量和数据库等）的标准配置以及正常行为模型，相较标准基线，对异常行为的分析可以帮助用户发现安全威胁和隐患。UEBA 常用来检测恶意的内部人员和外部攻击者对企业信息系统的渗透和数据窃取。

Gartner 从用例、用户、分析等三个维度上定义了 UEBA 方案，这三个支撑也可以是 3 个独立的产品，共同形成 UEBA 的解决方案。

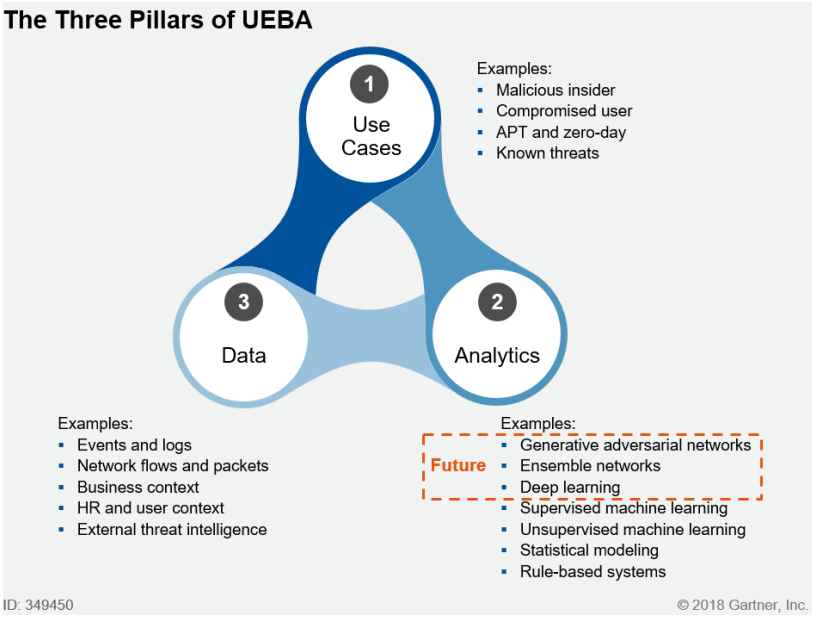


图 45　UEBA 的三个支撑维度

F.6.1 核心技术

1. 提供使用用例：

●提供高权限用户和访问对象的行为、外部黑客的攻击和 0day 漏洞以及已知的安全威

胁，用以监测所有异常用户行为和威胁。

- 对用户和操作对象的异常行为进行监控、检测和告警。
- 不能只针对单个用户或对象，而是通盘监控与分析。

2. 数据分析：

- 通过机器学习和统计模型，结合现有的访问策略形成用户行为的基本模型和画像。
- 避免只关注单体的访问行为，而是要结合所有用户及其操作对象的访问，整体进行异常分析。
- 未来此部分的分析将向深度机器学习及更智能的分析方向下钻。

3. 提供多种收集数据的方式：

- 从用户和实体活动中提取事件数据，可以从数据源本地获取，比如直接或通过现有存储结构中（中央日志管理 CLM，安全信息与事件管理 SIEM），而不应该主要依赖网络数据包作为主要数据源，或者只通过自己部署的代理程序来收集数据。
- 使用更多外部来源的数据，并支持结构化和非结构化等多种数据类型，也可以考虑商业途径、人力资源数据库以及外部威胁情报等数据来源。

F.6.2 主要场景和功能

独立的 UEBA 方案主要针对以下 5 个应用场景，体现其功能：

- 针对恶意内部人员：监控内部人员和授权的外包人员，针对异常、危险的操作进行监控和识别，而非针对外部黑客攻击。由于内部人员的恶意行为更难以发现，因此 UEBA 产品很难从日志文件中分析出危险行为，还需要更多获取非结构化数据，比如电子邮件、绩效信息以及社交媒体信息等，用以分析内部或外包授权人员的行为，结合人员背景和行为进行分析监测。
- 内部隐患及外部攻击威胁：企业和组织需要能够快速检测攻击行为，比如 APT 攻击及其他未知安全威胁，但是 0day 漏洞的攻击难以发现，而且经常伪装成合法用户进行攻击，如果只使用模型匹配和阈值控制很难监测。UEBA 提供对于这部分攻击的监测，由于该类攻击本身难以识别，UEBA 需要更好的降低误报率，通常需要与 SIEM 工具整合实施。
- 数据泄露：UEBA 在数据泄露场景下的实现需要结合 DLP 产品，基于 DLP 本身对异常行为的检测，结合网络流量和网络节点数据进行更深入的分析，提高对数据泄露威胁的告警质量和优先级。
- 身份和特权访问管理（IAM 和 PAM）：UEBA 产品通过已经建立的权限访问策略监控用户行为，识别特权用户和应用用户的越权访问行为，也有企业使用 UEBA 清理权限分配过大的用户，实现身份和特权访问管理。威胁优先级：基于安全基线的建立和威

胁模型的构建，匹配数据资产和人员角色的访问权限，UEBA 能够指导企业目前存在的安全威胁中哪些级别较高，需要优先处理。

F.7 数据透明加密保护技术

透明加密是一种利用密码技术为基础的数据加密方案，该技术的核心在于解决数据加密防护和密钥管理引起的数据处理效率、系统部署和应用及工具改造的代价，以及对数据自动化运维的影响。所以，需要通过透明加密方案来解决这一难题，并且要根据稳定性和性能的需求，进行平衡，选择合理的系统层进行数据加密处理。

F.7.1 核心功能

F.7.1.1 透明数据加密

透明数据加密的关键就是应用透明，使具有权限的用户对加密“无感”。这样的透明性主要体现在以下方面：

1）SQL 语句透明：SELECT、UPDATE、INSERT、DELETE 等语句进行操作，应用程序不用作修改即可拥有安全特性。

2）存储程序透明：对于应用透明支持的含义还包括对存储过程和函数透明的支持。

3）开发接口透明：提供对应用开发接口的全面透明支持，包括：JDBC、ODBC 等。

4）管理及运维工具透明：数据库自身的管理工具如备份、迁移、导入导出工具等，仍然可以正常使用，不影响日常运维工作。

F.7.1.2 加密算法合规

兼容主流加密算法，支持国家指定的 SM4 加密算法。

F.7.1.3 密文访问控制

产品具备三权分立体系，在传统的数据库超级管理员 DBA 体系上，增设数据安全管理员 DSA，数据库安全审计员 DAA。DBA 和 DSA 相互独立，在不影响数据库本身权限的同时，增强了密文的权限控制，分别从数据库用户，客户端 IP，应用系统等不同层面对密文的访问权限进行了控制，全面防止越权访问，防止数据泄露。而 DAA 可以对 DSA 的配置情况作出有效审计。

对于没有权限的数据库用户，读取加密数据表的时候，可以就密文列返回预设置的缺省值，非密文列正常返回数据。满足数据安全要求的同时，不影响正常的数据库维护或应用测试等场景。

F.7.1.4 性能影响小

数据加密后，对数据库的性能影响应尽量小，特别对加密数据的查询、分组、排序、聚合等操作。

F.7.2 主要技术

为了实现数据透明加密，在技术上可以采用多种加密方案，不同的加密方案在透明性、性能、安全性三个重要方面有不同的效果和表现。下图展示的是典型的“多层数据加密”方案，这里我们主要分析数据透明加密、文件系统透明加密、磁盘加密这三种技术，主要是应为这些技术能够带给用户很好的透明性。

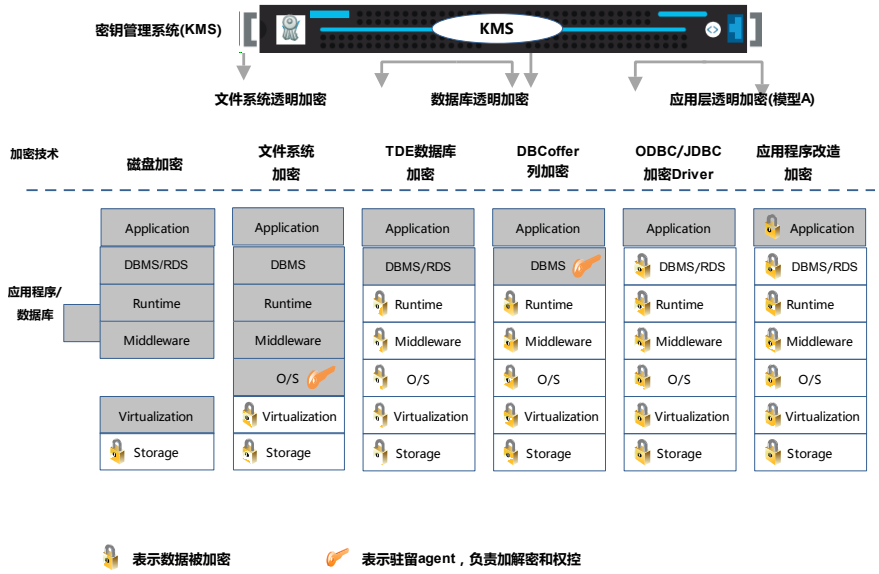


图 46　多层数据加密方案

F.7.2.1 数据库透明加密技术（列加密）

数据库列透明加密是按列对数据进行加密的，针对指定的列，采用指定的加密算法和密钥、盐值等进行加密处理。加密后的数据以密文的形式存储在 DBMS 的表空间中。

只有经过授权的用户才能看到明文数据，并且授权也是按列进行的，这种方式具备很好的灵活性和安全性。非授权用户，将无法读取（查询）加密列和更改加密列的数据。

权限管理上，数据库列透明加密采用了分权的机制，实现了三权分立，有效制约了数据库管理员（DBA）这样的特权用户对数据的访问。同时这种保护又是透明的，不会对管理员的日常工作造成不便。

数据库列透明加密具有应用透明的特性，应用系统和外围维护工具无需改造，涵盖 SQL 语句透明、存储程序透明、开发接口透明、数据库对象透明、管理工具透明。

下图说明了列加密的数据处理机制：当明文数据到达数据库时，被列加密组件自动进行加密处理，之后数据以密文形式保存在数据文件中；在读取数据时，数据被列加密组件根据权限进行自动的解密处理。这些操作对应用都是透明的。

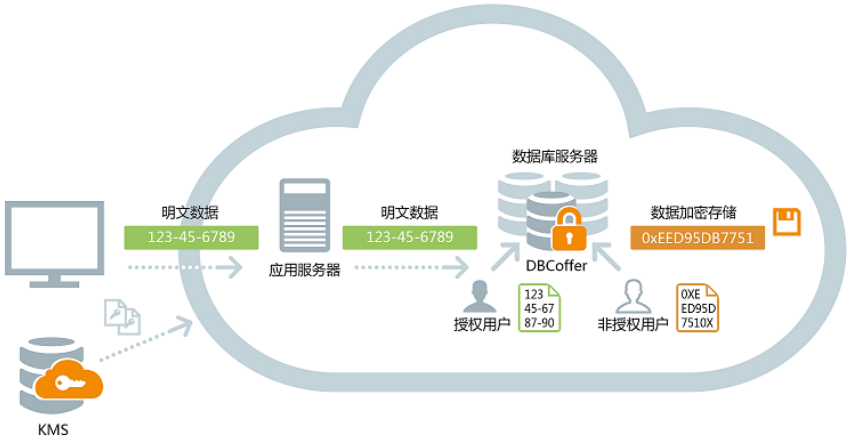


图 47　数据库列透明加密防护技术

F.7.2.2 数据库透明加密技术（TDE 表空间加密）

数据库透明加密（TDE 表空间加密）系统是基于透明加密技术（TDE）的数据库表空间加密。该产品能够实现对数据库中的敏感数据自动加密存储、访问控制增强及三权分立功能。

下图以 Oracle 数据库为例，说明了 TDE 加解密的关键机制：TDE 插件作为 Oracle 的插件，负责对数据存储时对数据进行加密处理；在数据从表空间读取时，负责对数据进行解密处理；并且根据读取数据的数据库账户，进行相应的权限控制。

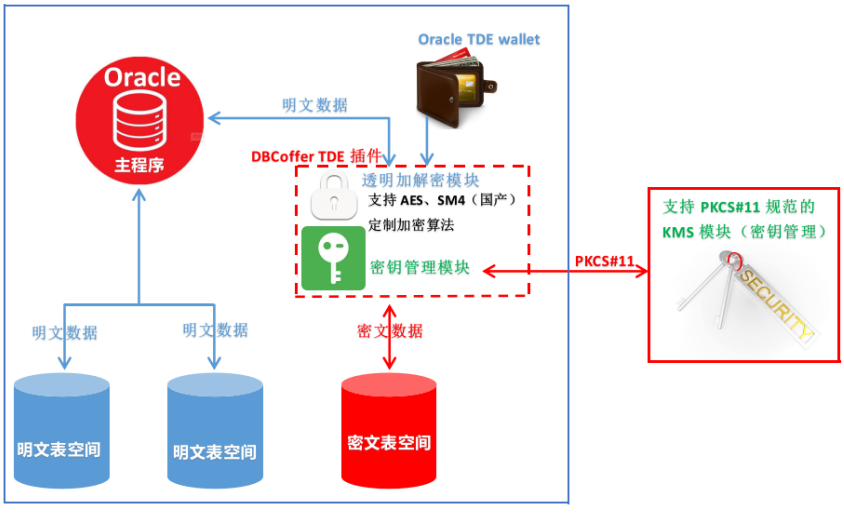


图 48　OracleTDE 加密技术

1）数据加密

针对表空间实现表空间级加密，对表空间内的所有数据全部进行加密，增强数据安全性；支持表级加密，增强安全的同时又兼具灵活性。

2）权限控制

在不影响数据库本身权限的同时，增强了权限控制，分别从数据库用户，客户端 IP，应用系统等不同层面对权限增强，全面防止越权访问，防止数据泄露。

3）独立密钥管理

安全服务组件实现对密钥的管理，包含加密密钥生成，分配，备份，恢复，密钥不出设备，让用户自己掌握密钥，即使数据被盗也无法查看明文。

4）透明访问

TDE 在实现数据安全加密的同时，另一个非常重要的特性就是应用透明，使用者和应用系统不需要关心 TDE 系统进行了哪些保护。这样的透明性主要体现在以下方面：

SQL 语句透明：SELECT、UPDATE、INSERT、DELETE 等语句进行操作，应用程序不用作修改即可拥有安全特性。

存储程序透明：对存储过程和函数透明的支持。

开发接口透明：提供对应用开发接口的全面透明支持，包括：JDBC、ODBC 等。

管理工具透明：支持对数据库的图形管理工具（如：workbench），及常用的第三方管理工具（TOAD、navicat 等）透明，可以正常使用。

5）性能影响小

TDE 加密对数据库性能的影响不超过 7%，不会增加存储空间，对系统 IO 无影响。特别是针对加密数据的分组、聚合等复杂计算，比列加密具有极好的性能优势。

F.7.2.3 文件系统透明加密技术（TDE 表空间加密）

文件系统级透明加密防护是通过在主机操作系统上部署专门的加解密 agent，实现对专门的数据文件或卷（Volume）的加解密。

对操作系统帐户具有权限控制能力，通过指定只有专门的 DBMS 系统帐户才有对文件或卷进行加解密的权限，没有权限的程序无法对数据文件进行读写操作。

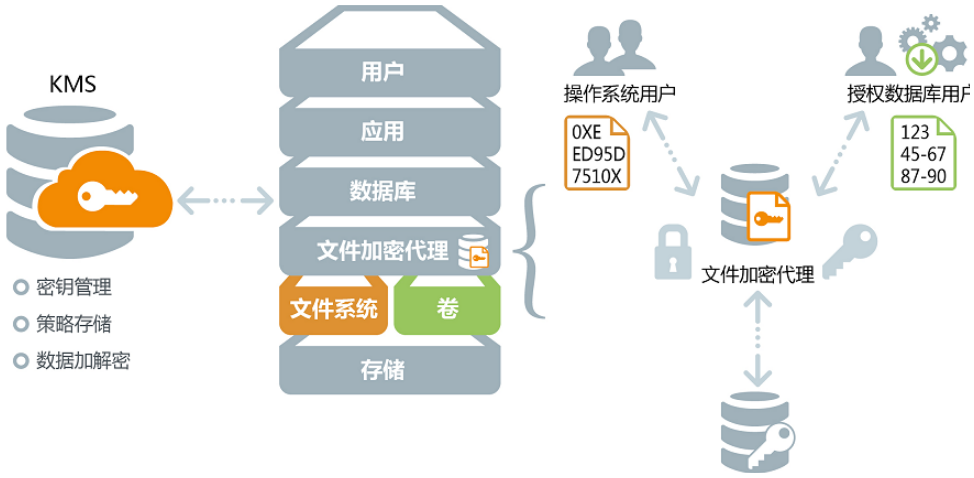


图 49　文件系统级透明加密防护技术

优势：

对数据库系统（DBMS）和应用透明

同时支持结构化（关系型数据库）和非结构化文件（NoSQL 数据库）的加密

有效控制操作系统用户的访问，满足通常的控制需求，例如数据库的执行账户（oeacle、mysql、root 等）

限制：

无法提供细粒度的数据访问审计能力

需要针对不同的操作系统平台提供专门的 agent

无法控制数据库帐户对敏感数据的访问，例如 DBA 账户

F.7.2.4 透明数据加密技术比较

数据透明加密是否能够有效的关键，企业需要在关键数据的安全性、应用系统的功能可用性，和系统可维护性方面综合考虑，来确定适合企业需要的加密保护的技术方案。

下面的两张图表对前面提到的加密防护的关键技术能够提供的防护效果，安全性和部署复杂性进行了对比，供读者参考：

风险	整盘加密	文件系统加密	数据库加密		应用层加密
			TDE 表空间加密	列加密	
防止磁盘丢失引起数据泄漏	√	√	√	√	√
防止操作系统 root 帐户和管理员帐户访问数据	X	√	√	√	√
控制数据库管理员 DBA 访问数据	X	X	√	√	√
抵抗 APT 持续攻击造成的数据泄漏	X	√	√	√	√
提供细粒度的访问记录，法规遵从报告和风险分析	X	X	X	√	√
确保备份数据和数据快照加密存储	X	√	√	√	√
非结构化数据和文件的保护	√	√	X	X	√
防止硬件和数据库厂商“偷窥”	X	X	√	√	√

表 10　各种数据加密技术比较

●文件系统加密 VS 数据库 TDE 加密

性能对比：文件系统的加解密是在文件系统层进行的，并且能够和好的利用文件缓存优化数据读写，所以一般情况下，性能要比数据库 TDE 加解密的性能好。

安全性对比：文件系统加解密的访问控制能力作用在文件系统层，能够控制对文件的访问权限；数据库 TDE 加解密的权限控制作用在数据库内部，能够控制数据库账户对数据为访问，所以在安全性上数据库 TDE 加密要比文件系统加密更加安全。

可靠性对比：数据加密的可靠性在一定程度上是与数据库系统的复杂性相关的；特别的由于 Oracle 数据库的复杂性高，其复杂的外围工具和程序，以及复杂的文件处理（ASM）机制，造成文件系统层的加解密处理要适配这些特性，这在一定程度上造成了文件系统加密机制对 Oracle 数据库的可靠性不足。因此从技术路线的选择上，对于复杂性不是很高的数据库系统加密，文件系统加密和数据库 TDE 加密的可靠性都可以满足；但对于像 Oracle 这种复杂性非常高的数据库系统，文件系统加密对数据库自身可靠性会带来一定的风险，以国外的某主流文件透明加密系统为例，在官方网站上可以看到该系统对 Oracle 数据库带来以下的影响：

1）稳定性影响

造成系统宕机异常。以下为来自官网的资料。

第一个稳定性异常：

Kernel panic at gsch_flt_aio_write() function.

SOLUTION UNVERIFIED - Updated January 24 2017 at 3:24 PM - English

Issue

- Kernel panic occurred during NULL pointer dereference inside gsch_flt_aio_write() function.

Raw

```
[6428(bash)]: gsch_scan(525204,1,0) - interrupted & wait(1000)
[6428(bash)]: gsch_scan(525204,1,0) - interrupted & wait: done
BUG: unable to handle kernel NULL pointer dereference at 0000000000000018
IP: [<ffffffffa036a7b1>] gsch_flt_aio_write+0x31/0x120 [gsch]
PGD 1d6215067 PUD 1d6216067 PMD 0
Oops: 0000 [#1] SMP
last sysfs file: /sys/devices/system/cpu/online
CPU 0
Modules linked in: autofs4 nfs lockd fscache auth_rpcgss nfs_acl sunrpc secvm2(P)(U) secfs2(P)(U) gsch(U) redirfs(U) nf_conntrack_ipv4
nf_defrag_ipv4 iptable_filter ip_tables vsock(U) dsa_filter(P)(U) ip6t_REJECT nf_conntrack_ipv6 nf_defrag_ipv6 xt_state nf_conntrack
ip6table_filter ip6_tables ipv6 uinput ppdev microcode vmware_balloon parport_pc parport sg vmci(U) i2c_piix4 i2c_core shpchp ext4 jbd2
mbcache sd_mod crc_t10dif sr_mod cdrom vmxnet3 vmw_pvscsi pata_acpi ata_generic ata_piix dm_mirror dm_region_hash dm_log dm_mod [last
unloaded: speedstep_lib]
```

第二个稳定性异常：

```
* 3910356 (Tracking ID: 3908785)

SYMPTOM:
System panic observed because of null page address in writeback structure in case of
kswapd
process.

DESCRIPTION:
Secfs2/Encryptfs layers had used write VOP as a hook when Kswapd is triggered to
free page.
Ideally kswapd should call writepage() routine where writeback structure are correctly filled.  When
write VOP is
called because of hook in secfs2/encrypts, writeback structures are cleared, resulting in null page
address.

RESOLUTION:
Code changes has been done to call VxFS kswapd routine only if valid page address is
present.
```

2）平台特性无法支持

典型的是对 ASM 这一 Oracle 数据库高端特性无法兼容。

SYMPTOMS

ASM disks are changed from Character to Block devices using "vormetric" encryption and after that not able see ASM disks to add back

CHANGES

Changed Character to Block devices

crw-rw---- 1 oragrid asmadmin 18, 8 Sep 13 02:17 /dev/asmdevices/asm001

crw-rw---- 1 oragrid asmadmin 18, 12 Sep 13 02:17 /dev/asmdevices/asm003
crw-rw---- 1 oragrid asmadmin 18, 14 Sep 13 02:17 /dev/asmdevices/asm004
crw-rw---- 1 oragrid asmadmin 18, 23 Sep 13 02:17 /dev/asmdevices/asm005

to

brw-rw---- 1 oragrid asmadmin 18, 8 Sep 13 02:18 /dev/asmdevices/asmve001>>>>>>
brw-rw---- 1 oragrid asmadmin 18, 12 Sep 13 02:18 /dev/asmdevices/asmve003>>>>>
brw-rw---- 1 oragrid asmadmin 18, 14 Sep 13 02:18 /dev/asmdevices/asmve004>>>>>
brw-rw---- 1 oragrid asmadmin 18, 23 Sep 13 02:18 /dev/asmdevices/asmve005>>>>>

☆ **Block devices not supported for ASM (Doc ID 2310512.1)**

In this Document

Symptoms
Changes
Cause
Solution
References

APPLIES TO:

Oracle Database - Enterprise Edition - Version 11.2.0.3 and later
Oracle Database Cloud Schema Service - Version N/A and later
Oracle Database Exadata Express Cloud Service - Version N/A and later
Oracle Database Exadata Cloud Machine - Version N/A and later
Oracle Cloud Infrastructure - Database Service - Version N/A and later
IBM AIX on POWER Systems (64-bit)
IBM AIX on POWER Systems (32-bit)

3）性能影响


Copyright (c) 2019, Oracle. All rights reserved. Oracle Confidential.

Performance issue when using Vormetric agent for encryption of database files (Doc ID 2098275.1)

In this Document

Symptoms
Cause
Solution
References

APPLIES TO:

Oracle Database - Enterprise Edition - Version 11.2.0.1 and later
Information in this document applies to any platform.
Specifically when using Vormetric agent for encryption of database files.

CAUSE

Introduction of a third-party encryption module that mediates interaction between the database instance and the database files. In this particular case, the customer configured Vormetric Encryption Expert Agent to protect Oracle Database files, including redo and archive logs. I/O speeds were impacted slightly for all write operations. Under normal database load, the impact did not introduce problems, but during heavy write activity, the increase in write time impacted the archiver's ability to copy archive logs to the encrypted file system enough that the archiver lagged the lgwr processes. This caused a cascade of wait events that resulted in significant performance issues.

SOLUTION

Modify Archive Log destination to a volume that does not use the Vormetric encryption agent.

Note:
Oracle does not support any 3rd party kernel/user modules, libraries or filters that inspect or change the behavior of the Oracle Database, including agents that modify the way in which the database interacts with the file system. When a database with these 3rd party modules, libraries or filters encounters performance, stability or corruption issues, Oracle will request that you reproduce the problem on systems that do not include such intrusive software.

REFERENCES

NOTE:1970146.1 - Database Instability Caused by 3rd Party Kernel Modules

F.8 数据库防勒索技术

从 2016 年 RushQL 勒索病毒对 Oracle 数据库勒索开始，勒索病毒已经成为了一个新的数据库安全威胁，并且被不断的进行升级，使得传统的防护手段防不胜防。

这种数据库勒索病毒的泛滥，很重要的原因是随着数据越来越重要，使病毒技术从纯攻击转化为通过病毒攻击进行获利的商业模式，而数据库文件作为重要的数据载体，一旦被攻击，会造成非常严重的数据丢失等后果，从而成为最重要的一种攻击目标。

F.8.1 数据库勒索手段分析

从勒索手段上，一般有以下几种情况：

1：通过对数据库管理工具植入病毒程序，在数据库操作时对数据库安装勒索存储程序。典型的病毒为 RushQL 勒索病毒。

2：通过在操作系统层植入病毒程序，对数据文件进行加密，使得数据文件无法再被使用，从而达到勒索的目的。典型的病毒为 Globelmposter 勒索病毒。

以上勒索手段，从技术上讲，都是病毒技术的变种。

F.8.1.1 防勒索技术

由于勒索手段的多样性，防勒索手段从技术上，存在几种不同的技术路线：

1：针对 RushQL 这类通过数据库客户端工具，向数据库系统植入数据库勒索程序进行勒索，可以通过数据库防攻击技术（数据库防火墙），对数据库的操作进行过滤，对植入数据库勒索程序的行为进行拦截阻断和报警，这种方式可以有效防护来自客户端程序的勒索攻击。

2：针对 Globelmposter 这类通过操作系统，获得对数据库文件的操作权限，从而对数据库文件进行加密，来达到勒索目的，通常的防护是采用防病毒技术，查杀勒索病毒，来达到防护作用；但是由于勒索病毒的不断升级和变种，往往是病毒升级并爆发后才能进行防护，0day 期间的防护能力几乎没有，这也是为什么会造成勒索病毒周期性大面积爆发的一个重要原因。所以需要在防病毒技术的基础上进行针对性的增强，通过采用白名单机制来达到“一劳永逸”的防护效果，关键技术点如下：

2.1：通过部署操作系统的安全防护组件，严格控制允许访问数据库文件的程序—建立白名单程序，只有白名单内的程序才能操作数据文件，其他的程序的操作全部进行拦截告警。

2.2：通过对白名单程序进行“签名”，保证白名单程序一旦被篡改，在程序操作数据库文件时可以及时被发现，并对篡改后（植入了勒索病毒）的程序进行拦截告警。

附件 G　白皮书参与单位介绍

发布单位介绍

中国网络安全与信息化产业联盟数据安全治理委员会（以下简称数据安全治理委员会）是在中国网信联盟的指导与支持下，由北京市“数据库安全保障小组组长单位”安华金和牵头，联合业内知名企业发起的专业技术创新工作组织，这也是迄今为止，全国首家数据安全领域的专项委员会。

委员会将在中国网信联盟的指导下，在行业专家及学术专家的支持下，以行业数据安全应用为目标、以产业协作为主线、以技术创新为核心，形成在数据安全领域的技术研究、思维碰撞、学术探讨、行业实践分享的交流平台，探索和推动政府、行业、企业在数据安全治理工作上的思路、规范和技术实践；以期达成在数据即资产时代，既保障数据安全、又促进数据的分享和使用。

2018 中国数据安全治理峰会，数据安全治理委员会正式成立并对外发布《数据安全治理白皮书》1.0 版本。2019 年推陈出新至 2.0 版本。未来，委员会各成员单位将发挥各自所长，持续开展产业研究与方案整合，共同推动数据安全治理理念与框架在各行业中的应用落地与经验分享，以期为各级政府与企业单位提供具有行业针对性的数据安全治理方案与技术支撑，帮助共同实现数据资产的价值释放。

委员会成员名单

北京安华金和科技有限公司	主 任 单 位
中国电子中国信息安全研究院	副主任单位
南开大学网络空间安全学院	副主任单位
中金金融认证中心有限公司	副主任单位
阿里云计算有限公司	副主任单位
北京炼石网络技术有限公司	
北京谷安天下科技有限公司	
北京国泰网信科技有限公司	
北京海泰方圆科技股份有限公司	
北京金源动力信息化测评技术有限公司	
北京九州云腾科技有限公司	

北京可信华泰信息技术有限公司
北京莱特思科技有限公司
北京立思辰科技股份有限公司
北京明朝万达科技股份有限公司
北京软件产品质量检测检验中心
北京数字观星科技有限公司
北京数字认证股份有限公司
北京亿赛通科技发展有限责任公司
北京中睿天下信息技术有限公司
广州竞远安全技术股份有限公司

G.1 主要撰写单位介绍北京安华金和科技有限公司

北京安华金和科技有限公司（以下简称安华金和），公司 2009 年 3 月 2 日成立至今，一直专注于数据安全领域，是中国专业的数据安全产品及解决方案提供商，由长期致力于数据处理和信息安全领域的专业人士共同创造。安华金和能够提供数据库安全全线产品及方案，并以此为支撑，全国首家提出“数据安全治理”框架，提供涵盖人员组织、安全策略、流程制定及技术支撑全方位的整体安全思路与方案；安华金和作为独立的第三方云数据安全服务商（CDSP），为国内外各大云平台用户提供专业的数据安全保障，同时，安华金和是中国最大的公有云平台——阿里云在云数据安全领域的重要战略合作方。

围绕公司使命与愿景，安华金和主营业务方向分为三大部分：

1. 围绕数据库安全，安华金和推出全线数据库安全产品及解决方案。

2. 推进数据安全治理理念在各行业的方案落地和实践。

3. 面向公有云和私有云环境特性，提供云数据安全全线产品，为公有云和私有云用户提供数据安全整体解决方案。

北京数字认证股份有限公司

北京数字认证股份有限公司（简称“BJCA”）是北京市国有资产经营有限责任公司控股的国有企业，是国内领先的信息安全解决方案提供商，主要业务为电子认证服务、电子认证产品及可管理的信息安全服务。

作为领先的电子认证企业，BJCA 建立了覆盖全国的电子认证服务网络和完善的电子认证产品体系，应用领域覆盖政府、金融、医疗卫生、彩票、电信等市场，在电子政务、医疗信息化领域的市场占有率位居行业前列。作为专业的可管理信息安全服务提供商，BJCA 拥有国内一流的信息安全专家和服务团队，建立了服务专业、响应及时、保障可靠的可管理的

信息安全服务体系，为广大客户提供涵盖信息系统全生命周期的安全集成、安全咨询、安全运维等服务。

中金金融认证中心有限公司

中金金融认证中心有限公司（即中国金融认证中心 China Financial Certification Authority，简称 CFCA），是由中国人民银行于 1998 年牵头组建、经国家信息安全管理机构批准成立的国家级权威安全认证机构，是国家重要的金融信息安全基础设施之一。

在《中华人民共和国电子签名法》颁布后，CFCA 成为首批获得电子认证服务许可的电子认证服务机构。截至目前，超过 2400 家金融机构使用 CFCA 的电子认证服务，在使用数字证书的银行中占 98% 的份额。自 2000 年挂牌成立以来，CFCA 一直致力于全方位网络信任体系的构建，历经十多年发展，已经成为国内最大的电子认证服务机构。

北京亿赛通科技发展有限责任公司

北京亿赛通科技发展有限责任公司，成立于 2003 年，是绿盟科技全资子公司，已发展成为国内领先的数据安全、网络安全及安全服务三大业务供应商。拥有完全自主知识产权的软件企业，并已取得“高新技术企业证书”、“涉密信息系统产品检测证书”、“军用信息安全产品认证证书”、“商用密码生产定点单位证书”等多项资质认定。作为国内具实力的、拥有完全自主知识产权的安全厂商，公司业务已进军海外市场，并为八大行业、万余家企业、过百万终端铸就了坚不可摧的核心技术保障。