中国企业数字化转型合规白皮书

MeritsTree 植德

北京植德律师事务所

二〇一九年五月

中国企业数字化转型合规白皮书

植德律师事务所

王伟、朱宣烨、曾雯雯

Orrick, Herrington & Sutcliffe LLP

Antony Kim, Kolvin Stone, Aravind Swaminathan, Xiang Wang, Jeff Zhang and Betty Louie

Kelvin Gao

北京市东城区东直门南大街 1 号来福士中心办公楼 5 层，100007
5th Floor, Raffles City Beijing Offices Tower, No.1 Dongzhimen South Street, Dongcheng District, Beijing 100007 P.R.C.

T. 010-56500900 F. 010-56500999

www.meritsandtree.com

Cybersecurity is never just a technology problem, it’s a people, processes and knowledge problem.

-National Institute of Standards and Technology (NIST)

版权所有 翻印必究
版权所有 翻印必究

目录

版权所有 翻印必究

版权所有 翻印必究

版权所有 翻印必究

中国企业数字化转型合规白皮书

1. 前言

1.1. 中国企业数字化转型的必然

根据全球著名信息技术、电信行业和消费科技咨询公司 IDC 预计，到 2020 年，亚太地区（不含日本）55%的企业都将以新型业务模式及数字化产品和服务重塑市场格局。

麦肯锡也在其报告《中国数字经济如何引领全球新趋势》中指出，随着中国的数字化进程逐步推进，各个行业的价值链都将经历营收和利润池的彻底变革。这种创造性变革将发生在世界每一个角落，但由于中国的传统行业效率低下、拥有巨大的商业化潜能，因此这一变化在中国将尤为迅猛和激烈。经历这次转变脱颖而出的企业很有可能拥有庞大体量，足以影响全球数字化格局。

因此，对于任何一个中国企业的领导者而言，必须考虑本企业的数字化转型问题。

1.2. 网络与数据是中国企业数字化转型中的核心

无论是传统行业的互联网化、智能化、数据化改造还是新兴行业、新型商业模式，任何一个中国企业的数字化转型都首先必然涉及网络和数据。

正如曾鸣先生在《智能商业》中一再强调的，智能商业的双螺旋是网络协同和数据智能。在中国企业数字化转型中网络和数据无疑占据核心位置。因此，在中国企业数字化转型的过程中，每个企业都应该关注本企业的网络安全与数据合规问题。

1.3. 网络安全与数据合规的重要性

中国政府历来十分关注互联网可能引发的风险。中国企业须时刻考虑如何在中国监管部门允许范围之内合规经营。

2016 年 11 月 7 日《中华人民共和国网络安全法》（下称“《网络安全法》”）通过具有里程碑式的意义。《网络安全法》是我国第一部有关网络安全与数据合规的综合性立法。

此后，网络安全、数据泄露与丢失的监测与防范，将成为企业在转型过程中建立安全管理体系的焦点之一。

版权所有 翻印必究

网络安全与数据合规是相对较新的领域，而且与网络技术、新兴商业模式相关，很多企业家和投资人只预见到数字化转型广阔的商业前景，但尚未能洞察网络安全与数据合规的风险。以数据合规中较常见的个人信息保护为例，根据中华人民共和国首席大检察官、最高人民检察院检察长张军 2018 年 11 月 8 日在第五届世界互联网大会“大数据时代的个人信息保护”分论坛的发言，2016 年 1 月至 2018 年 9 月，中国检察机关以侵犯个人信息罪共起诉 8,700 多人。

因此，任何一个公司在进行数字化转型时必须对网络安全与数据合规的重要性有清晰的认识。

1.3.1. 维护企业资产价值和核心竞争力

企业的原数据、衍生数据、数据的算法等，是数字化企业的宝贵资产以及核心竞争力。网络安全与数据合规建设，对企业持有数据作 data mapping，确保企业合规使用数据，是维护企业资产价值和核心竞争力的重要前提和保障。网络安全不合规，或者数据处理不合规都会直接导致企业持有的数据资产价值甚至企业本身价值的降低甚至归零，在投融资并购、上市、融资、争取政府采购项目等情形下丧失交易机会。

1.3.2. 避免法律责任

各国监管者高度关注网络安全和数据合规。为应对数字化转型背景下网络安全和信息保护的机遇与挑战，包括中国在内的诸多国家，均纷纷围绕数字经济和网络安全的主题，制定了多层次、各领域的数据安全保护法规，对网络安全和个人信息保护的内容加以强化保护，并对于违反相应制度的行为设定了多种法律责任，包括司法机关裁定的损害赔偿、赔礼道歉、恢复原状等民事责任；行政监管部门给出的责令整改、取消市场准入资格、罚款、警告等行政责任；司法机关针对严重的违法行为判处的剥夺人身自由、罚金等刑事责任。更为重要的是，由于网络的无国界性，如果一个公司的业务涉及多个司法区域，那么有可能同时涉及多个司法区域的法律监管，这对于公司的合规是个重大的挑战。

在科技飞速发展的时代，并没有防范信息泄露等安全事故发生的万无一失的方法。企业依法建立网络安全和数据合规内控制度并且切实执行将是企业证明自己尽到合规义务的重要证据。退一步说，即

版权所有 翻印必究

便出现了安全事故，企业也可以基于已经尽到的合规义务而降低甚至避免承担法律责任。

1.3.3. 主动维权

企业通过对自身合规的梳理，可以发现自身数据被侵害的情况，以及侵害行为可能触犯的法律规范，从而能够选择适当的方式维护自身的合法权利。

我们大胆预测，正如专利侵权诉讼一样，一定有越来越多的公司会主动发起数据侵权之诉。

2. 网络安全与数据合规风险

网络安全和数据合规最直接的目的在于防范承担法律责任。企业数据战略的实现以及数据价值的保护和商誉的维护核心是避免触及法律责任的红线。如前所述，网络安全与数据合规过程中涉及的法律规范繁杂，责任制度多元。就此，我们简单分析民事、行政以及刑事风险如下。

2.1. 民事争议风险

我们注意到，随着企业数字化转型进程不断加快，与网络安全和数据泄露有关的民事案件越来越多。根据我们对案例的分析和归纳，民事案件主要涉及合同、不正当竞争、侵权等三种民事案由。

2.1.1. 合同纠纷

很多企业在缺乏对网络安全及数据合规充分理解的前提下即开展业务、签订协议，这种情况极易产生合同纠纷，典型案例如下:

序号	典型案例	案情简要	植德合规建议
1	北京亿维视讯网络技术有限公司与北京企商在线数据通信科技有限公司网络服务合同纠纷	双方签署合同约定亿维公司租用企商在线公司的服务器经营网站。后企商在线公司的服务器损坏导致永久丢失了3.5个月内网站运营相关的数据，修复及租赁到期后，企商在	（1） 公司应建立统一的第三方供应商管理制度，对供应商的选择和监督作出科学安排; （2） 无论是供应商还是公司本身，都应该制定数据安全应急预案，对数据的存储、

序号	典型案例	案情简要	植德合规建议
		线又告知亿维公司网站数据被删除且无法恢复。	备份做预先安排; （3） 在服务合同中，双方应明确权利义务，并阐明特殊事件（如数据泄漏）发生后的责任承担问题。
2	智慧云游(北京）科技有限公司与北京塔塔信息咨询有限公司合同纠纷	塔塔信息以接口的方式向智慧云游提供数据及服务,并按照查询次数收取费用,后双方因费用退换问题发生经济纠纷,智慧云游将塔塔信息诉至法院。法院认为,塔塔信息提供的数据项目包括:个人学历数据库、手机号在网时长数据库、个人金融征信画像库等,本案所涉相关事实已涉嫌刑事犯罪,故驳回原告起诉并移送公安机关处理。	（1） 如果合作双方中，有一方的商业模式有无法弥补的缺陷（如涉及侵权或违反法律法规的规定），那么与该方有关的其他合同权利也可能受到影响，不一定能得到保障; （2） 公司应重点关注数据业务中是否包含个人信息的问题，如果涉及个人信息，无论是服务提供方还是服务接受方都会面临巨大的法律风险。
3	冯某与交通银行股份有限公司连云港分行信用卡纠纷	交通银行股份有限公司连云港分行在未严格履行信用卡开户所必经程序的情况下,将他人所持账号为 52×××30 的信用卡，登记在冯某名下,并对冯某的信用记录产生了不良影响。	由于金融机构往往掌握着个人征信信息、身份信息等敏感信息，因此应该格外关注业务的数据合规风险。

版权所有 翻印必究

序号	典型案例	案情简要	植德合规建议
4	黄某诉中国移动通信集团湖南有限公司、中国移动通信集团湖南有限公司长沙分公司合同纠纷	黄某起诉称移动长沙分公司通过飞信后台非法窃取黄某个人信息且在黄某不知情的情况下擅自增加其飞信好友人数。	App 违法违规收集使用个人信息是监管机构的关注要点之一，未经同意收集使用个人信息以及未经同意向他人提供个人信息极易被用户投诉或者起诉。
5	黄某诉中国东方航空股份有限公司航空旅客运输合同纠纷	黄某通过东航公司的销售热线购买了 4 张机票，之后收到包含其个人信息的诈骗短信。案外人中国 XX 股份有限公司与东航签订了《航空公司服务协议》，约定东航在中国境内的所有机票销售全部使用 XX 股份公司的系统处理完成。原审审理过程中，法院依职权向当地公安分局就黄某的报案情况进行调查，公安分局经审查认为符合刑事立案条件。	公司应当慎重选择第三方供应商，并在合同中约束第三方供应商使用数据的权利。

2.1.2. 不正当竞争纠纷

由于目前对企业的数据权利、数据产品的权利尚没有法律层面的明确界定，所以《中华人民共和国反不正当竞争法》（下称“《反不正当竞争法》”）成为了数据权属、数据产品利益纠纷案件的主要适用法律。企业使用爬虫等技术、或者通过 API、SDK 等获取其他企业数据极易引发不正当竞争的质疑，涉及反不正当竞争的案件甚至有可能导致刑事责任。典型案例如下：

版权所有 翻印必究

序号	典型案例	案情简要	植德合规建议
1	新浪诉脉脉不正当竞争纠纷	根据新浪微博开放平台的《开发者协议》，脉脉和新浪通过微博平台 Open API 进行合作，基于该合作，用户可以使用手机号和新浪微博账号注册脉脉。后新浪发现，脉脉利用爬虫技术抓取非脉脉用户的微博账户信息。	（1） 公司通过 OpenAPI 模式获取用户信息时应遵守“用户授权”+“平台授权”+“用户授权”的三重授权原则，即用户同意平台向第三方提供信息，平台授权第三方获取信息，用户再次授权第三方使用信息。而且用户的同意应是在充分知晓的前提下作出的明确同意。 （2） 如果公司的行为实为一种“不劳而获”、“食人而肥”的行为，或对同类产品产生了“此消彼长”的不良影响，则可能被视为扰乱了竞争秩序，构成不正当竞争行为。
2	大众点评诉百度地图不正当竞争纠纷	百度地图在用户搜索某商户时，将来源自大众点评的对该商户的评价信息显示在搜索结果上，注明了信息来自大众点评并且设置了跳转链接。法院认为，百度地图采用技术手段从大众点评获得点评信息用于充实自己的产品，具有明显的搭便车、不劳而获的特点，构成不正当竞争。	
3	淘宝诉美景公司不正当竞争纠纷	淘宝公司开发了的某衍生数据产品，该数据产品主要为淘宝、天猫商家的网店运营提供数据化参考服务、帮助商家提高经营水平。美景公司经营的“咕咕互助平台”以远程登录方式抓取该衍生数据产品中的数据内容并从中获利。	

版权所有 翻印必究

此外，也有极少的案件原告选择通过寻求著作权的保护以解决纠纷，例如上海汉涛信息咨询有限公司与北京搜狐互联网信息服务有限公司侵犯著作权纠纷一案。

根据《反不正当竞争法》第十二条的规定，经营者利用网络从事生产经营活动，应当遵守本法的各项规定。经营者不得利用技术手段，通过影响用户选择或者其他方式，实施下列妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为：（一）未经其他经营者同意，在其合法提供的网络产品或者服务中，插入链接、强制进行目标跳转；（二）误导、欺骗、强迫用户修改、关闭、卸载其他经营者合法提供的网络产品或者服务；（三）恶意对其他经营者合法提供的网络产品或者服务实施不兼容；（四）其他妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为。

因此，企业在设计新的商业模式时须考虑诸多因素，譬如该等商业模式是否可能导致违反前述规定而被认定为“经营者在生产经营活动中，违反本法规定，扰乱市场竞争秩序，损害其他经营者或者消费者的合法权益的行为”。此外，在与其他企业的合作中，公司也要注意多重授权的获得，以免被认定为采用不当手段进行不正当竞争。

2.1.3. 人身权类的侵权纠纷

中国是世界上最有活力的市场，因此中国的新商业模式很多都是与庞大的消费人群有关的 To C 业务。众所周知，To C 业务估值的一个重要指数是用户人数，因此个人信息也成为 To C 企业最有价值的数据类型之一。与个人信息相关的人身权类侵权纠纷主要涉及侵犯隐私权、名誉权，其中多数为企业未经授权使用用户个人信息、信息记录错误以及不当精准营销等情形，典型案例如下：

序号	典型案例	案情简要	植德合规建议
1	朱某诉北京百度网讯科技有限公司隐私权纠纷	百度网讯公司使用了 Cookie 技术记录和跟踪了原告所搜索的关键词，利用记录的关键词，对原告浏览的网页进行广告投放。原告起诉百度网讯公	（1） 该案件发生在《网络安全法》及相关法律、规范性文件颁布和生效之前，该案件中认定的 Cookie 的性质已经不具有参考意义。此

序号	典型案例	案情简要	植德合规建议
		司的行为侵犯了其隐私权。终审法院认为，该 Cookie 关键词记录未能与原告的个人身份对应识别，不符合“个人信息”的可识别性要求;且因为百度网讯公司利用网络技术提供个性化推荐服务，并未直接将搜索引擎服务而产生的数据和 Cookie 信息向第三方或公众展示，没有任何的公开行为，因而不属于侵害个人隐私的行为。	外，该案件的终审法院也不是最高院，因此不会对后续案件构成有约束力的先例。 （2） 根据目前的规定，企业应在网站或 App 的隐私政策中具体阐明 Cookie 技术的使用方式。
2	王某诉北京奇虎科技有限公司隐私权纠纷	王某使用手机给朋友沈某的号码为 136XXXXXXXX 的手机拨打电话时，在 360 手机卫士软件的“防窃听”模块下，显示该号码被标记为“维特网络信息有限公司（合肥分公司）浙江杭州移动”。法院判定“如非号码所有人主动申请标记，建议针对被标记号码采取短信确认的方式，对所有人有所提示，有助于其获得相应知情权”。	（1） 公司业务中如涉及个人信息，则需要时刻注意是否符合监管部门的要求。例如最近 App 专项治理工作组的《App 违法违规收集使用个人信息行为认定方法（征求意见稿）》等文件。 （2） App 收集个人信息和使用个人信息时要履行对用户的通知义务。
3	王某诉沈丘县农村信用合作联社名誉权纠	由于信用合作社对其工作人员管理不善，致使冒名贷款事件的发生，使王某在中国人民银行个人信息	由于金融机构掌握大量个人敏感信息，一旦泄漏或发生错误，可能对个人产生重大不利影响，故金融机构应

版权所有 翻印必究

序号	典型案例	案情简要	植德合规建议
	纷	数据库中产生不良信用记录。	妥善管理数据库，并在不良事件发生时尽快删除、改正相关信息。
4	庞某诉北京趣拿信息技术有限公司等隐私权纠纷	庞某在趣拿公司下辖网站“去哪儿网”购买东航机票，因此导致个人信息被泄露，庞某收到内容为声称原告航班取消的诈骗短信。法院判决东航和趣拿公司存在泄露庞某隐私信息的高度可能，并且存在过错，应当承担侵犯隐私权的相应侵权责任。	（1） 合同内容，用户姓名、电话号码及行程安排等事项属于个人信息，基于合理事由掌握个人整体信息的组织或个人应积极谨慎地采取有效措施防止信息泄露； （2） 如果经营者外包了涉及个人信息的业务，即便是第三方供应商泄露了用户的隐私信息，也首先由经营者承担责任。经营者在承担责任后可以依据其与第三方供应商之间的服务合同条款，在相关证据具备的情况下，向第三方供应商主张权利。
5	任某与北京百度网讯科技有限公司名誉权、姓名权、一般人格权纠纷	百度搜索任某，“相关搜索”栏中显示出任某曾经的职业，并对任某产生了不利影响。	（1） 本案涉及被遗忘权的概念，尽管该概念在学术界已有讨论，但我国现行法律中并无对“被遗忘权”的法律规定，亦无“被遗忘权”的权利类型。 （2） 在公安部第三研究

版权所有 翻印必究

序号	典型案例	案情简要	植德合规建议
			所发布的《App 违法违规收集使用个人信息行为认定方法（征求意见稿）》中，未提供更正、删除个人信息，注销用户账号的功能已经被认定为“未按法律规定提供删除或更正个人信息功能的情形”。
6	周某与中国保险监督管理委员会、北京中科汇联科技股份有限公司网络侵权责任纠纷	中国保监会也依法负有保护申请政府信息公开申请人信息安全的义务。该会网站因网络漏洞泄露了周某的个人注册信息。	（1） 根据《中华人民共和国侵权责任法》第三十六条，网络用户、网络服务提供者利用网络侵害他人民事权益的，应当承担侵权责任。网络用户利用网络服务实施侵权行为的，被侵权人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施…… （2） 即使是政府部门，亦负有法律义务保护数据安全。
7	赵某与纽海电子商务（上海）有限公司其他侵权责任纠纷	纽海电子经营的电商购物平台利用赵某在购物时留存的手机信息，给赵某手机发送商业短信。	（1） 如果企业合法取得用户个人信息并指示了取消发送商业短信的方式，且发送商业短信不过于多，则属于合理范围。

版权所有 翻印必究

序号	典型案例	案情简要	植德合规建议
			（2） 利用用户信息和算法定向推送新闻、广告等，且未提供终止定向推送的选项则属于被关注的风险业务。

2.1.4. 涉及个人信息案件统计分析

除了上述的典型案例外，以“个人信息”为关键词，我们从专业数据库上筛选了 2015 年 5 月 1 日至 2018 年 3 月 1 日期间涉及“个人信息”的 146 件民事案例，统计分析如下:

- ✓ 侵权纠纷案件 139 件(其中被认定存在侵权事实的案件数为 94 件)，合同纠纷案件共计 7 件;
- ✓ 涉案行业中金融行业和互联网行业居多，其他行业也有较快增长;
- ✓ 信息收集量大、使用比较频繁的领域涉诉风险较高;
- ✓ 涉案争议行为具体类型涵盖了个人信息收集、保存、使用等全生命周期的全流程;
- ✓ “个人信息记录错误” 、“未经同意使用个人信息” 以及“个人信息泄露”三类行为涉案数量最多;
- ✓ 不少案件反映的是对个人信息收集使用的商业模式的争议，典型的如朱烨诉百度收集 Cookie 侵犯隐私权的案件;
- ✓ 涉及个人信息违法收集、信息共享、遗忘权的案件也开始出现;
- ✓ 以庞理鹏诉去哪儿网、东航为标志，信息共享者共同担责，数据控制者对数据处理者的行为担责或成为趋势。

2.2. 行政处罚风险

2.2.1. 《网络安全法》项下的行政法律责任

《网络安全法》是网络安全和数据合规行政处罚最重要的依据。在此就《网络安全法》规定的行政责任简单梳理如下:

版权所有 翻印必究


网络安全法下的法律责任
网络运营者违反网络安保义务的责任
违反网络安全等级保护制度的要求
未制定网络安全事件应急预案
由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款
网络运营者为用户提供特定网络服务时，未履行核实用户真实身份信息义务
由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、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，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
网络运营者不按照有关部门的要求采取处置措施，拒绝、阻碍依法实施的监督检查的，拒不提供技术支持和协助的
由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，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
网络运营者、网络产品或者服务的提供者侵害个人信息权利
搜集用户信息未向用户明示并取得同意，违反遵守关法律、行政法规关于个人信息保护的规定
运营者未依个人合法请求采取措施删除或者更正其个人信息
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
网络产品服务的提供者、电子信息的发送者不法行为的责任
设置恶意程序
对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的
擅自终止为其产品、服务提供安全维护
由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款
关键信息基础设施的运营者违反网络安保义务的责任
违反设施性能保障及安全技术措施“三同时制度”（同步规划、同步建设、同步使用）
违反网络安全等级保护制度下的一般和特殊要求
采购网络产品和服务时，未按照规定与提供者签订安全保密协议。
未定期进行网络安全性风险评估和履行报告义务
有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款
关键信息基础设施的运营者使用未经安全审查或者安全审查未通过的网络产品或者服务
有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；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
关键信息基础设施的运营者在境外存储网络数据，或者向境外提供网络数据
由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，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；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
有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示
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
从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者帮助从事危害网络安全的活动，尚不构成犯罪的
单位
公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚
个人
公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。
受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作
未遵守国家有关规定开展网络安全认证、检测、风险评估等活动，或者向社会发布网络安全信息的
由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、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，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款
设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的
单位
由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚
个人
由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组
网络运营者对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的
电子信息发送服务、应用软件下载服务提供者未履行对用户安全管理义务
由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，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，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

2.2.2. 行政处罚典型案件

序号	事件名称及经过	行政处罚决定机关	违规行为	违规行为类型	行政措施	法律依据
1	山西忻州市某省直事业单位网站不履行网络安全保护义务被处罚 2017 年 6 月至 7 月间，山西忻州市某省直事业单位网站存在 SQL 注入漏洞，网站信息安全存在严重安全隐患，其连续被国家网络与信息安全信息通报中心通报，并被忻州市、县两级公安机关网安部门处以行政警告处罚并责令其改正。	忻州市、县两级公安机关网安部门	未按照网络安全等级保护制度的要求，采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施	违法网络安全义务	警告并责令其改正	《网络安全法》第 21 条、第 59 条
2	某求职网站被网信办责令整改 2017 年 8 月 11 日，北京市网信办、天津市网信办联合约谈了某求职网站法定代表人,并要	北京市网信办、天津市网信办	为未提供真实身份信息的用户提供信息发布服务；未采取有效措施对用户发布传输的	违法网络安全义务	责令改正	《网络安全法》第 24 条、61 条、47 条、68 条

版权所有 翻印必究

序号	事件名称及经过	行政处罚决定机关	违规行为	违规行为类型	行政措施	法律依据
	求该网站整改网站招聘信息。		信息进行严格管理，导致违法违规信息扩散			
3	汕头某公司未及时履行网络安全义务，网警依据网安法责令改正 汕头市某信息系统安全等级为第三级的信息科技有限公司自 2016 年至今未按规定定期开展等级测评。	广东汕头网警支队	未按规定履行网络安全等级测评义务	违法网络安全义务	警告并责令其改正	《信息安全等级保护管理办法》第 14 条第 1 款和《网络安全法》第 21 条第（5）以及《网络安全法》第 59 条
4	重庆某网络公司未留存用户登录日志被网安查处 自《网络安全法》正式实施以来，重庆市某科技发展有限公司在提供互联网数据中心服务时，未依法留存用户登录相关网络日志。	重庆公安局网安总队	未依法留存用户登录相关网络日志	违法网络安全义务	警告并责令其改正	《网络安全法》第 21、第 59 条

版权所有 翻印必究

序号	事件名称及经过	行政处罚决定机关	违规行为	违规行为类型	行政措施	法律依据
5	四川某网站因高危漏洞遭入侵被罚 2017 年 7 月 22 日，四川宜宾市某网站因未将网络安全防护工作落实到位，进而导致网站存在高危漏洞，最终造成了网站发生被黑客攻击入侵的网络安全事件。	宜宾网安部门	未落实网络安全等级保护制度，未履行网络安全保护义务	违法网络安全义务	对直接负责的主管人员罚款 5 千，机构罚款 1 万元	《网络安全法》第 21 条、第 59 条
6	三家互联网公司因用户隐私问题被工信部约谈 2018 年 1 月，工信部信息通信管理局针对手机软件对用户个人信息收集使用规则、使用目的告知不充分的情况，约谈了该三家互联网企业，要求三家企业本着充分保障用户知情权和选择权	工信部信息通信管理局	用户个人信息收集使用规则、使用目的告知不充分	侵犯公民个人信息	约谈并要求整改。	《网络安全法》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《电信和互联网用户个人信息保护规定》（工业和信息化部令第 24 号）有

版权所有 翻印必究

序号	事件名称及经过	行政处罚决定机关	违规行为	违规行为类型	行政措施	法律依据
	的原则进行整改。					关规定
7	某应用程序非法共享热点被罚 25 万 2018 年 5 月 22 日，根据媒体反映，对两款移动应用程序，工信部针组织了网络安全专业机构进行技术分析，发现两款移动应用程序具有共享用户所登录 WiFi 网络密码等信息的功能，最终对其给予了处罚。	上海市通信管理局	未经同意共享用户 WiFi 网络密码等信息	侵犯公民个人信息	责令改正、罚款	《网络安全法》第 41 条
8	多家平台自媒体平台存在内容违法违规，涉嫌抄袭等问题被集中约谈整改 北京市网信办于 2017 年 7 月 18 日依法约谈了多家自媒体网站的相关负责人，责令网站	北京市网信办	违法违规，涉嫌抄袭等	违反网络信息内容管理义务	约谈并责任改正	《网络安全法》第 48 条、第 50 条

版权所有 翻印必究

序号	事件名称及经过	行政处罚决定机关	违规行为	违规行为类型	行政措施	法律依据
	立即对自媒体平台存在八个问题进行专项清理整治。					
9	某知名社交平台和某知名网络社区平台因对网络信息内容未尽到管理义务被北京市网信办行政处罚 2017 年 9 月，针对某知名社交平台对其用户发布传播“淫秽色情信息、宣扬民族仇恨信息及相关评论信息”未尽到管理义务以及某知名网络社区平台对其用户发布传播“淫秽色情信息、暴力恐怖信息帖文及相关评论信息”未尽到管理义务的违法行为，北京市网信办分别作出行政	北京市网信办	未采取有效措施对用户发布传输的信息进行严格管理,导致违法违规信息扩散。	违反网络信息内容管理义务	罚款、责令改正	《网络安全法》47 条、68 条

版权所有 翻印必究

序号	事件名称及经过	行政处罚决定机关	违规行为	违规行为类型	行政措施	法律依据
	处罚。					
10	某网络媒体平台因对网络信息内容未尽到管理义务被行政处罚 2017 年 9 月，广州某网络技术有限公司在发现有用户利用其网络平台发布和传播违法有害信息后，未立即停止传输，防止信息扩散，保存有关记录并向主管部门报告。后广东省通信管理局责令该公司立即整改，并给予警告处罚，要求该公司切实落实信息服务管理责任。	广东省通信管理局	未采取有效措施对用户发布传输的信息进行严格管理,导致违法违规信息扩散。	违反网络信息内容管理义务	警告并责令其改正	《网络安全法》第 47 条、第 68 条，《互联网信息服务管理办法》第 16 条、第 23 条
11	某两家新闻客户端涉低俗信息被责令停止违法违规行为 2017 年 12 月，某两家新闻客	北京市网信办	传播违法违规有害信息、违规自采转载新闻信息	违反网络信息内容管理义务	约谈并停止违规转载新闻信	《网络安全法》第 48 条、第 50 条

版权所有 翻印必究

序号	事件名称及经过	行政处罚决定机关	违规行为	违规行为类型	行政措施	法律依据
	户端客户传播色情低俗信息，且获得转载。北京市网信办责令两家企业深入自查自纠。					
12	某社交平台未尽到义务，某业务版块暂时下线一周 2018 年 1 月，某社交平台因未对用户发布违法违规信息尽到审查义务，并传播了违法违规信息，被北京市网信办约谈，责令其立即自查自纠，全面深入整改。	北京市网信办	对用户发布违法违规信息未尽到审查义务，传播违法违规有害信息	违反网络信息内容管理义务	约谈并责令改正	《网络安全法》第 47 条、第 68 条第 48 条、第 50 条
13	某公众号发低俗文章被责令整改 2018 年 5 月，某公众号在其头条推文发布了低俗文章，同时对事件进行了不当的描述，后浙江省网信办	浙江省网信办、杭州市网信办	传播违法违规有害信息	违反网络信息内容管理义务	约谈并责令改正	《网络安全法》第 48 条、第 50 条

版权所有 翻印必究

序号	事件名称及经过	行政处罚决定机关	违规行为	违规行为类型	行政措施	法律依据
	会同杭州市网信办约谈了该公众号主要负责人，并责令限期整改。					
14	北京市网信办、工商局针对广告存在侮辱英烈的内容约谈查处某知名短视频平台及知名搜索引擎并责令整改 2018 年 6 月，针对某知名短视频平台在某知名搜索引擎投放的广告中出现侮辱英烈内容的问题，北京市网信办、市工商局依法联合对两者约谈查处，责令整改。	北京市网信办、市工商局	制作、发布内容违法的广告	违反网络信息内容管理义务	约谈并责令整改	《网络安全法》第 12 条、第 47 条《中华人民共和国英雄烈士保护法》第 22 条、《中华人民共和国广告法》第 9 条

版权所有 翻印必究

2.3. 刑事处罚的风险

涉及网络或者数据的业务，还须关注网络安全、数据合规以及隐私保护等方面的刑事违法风险。企业数字化转型过程中运用新的数字技术或者商业模式超过合理的边界，有可能会导致公司、公司实际控制人或者员工承担刑事责任，相关案例屡见不鲜。司法实践中，与网络安全、数据合规相关的刑事罪名主要如下。

2.3.1. 计算机系统安全类罪名

具体包括：非法侵入计算机信息系统罪，破坏计算机信息系统罪，非法获取计算机信息系统数据罪，非法控制计算机信息系统罪和提供侵入、非法控制计算机信息系统程序、工具罪。

大数据时代，数据的存储、处理、应用离不开计算机系统构成的网络环境，商业模式先天缺陷或者实际操作的不合规很容易导致构成前述罪名。典型的案例有：

序号	罪名	典型案例	案情简要	植德合规建议
1	非法获取计算机信息系统数据罪	北京某科技股份有限公司（新三板公司）	该公司利用自主编写的恶意程序，劫持运营商流量，并通过清洗、还原等技术，从中窃取Cookie、访问记录等信息30亿条，将该数据导出存放在该公司境内外的多个服务器上。 该公司已被停牌，公司监事黄某、梁某、员工王某、石某已于2018年8月被检察院批捕，原法人、董事周某取保候审。	进行软件开发时需注意产品逻辑是否合规，不得开发破坏其他产品的正常功能、运行逻辑及相关秩序的软件，不得利用技术手段非法获取数据。
2	提供侵入、非法控制计算机信息系统程序、工具罪	辜某、资某等提供侵入、非法控制计算机信息系统程序、工具罪	辜某注册成立并担任法定代表人的成都某科技有限公司，开发具	

版权所有 翻印必究

序号	罪名	典型案例	案情简要	植德合规建议
		一案	有在某电商平台网站中可批量注册账户，并对不同账户在短时间内实现批量下单、批量抢领电商给予常规客户的优惠券和红包、批量付款等功能的计算机软件，并通过网络进行软件出售牟利。 法院认为，针对某电商平台网站的软件的研发、使用，未获得该电商平台的许可。辜某及其雇用的人员构成提供侵入、非法控制计算机信息系统程序、工具罪。	
3	破坏计算机信息系统罪	湖南某网络科技有限公司	该公司为牟取非法利益，开发运行用于非法核验身份的“VTOOL”软件，绕过铁路身份证识别仪,在铁路售票系统上对铁路购票网站存储冻结的	

版权所有 翻印必究

序号	罪名	典型案例	案情简要	植德合规建议
			1295365 条旅客身份信息数据，由“需线下核验—不能网上购票”修改为“正常—可以网上购票”，破坏了铁路售票秩序。 法院认为该公司的行为构成破坏计算机信息系统罪。	
4	非法获取计算机信息系统数据罪	上海某网络科技有限公司	被告人张某、宋某、侯某经共谋采用技术手段抓取被害单位北京某网络技术有限公司服务器中存储的视频数据，并破解北京某网络技术有限公司的防抓取措施，使用“tt_spider”文件实施视频数据抓取行为。 法院认为该公司及直接负责的主管人员和其他直接责任人员犯非法获取计算机信息系统数据罪。	利用爬虫技术须谨慎，避免抓取 Robots 协议中明确禁止抓取的数据及他人服务器中的数据。
5	非法侵入计算	四川某汽车服务	钟某经营的该汽	进入计算机信息系

版权所有 翻印必究

序号	罪名	典型案例	案情简要	植德合规建议
	机信息系统罪	有限公司	车服务有限公司，通过交警黄某管理的执法终端设备查询车辆和驾驶人违章信息二万余次，并以几名交警的警号和密码侵入公安交警警务云平台共计 24**余次。 法院认为被告单位、钟某均已构成非法侵入计算机信息系统罪。	统必须按照正规途径获得相关账号和相应权限，避免私自登陆他人已获得授权的账号。
6	非法控制计算机信息系统罪	羊某犯非法控制计算机信息系统罪一案	羊某向楚某等人收购“webshell”（网站控制权限），后羊某使用黑客工具及收购的“webshell”非法侵入被控制网站 69 个，并向被控制的网站服务器上传广告网页，将广告网页链接指向羊某搭建的网站，羊某利用该网站谋取非法利益。 法院认为被告人羊某犯非法控制	拒绝使用黑客工具，不得对他人发起网络攻击。

版权所有 翻印必究

序号	罪名	典型案例	案情简要	植德合规建议
			计算机信息系统罪。	
7	破坏计算机信息系统罪	成都某安全技术有限公司	该公司及其直接负责的主管人员雇佣黑客对其竞争对手公司的网络游戏计算机信息系统功能进行干扰。 法院认为该公司行为已构成破坏计算机信息系统罪。	通过正常的市场竞争机制进行竞争，不得对竞争对手等实施网络攻击等违法犯罪手段。

2.3.2. 侵犯公民个人信息罪

个人信息一方面是大数据时代企业的重要资源，另外一方面也涉及每个人的隐私，不当的商业模式或者操作将可能导致企业被认定侵犯公民个人信息罪。最高人民法院、最高人民检察院和公安部都曾陆续发布过与此相关的典型案例，我们选取其中具有代表性的案例分享如下:

序号	发布单位/督办单位	案件名称	案情简要
1	公安部、最高人民检察院督办	某新三板公司买卖数据案	该公司人员从某经贸有限公司购入涉案数据，此后将经过清洗和处理的数据卖给其他公司。该公司多名股东都曾接受过调查，最终包括首席运营官、平台资源部总监等在内的 6 名员工被诉。
2	最高人民法院(2017-05-09)	邵某等侵犯公民个人信息案	非法出售户籍信息、手机定位、住宿记录等个人信息，构成侵

版权所有 翻印必究

序号	发布单位/督办单位	案件名称	案情简要
			犯公民个人信息罪。
3	最高人民法院 (2017-05-09)	韩某、旷某、韩某等侵犯公民个人信息案	非法查询征信信息牟利，构成侵犯公民个人信息罪。
4	最高人民法院 (2017-05-09)	丁某侵犯公民个人信息案	非法提供近二千万条住宿记录供他人查询牟利，构成侵犯公民个人信息罪“情节特别严重”。
5	最高人民检察院 (2017-05-16)	郭某某侵犯公民个人信息案	将在提供服务过程中获得的公民个人信息出售、提供给他人，构成侵犯公民个人信息罪。
6	最高人民检察院 (2017-05-16)	鲁某等侵犯公民个人信息案	单位实施侵犯公民个人信息犯罪，依法追究单位和相关责任人员的刑事责任。
7	公安部 (2016-07-20)	江苏淮安侦破陈某某等人侵犯公民个人信息案	利用互联网大肆倒卖车主、车牌号、车辆类型等公民个人信息。
8	公安部 (2016-07-20)	湖北襄阳侦破郑某某等人侵犯公民个人信息案	利用其短信营销平台，不断获取客户上传信息，贩卖公民个人信息。
9	公安部 (2016-07-20)	湖北荆门侦破李某某等人侵犯公民个人信息案	贩卖利用在某证券公司上班时的便利获得的以及使用软件和论坛下载保存下来的大量各类公民个人信息。
10	公安部 (2016-07-20)	上海侦破吴某、刘某某等人非法获取公民个人信息案	通过快递公司的内部系统员工账号，下载和大量购买个人信息出售牟利。
11	公安部 (2016-12-17)	北京顾某等人非法获取计算机信息系统数据案	制作用于非法获取该公司账号的软件程序，并在互联网上大肆收购网站身份认证信息，使

序号	发布单位/督办单位	案件名称	案情简要
			用软件大量实施“撞库”行为，非法获取该公民个人账号约 10 万组。
12	公安部 (2016-12-17)	江苏淮安某社工库侵犯公民个人信息案	该网络社工库涉及公民个人信息 20 亿条，已被主管机关封查。
13	公安部 (2016-12-17)	福建泉州某网站侵犯公民个人信息案	该网站买卖公民个人信息，被主管机关封查。
14	公安部 (2016-12-17)	江苏徐州某非法获取计算机信息系统数据案	以黑客和快递公司内部员工为泄露源头倒卖快递信息。
15	公安部 (2016-12-17)	山东威海董某某侵犯公民个人信息案	非法查询公民个人银行账户余额、流水等信息进行出售。
16	公安部 (2016-12-17)	内蒙古赤峰李某某侵犯公民个人信息案	利用“快递单号生成器”等软件筛选快递单号，通过快递公司内部人员查询对应的公民个人信息出售获利。
17	公安部 (2016-12-17)	湖南怀化某侵犯公民个人信息案	在网上购买、搜索、下载等方式大量搜集公民个人信息，再通过“撞库”、“扫存”等非法软件比对公民网络账户密码，进行出售和“刷单”赢利。

2.3.3. 侵犯著作权罪

如果被侵犯的他人服务器中的数据属于著作权法意义上的作品的，则还可能构成侵犯著作权罪。典型案例如下:

序号	典型案例	案情简要	法院观点
1	薛某、潘某非法获取计算机信息系统数据、非法控制计算机信息系统	薛某、潘某等经共谋，侵入他人计算机窃取游戏的源代码，	被告人薛某与被告人潘某等人经共谋，以营利为目的，未经著作权人

	罪、侵犯著作权罪一案	破解游戏源代码密码后，租赁服务器、搭建“私服”游戏平台、充当“私服”客服进行经营谋利。	许可，复制发行非法获取的计算机信息系统数据，非法经营数额达120000余元，属于“有其他严重情节”，其行为均构成侵犯著作权罪。
2	邱某侵犯著作权罪一案	邱某私自取得某公司开发的棋牌游戏的源代码，并先后成立另外两家公司，对该棋牌游戏进行换皮、加工、更名等形式的修改，并进行运营。	被告人邱某未经著作权人许可，以营利为目的，以其窃取的源代码为基础，通过复制原程序的原始数据，以换皮、加工等形式制作成另外一款棋牌游戏并上线运营，符合《中华人民共和国刑法》（下称“《刑法》”）第二百一十七条所规定的侵犯著作权罪的“复制发行”要求。

2.3.4. 诈骗罪、非法经营罪

数字化转型过程中，如果对于新的概念、商业模式、利用方式没有合规审查，有可能认定实质上非法占有他人财产从而构成诈骗罪或者非法经营罪。典型案例如下：

序号	典型案例	案情简要	法院观点
1	深圳某网络科技有限公司、廖某某等数据刷量诈骗案	2016年4月至7月间，被告单位与被害单位签订了手机应用软件委托推广合同，约定由被告单位为被害单位	法院认为各被告单位、被告人均构成合同诈骗罪。首先，从犯罪构成客观行为的角度上看，被告单位和重庆某科技公司通过虚

版权所有 翻印必究

		开发的三款手机应用软件提供推广服务，并以下载量作为计费依据。被告人廖某在代表公司履行上述合同的过程中，指使重庆某科技有限公司商务部员工被告人杨某，利用手机群控软件模拟真实用户，虚增三款手机应用软件下载量，骗取被害单位推广费用共计人民币 1200 余万元。	增假量的受害单位推广费用，虚增的假量根本无法实现合同目的，致使被害单位直接遭受了经济损失。其次，从犯罪构成的主观方面看，各被告主观上均具有非法占有他人钱款的故意，且形成了共同犯罪的合意。最后，从社会危害性的角度看，网络推广合作模式与传统经济合作模式不同，由于互联网的虚拟性，很难对合同的履行情况进行有效监控。无法苛求被害单位单位能够像侦查机关一样调取到证明被告单位“刷量”的证据，其合法权益很难通过协商或民事途径予以充分保障。综上，无论从形式上还是实质上，本案均应认定构成合同诈骗罪。
2	李某某犯非法经营罪一案	李某某通过创建某网站和利用某语音聊天工具建立刷单炒信平台，吸纳淘宝卖家注册账户成为会员，并收取会员费。通过制定刷单炒信规则与流程，组织及协助会员通过该平台发布或接受刷单炒信任务。	被告人李某某违反国家规定，以营利为目的，明知是虚假的信息仍通过网络有偿提供发布信息等服务，扰乱市场秩序，情节特别严重，其行为已构成非法经营罪。

版权所有 翻印必究

2.3.5. 拒不履行网络安全管理义务罪

《刑法》第二百八十六条之一规定，网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：（一）致使违法信息大量传播的；（二）致使用户信息泄露，造成严重后果的；（三）致使刑事案件证据灭失，情节严重的；（四）有其他严重情节的。单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。拒不履行网络安全管理义务罪惩罚的是公司在网络安全与数据合规方面的不作为。

任何一个网络服务提供者应当履行信息网络安全管理义务，如果不履行且经责令改正而拒不改正，在发生特定不利后果的情形下，该行为已经从行政违法转变为刑事犯罪。典型案例如下：

序号	典型案例	案情简要	法院观点
1	胡某拒不履行信息网络安全管理义务案	胡某为非法牟利，租用国内、国外服务器，自行制作并出租某翻墙软件，为境内网络用户非法提供境外互联网接入服务。2016 年 10 月，上海市公安局浦东分局作出责令停止联网、警告、并处罚款以及没收违法所得的行政处罚。被告人胡某拒不改正继续出租该翻墙软件。	法院认为，被告人胡某非法提供国际联网代理服务，拒不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施后拒不改正，情节严重，其行为已构成拒不履行信息网络安全管理义务罪。

3. 谁需要考虑数字化转型中的合规风险

3.1. 绝大多数企业均须考虑网络安全和数据合规

市场上有一种错误的理解，即只有互联网公司才应当关注网络安全、数据合规的风险。

版权所有 翻印必究

其实不然，根据我们的理解，任何一个公司如果其业务涉及《网络安全法》中规定的“网络”、“网络安全”、“网络运营者”以及“网络数据”，都很有可能落入《网络安全法》的管辖范围。

根据《网络安全法》，前述词汇的定义分别如下:

- ✓ 网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

值得注意的是，除了计算机之外，便携式笔记本电脑、Ipad、IOT 设备、智能汽车、智能家居等任何可以发送、接受信息的设备都可能构成网安法下的信息终端。

- ✓ 网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。
- ✓ 不当的商业模式，无论其外在形式表现如何，如果事实上作为攻方突破了守方的网络安全措施，使得对方网络无法处于稳定可靠运行状态或者侵害了对方数据的完整性、保密性、可用性，将在很大可能上构成破坏网络安全的行为。
- ✓ 网络运营者，是指网络的所有者、管理者和网络服务提供者。
- ✓ 网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

在互联网时代，计算机或网络是所有企业都在使用的必要设备，且大量企业都在对客户数据进行搜集、储存或处理。因此，不难推测几乎绝大部分的境内机构都将不可避免的适用《网络安全法》。

3.2. 是否可以通过注册一个境外公司来规避中国法下的合规风险?

某些具有国际视野的企业家经常问的一个问题就是，是否可以通过注册一个境外公司来规避中国法下的合规风险？简单回答是：不能。

根据《网络安全法》第二条，在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。虽然《网络安全法》规制的是境内网络活动，但是我们不能简单的认为《网络安全法》只适用于在中华人民共和国大陆地区注册的公司。事实上，中国政府一直强调要从网络主权高度来看网络安全，没有网络安全就没有

版权所有 翻印必究

国家安全，且考虑到互联网自身的无国界性的特点，《网络安全法》影响范围必然不仅仅适用于在中国大陆注册的公司。

综合考虑目前现有的规范和法律实践，如下的一些企业都是应当关注《网络安全法》的：在中国境内注册的网络运营者，以及未在中国境内注册，但在中国境内开展业务，或向中国境内提供产品或服务的网络经营者。如果一个境外公司的经营中有如下一个或全部因素，那么该境外公司将很有可能被认定在中国境内开展业务，或向中国境内提供产品或服务：（1）网站使用中文；（2）以人民币作为结算货币；（3）向中国境内配送物流等。中华人民共和国境内的网络运营者仅向境外机构、组织或个人开展业务、提供商品或服务，且不涉及境内公民个人信息和重要数据的，不视为境内运营。

换句话说，通过设立境外公司这样简单粗暴的方案不可能从实质上规避违法的风险。

3.3. 关键信息基础设施运营者的特殊义务

《网络安全法》第三十一条明确规定了关键信息基础设施(Critical Information Infrastructure，下称“CII”)保护制度。 关键信息基础设施运营者（下称“CIIO”）较之一般的主体又负有更高的义务。

3.3.1. 关键信息基础设施范围的一般界定

根据《关键信息基础设施安全保护条例（征求意见稿）》，下列单位运行、管理的网络设施和信息系统应当纳入保护范围：

- ✓ 公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域；
- ✓ 其它一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施；
- ✓ 卫生医疗、教育、社保、环境保护；
- ✓ 云计算、大数据和其他大型公共信息网络服务的单位；
- ✓ 国防科工、大型装备、化工、食品药品等行业领域科研生产单位。

3.3.2. 关键信息基础设施范围的特别界定

版权所有 翻印必究

值得注意的是，根据《关键信息基础设施安全保护条例（征求意见稿）》，任何未被明确列举的行业和领域的主体所运营的网络设施和信息系统只要符合重要性认定，均有可能被认定为 CII。

网信办编制的《国家网络安全检查操作指南》进一步规定了确定 CII 的三个步骤:

a) 确定关键业务;
b) 确定支撑关键业务的信息系统或工业控制系统;
c) 根据关键业务对信息系统或工业控制系统的依赖程度,以及信息系统发生网络安全事件后可能造成的损失认定 CII。

可见，在特别界定 CII 范围的语境下，关键业务是重中之重。如何判断某项业务是关键业务呢？《国家网络安全检查操作指南》中的 CII 业务判定表（参见附件一）是判断某项业务是否是关键业务的重要指引。

对信息系统或工业控制系统，应根据本地区、本部门、本行业实际，参照具体标准认定 CII。以平台类为例，符合以下条件之一的，可认定为 CII:

- ✓ 注册用户数超过 1000 万，或活跃（每日至少登陆一次）用户数超过 100 万;
- ✓ 日均成交订单额或交易额超过 1000 万元;
- ✓ 一旦发生网络安全事故，可能造成以下影响之一的：造成 1000 万元以上的直接经济损失；直接影响超过 1000 万人工作、生活；造成超过 100 万人个人信息泄露；造成大量机构、企业敏感信息泄露；造成大量地理、人口、资源等国家基础数据泄露；严重损害社会和经济秩序，或危害国家安全；其他应该认定为关键信息基础设施的情形。

3.3.3. 关键信息基础设施运营者的保护义务

《网络安全法》规定：CIIO 对 CII 在网络安全等级保护制度的基础上进行特殊保护，CIIO 及网络安全关键岗位专业技术人员实行执证上岗制度，企业应设置安全管理负责人，CIIO 对建立 CII 安全检测评估制度等也具有相应义务。

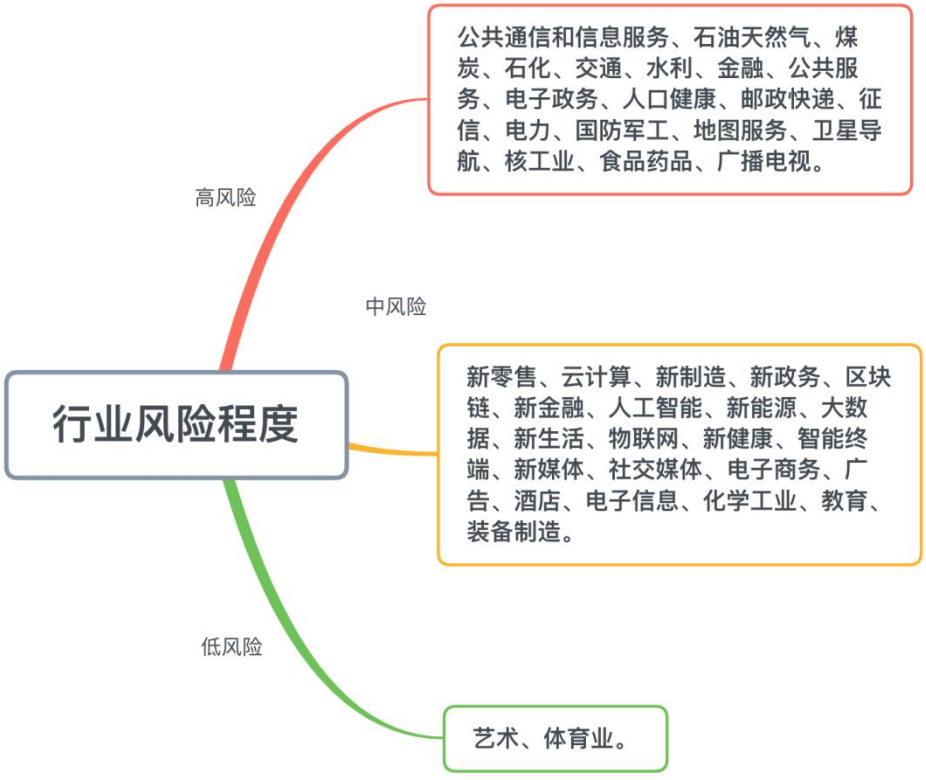
版权所有 翻印必究

此外，《关键信息基础设施安全保护条例（征求意见稿）》规定，CIIO 采购网络产品和服务，可能影响国家安全的（例如金融、电信、能源等重点行业领域），应当按照网络产品和服务安全审查办法的要求通过网络安全审查，并与提供者签订安全保密协议。

3.4. 不同行业对应不同的合规风险

任何一个行业如果涉及个人信息或者与国家安全、经济发展以及公共利益密切相关的数据，都应该格外关注网络安全、数据合规的风险。

为了方便大家简单直接的了解相关行业网络安全、数据合规的风险程度高低，我们制作了下述行业风险程度一览表。其中红色的为风险程度最高，黄色为须重点关注风险，绿色为风险程度相对较低。



3.5. 即便是网络事件的受害者也可能因忽略合规而遭受处罚

如果某个公司遭遇网络事件（例如网络攻击）后不能证明其已经履行信息网络安全管理义务，那么其作为网络攻击的受害者还可能被行政处罚甚至被刑事处罚。

据法制网报道，从 2018 年开始，公安机关已实行“一案双查”制度，即在对网络违法犯罪案件开展侦查调查工作时，同步启动对涉案网络服务提供者法定网络安全义务履行情况的监督检查。对拒不履行法定网

络安全义务、为网络违法犯罪活动提供帮助的网络服务提供者，公安机关将依法对其进行严厉查处，努力从源头遏制网络违法犯罪案件发生。

根据《网络安全法》的规定，网络运营者不履行制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入，发生危害网络安全事件时未及时启动应急预案并采取补救措施等网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

更为严重的是，企业还有可能构成拒不履行信息网络安全管理义务罪。根据《刑法》第二百八十六条之一的规定，网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：（一）致使违法信息大量传播的；（二）致使用户信息泄露，造成严重后果的；（三）致使刑事案件证据灭失，情节严重的；（四） 有其他严重情节的。单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。

3.6. 股东、高管的个人责任

3.6.1. 股东、高管的行政责任

《网络安全法》的“法律责任部分”对于违反该法的各个行为，都规定了网络安全的主管机关有权对“直接负责的主管人员”处以罚款、取消网络安全管理和网络运营关键岗位任职资格等处罚。不仅如此，对于某些特殊行业，行业主管部门也会对违反网络安全和数据保护的主管人员采取一定的措施，比如建议银行业金融机构对直接负责的高级管理人员和其他直接责任人员依法给予处分。

3.6.2. 股东、高管的刑事责任

根据《刑法》第三十一条的规定，单位犯罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员判处刑罚。在公司构成单位犯罪的情况下，直接负责的股东、高管也会判处相应的刑罚。在单位不构成犯罪的情况下，股东、高管可能构成个人犯罪。

需要特别引起注意的是财务投资人的责任问题。一般而言，财务投资人不直接参与公司的经营管理，因公司的违法犯罪行为受牵连的

版权所有 翻印必究

风险相对较小。但财务投资人在某些特定场景下仍有受到刑事处罚的风险。例如，在李某等 18 人合同诈骗罪一案中，李某等人成立某信息公司，并利用该信息公司从事售卖网络域名的合同诈骗活动。此后，被告人张某通过受让股权的方式入股该公司，同时兼任该公司的财务总监。张某辩称，其为财务投资人，并不参与公司管理，仅为该公司财务工作提供策划和咨询，不了解公司的实际业务模式。但法院最终认定，张某在入股某公司后，得知该公司从事合同诈骗行为，仍然从事上述相关工作。据此认为，张某构成合同诈骗罪。因此，对于私募基金等财务投资人，如果投资前不做好尽职调查、在投资后不做好投后管理的风控，那么在投资组合的业务模式涉嫌犯罪的情况下也有可能被牵涉其中。

4. 如何做好合规准备

4.1. 了解我国网络安全和数据合规的法律体系

了解我国网络安全和数据合规相关的法律体系是进行网络安全和数据合规建设的起点。网络安全和数据合规还是一个相对较新的领域，目前我国的相关法律规范呈现出如下特点:

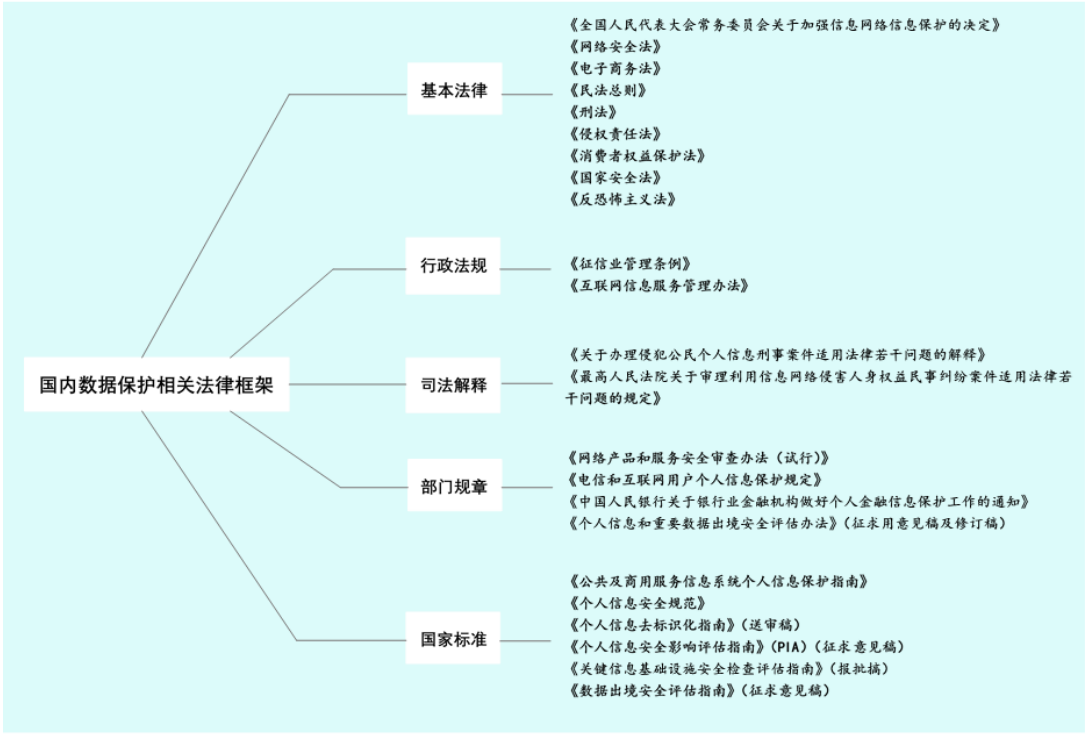
（1）目前我国网络安全和数据合规相关的法律规范众多，主要涉及五类规范（法律框架结构和典型规范列举详见下表），而且低效力位阶的规范众多。

（2）相关法律制度正在进一步完善的过程中，尤其是《网络安全法》的出台，意味着有一部综合性的法律在规制这个领域的问题，而且后续很多相关立法都会关注到网络安全和数据合规的内容;

（3）这个领域的立法技术尚未成熟，立法空白、规范繁杂零散、不一致甚至冲突等问题在短期内将持续存在，也会给合规工作带来不少困难和挑战。以医疗数据行业为例，据不完全统计相关的法规有 47 个之多。

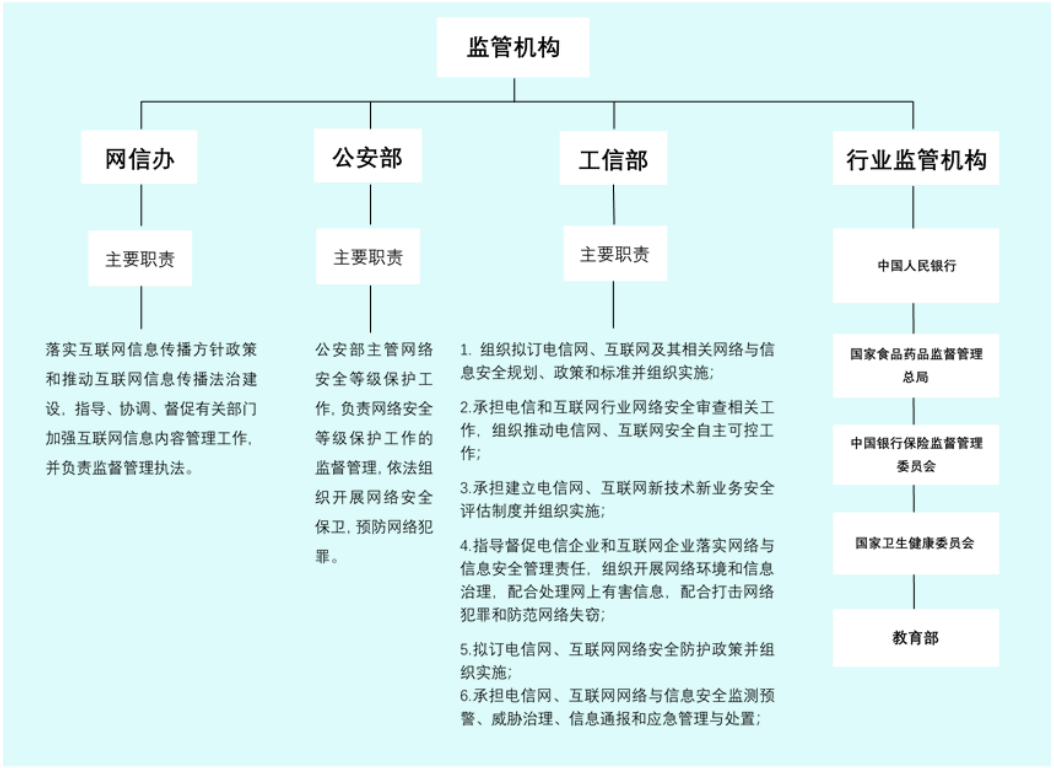
（4）国家标准、行业规范等软法将成为合规工作的重要依据。

版权所有 翻印必究



4.2. 主要监管机构

对于一个受到高度监管的领域而言，除了需要对法规做到充分理解外，进行合规建设的另一个重要方面就是应当了解监管机构。



4.2.1. 国家互联网信息办公室（下称“网信办”）

网信办是网络安全与信息合规最重要的监管机构。

网信办主导进行了一系列专项行动，例如 2019 年 1 月正式启动的网络生态治理专项行动，以及集中开展 APP 乱象专项整治行动。

网信办的主要职责是落实互联网信息传播方针政策和推动互联网信息传播法制建设，指导、协调、督促有关部门加强互联网信息内容管理工作，并负责监督管理执法。

4.2.2. 公安部

公安部主管网络安全等级保护工作，负责网络安全等级保护工作的监督管理，依法组织开展网络安全保卫，预防网络犯罪。

公安部 2018 年 4 月 9 日开展“净网 2018”专项行动，并将接续开展“净网 2019”专项行动，强化清理整治网络敲诈勒索、骚扰和网络水军，全面规范网络安全秩序，加强信息治理和网络治理能力。

2018 年 11 月 31 日，公安部网络安全保卫局发布了《互联网个人信息安全保护指引（征求意见稿）》，指导互联网企业建立健全公民个人信息安全保护的管理制度和技术措施，为《网络安全法》的落实和切实解决复杂网络环境中的现实问题提供了可行的解决方法和制度设计。

4.2.3. 工业和信息化部（下称“工信部”）

工信部也是网络安全、数据合规的重要监管部门。工信部的网络安全管理局下设综合处、信息安全处、网络与数据安全处以及重要通信处。

网络安全管理局的部分职责如下：

- ✓ 组织拟订电信网、互联网及其相关网络与信息安全规划、政策和标准并组织实施；
- ✓ 承担电信和互联网行业网络安全审查相关工作，组织推动电信网、互联网安全自主可控工作；
- ✓ 承担建立电信网、互联网新技术新业务安全评估制度并组织实施；
- ✓ 指导督促电信企业和互联网企业落实网络与信息安全管理责任，组织开展网络环境和信息治理，配合处理网上有害信息，配合打击网络犯罪和防范网络失窃；

版权所有 翻印必究

- ✓ 拟订电信网、互联网网络安全防护政策并组织实施;
- ✓ 承担电信网、互联网网络与信息安全监测预警、威胁治理、信息通报和应急管理与处置;
- ✓ 承担电信网、互联网网络数据和用户信息安全保护管理工作。

4.2.4. 行业监管机构

《网络安全法》明确指出国家网信部门负责统筹协调网络安全工作，相关行业部门负责网络安全保护和监督管理工作。各行业监管机构在《网络安全法》的框架下对本行业的网络安全践行安全建设，进行合规监管。以下列行业监管部门为例:

中国人民银行: 负责监督管理银行计算机网络安全、跨境金融网络信息服务、征信信息安全，开展网络安全专项检查，保护金融消费者个人信息。

国家食品药品监督管理总局: 负责监督管理医疗器械网络销售和网络交易服务。

中国银行保险监督管理委员会: 负责监督管理自媒体保险营销宣传和保险销售，维护保险消费者的合法权益。

国家卫生健康委员会: 负责监督全国健康医疗大数据的标准管理、安全管理和服务管理工作。

教育部: 加强教育信息化和网络安全统筹部署，规范教育信息化标准化管理，提升网络安全人才支撑和保障能力。

4.3. 区分不同的数据类型

在企业数字化转型过程中涉及的数据纷繁复杂。不同类型的数据类型对应不同的合规要求和法律风险，因此区分不同的数据类型对于企业数字化转型的风险控制至关重要。

4.3.1. 个人信息

《网络安全法》第七十六条（五）对于个人信息的定义为，以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。个人信息还包括

版权所有 翻印必究

通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

4.3.2. 个人敏感信息

2018年5月1日全国信息安全标准化技术委员会(下称“信安标委”)实施的《信息安全技术 个人信息安全规范》(GB/T 35273—2017,下称“《个人信息安全规范》”)在此基础上进一步界定了“个人敏感信息”的内涵和外延。2019年2月1日发布的《信息安全技术 个人信息安全规范(草案)》(下称“《个人信息安全规范草案》”)对《个人信息安全规范》中个人敏感信息的表述做了微调。

个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。通常情况下,14岁以下(含)儿童的个人信息和自然人的隐私信息属于个人敏感信息。

对于敏感信息,企业应当承担更多的合规责任,譬如,收集个人敏感信息时,应取得个人信息主体的明示同意。应确保个人信息主体的明示同意是其在完全知情的基础上自愿给出的、具体的、清晰明确的愿望表示。因此,企业在数字化转型过程中应当就业务中是否涉及敏感信息、敏感信息的收集程序、敏感信息的传输、存储、共享和转让等流程均有针对性的合规方案设计。

4.3.3. 重要数据

重要数据的定义,首次出现在《个人信息和重要数据出境安全评估办法(征求意见稿)》中,其后国标《信息安全技术数据出境安全评估指南(征求意见稿)》以规范性附录的方式对重要数据作出界定:重要数据是指相关组织、机构和个人在境内收集、产生的不涉及国家秘密,但与国家安全、经济发展以及公共利益密切相关的数据(包括原始数据和衍生数据)。

一旦企业拥有的数据被认定为重要数据,企业应当履行相应的合规义务,譬如在中国境内运营中收集和产生的重要数据,应当在境内存储。因业务需要,确需向境外提供的,应当进行安全评估。

《信息安全技术数据出境安全评估指南(征求意见稿)》以附录的形式列举了各行业(领域)重要数据的范围,并指出各行业(领域)主

管部门可结合实际，明确本行业（领域）重要数据定义、范围或判定依据。

因此，除个人信息之外，数字化转型的企业亦须重点关注重要数据并相应制订合规方案。

5.数据相关的商业模式合规

中国是互联网经济最为发达的国家之一，中国企业在商业模式方面的创新远远地走在了世界各国的前面。随着自动驾驶、人工智能、智能手机、可穿戴设备、机器人、物联网传感器、智能摄像头等智能设备爆炸式增长，越来越多新的商业模式在数据收集基础之上不断产生，商业价值增长的同时企业的网络安全和数据合规风险也越来越大。

对于任何企业而言，其商业模式的合法性都具有重要意义。如果一个企业的商业模式违规，那么无论是在日常经营、融资阶段还是随后的境内外上市，都将存在巨大的风险。投资人和监管机构的审查重点之一是商业模式的合法性。从另外一个角度而言，即使企业在融资的时候没有遇到障碍，不合规的经营模式可能在任何一个时点爆发风险，数据堂案就是很典型的一个案例。

确保商业模式的合规从方法论上来说，包括两个步骤，首先是对监管法规的深入理解；其次，是在此基础上对商业模式本质的精准认定。 对商业模式本质的合规判断需要商业逻辑和法律逻辑的高度统一，这也是知易行难的一个环节。

用户画像、基于数据的区别定价、数字营销中的“效果优化”、增长黑客、捆绑下载、精准广告推送、精准信息流分发、个性智能化服务、DMP、流量买卖、诱导分享，这些都是在新经济领域炽手可热的智能商业模式，那么这些商业模式是否存在法律风险呢？

5.1. 用户画像

精准广告推送、精准信息流分发、个性智能化服务等商业模式的基础之一就是用户画像。

根据《个人信息安全规范》，用户画像（user profiling）是指通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如其职业、经济、健康、教育、个人喜好、信用、行为等方面做出分析或预测，形成其个人特征模型的过程。

版权所有 翻印必究

用户画像可以分为直接用户画像和间接用户画像。直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

用户画像需要遵守如下规则:

- ✓ 隐私政策中应当包括收集、使用个人信息的目的，以及目的所涵盖的各个业务功能。例如将个人信息用于推送商业广告，将个人信息用于形成直接用户画像及其用途等。因此，在讨论商业模式时，如果需要用个人信息生成直接用户画像，首要工作是考虑如何修订隐私政策。
- ✓ 除目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。我们理解，除非是类似于网络信贷等有限商业模式须对个人信用状况准确评价，一般的商业模式很难达到“必需”的程度。
- ✓ 为准确评价个人信用状况，可使用直接用户画像，而用于推送商业广告目的时，则宜使用间接用户画像。值得注意的是，如果根据用户画像而推送商业广告，除前述关于“间接用户画像”的合规建议还须考虑“个性化展示以及推出”的合规要求。
- ✓ 当仅依据信息系统的自动决策而做出显著影响个人信息主体权益的决定时（例如基于用户画像决定个人信用及贷款额度，或将用户画像用于面试筛选），个人信息控制者应向个人信息主体提供申诉方法。
- ✓ 如果一个公司的商业模式是提供直接用户画像给第三方，则其合规风险较高。

值得注意的是:

考虑到数据技术的飞速发展，高精度算法在某些情况下已经可能让匿名数据重新被识别。即便是在商业模式中使用间接用户画像，仍然可能因为技术问题而存在合规风险。因此，判断涉及用户画像的商业模式是否合规须由商务团队、技术专家以及律师等各方从不同角度审查。

此外，对于投资人而言，如果一个 to B 业务的公司把数据用于用户画像进行精准营销时，须重点关注其业务合规风险，即其是否已经获得用户的充分授权。

5.2. 基于数据的区别定价

版权所有 翻印必究

基于数据的区别定价也就是所谓的“大数据杀熟”，是指商家通过对用户的分析，梳理出经济能力较强或对价格不敏感的用户，从而有针对性的进行差异化定价，以增加销售利润的做法。

根据网络公开信息，大数据杀熟的最早案例是亚马逊在 2000 年进行的一个“实验”。用户偶然在亚马逊电商平台上发现《泰特斯》（Titus）的碟片对老顾客的报价为 26.24 美元，但是在删除 Cookie 后发现报价变成了 22.74 美元。曝光后，亚马逊 CEO 贝索斯亲自道歉，称一切只是为了“实验”。与传统实体售卖平台不同，电商平台通过用户和 App 或 Web 的单向交互进行销售，也就是千人千面的展示形式，这就为商家提供了提高价格的“绝佳”机会。电商平台对用户数据的大量收集和分析更使得基于数据的区别定价变得容易。究其本质，“大数据杀熟”其实是基于用户画像进行个性化展示并提供不同售价的商业模式。

互联网发展迅猛而法规总是滞后于实践，但是这并不意味着“大数据杀熟”处于法外之地。监管机构可能根据如下法规对“大数据杀熟”行为进行监管：

- ✓ 《中华人民共和国价格法》第七条，经营者定价，应当遵循公平、合法和诚实信用的原则。
- ✓ 《中华人民共和国电子商务法》第十八条第一款，电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益。第七十七条，电子商务经营者违反本法第十八条第一款规定提供搜索结果，或者违反本法第十九条规定搭售商品、服务的，由市场监督管理部门责令限期改正，没收违法所得，可以并处五万元以上二十万元以下的罚款；情节严重的，并处二十万元以上五十万元以下的罚款。
- ✓ 《中华人民共和国反垄断法》第十七条，禁止具有市场支配地位的经营者从事下列滥用市场支配地位的行为：（六）没有正当理由，对条件相同的交易相对人在交易价格等交易条件上实行差别待遇。第四十七条，经营者违反本法规定，滥用市场支配地位的，由反垄断执法机构责令停止违法行为，没收违法所得，并处上一年度销售额百分之一以上百分之十以下的罚款。

值得注意的是，监管机构质疑的是大数据杀熟，但是并没有完全禁止个性化展示。对于个性化展示，须遵循相应的诸多合规要求，譬如电子商

务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项。

5.3. 数字营销中的刷量是“效果优化”还是数据流量造假?

广告大师约翰·沃纳梅克曾说过,“我知道我的广告费有一半是浪费的,但我不知道浪费的是哪一半”,这句至理名言堪称广告营销界的“哥德巴赫猜想”。有个非常经典的事件，2015 年某主播在某平台直播游戏“英雄联盟”时，聊天室显示观看人数竟然超过了 13 亿。任何真实用户的访问记录，包括但不限于 IP 地址、访问时间、频次都有可能被伪造。某些所谓的数字营销中的“效果优化”很可能就是刷量的结果。常见的刷量方式包括购入海量手机由特定程序控制进行点击，黑客劫持终端等多种方式。

在爱奇艺与飞益公司的案件中，法院认定“刷量”行为不仅会造成爱奇艺公司多支出不应承担的著作权许可使用费，还会让其基于不真实的访问数据，做出错误的商业决策，导致竞争优势的丧失。对消费者而言，因虚假访问量而排位在先的视频由于并不能真实反映消费者以及市场的需求，被访问量误导的消费者一旦发现视频排位与质量不相吻合时，将产生不良用户体验，从而怀疑爱奇艺网站的访问数据，进而不再信赖爱奇艺公司的商业信誉，最终选择其他服务提供商导致爱奇艺公司经济利益的再损失。法院判定，飞益公司违反公认的商业道德，损害爱奇艺公司以及消费者的合法权益，构成不正当竞争。

此外，值得注意的是，越来越多的司法机关已经将伪造流量认定为新型网络诈骗案,这意味着伪造流量除了民事责任之外还可能承担刑事责任。

5.4. 互联网新媒体公司的“加粉”

新三板挂牌公司北京瑞智华胜科技股份有限公司（下称“瑞智华胜”）一度是市场上的明星项目。根据其官方表述，作为互联网新媒体营销解决方案提供商其业务是“分析互联网用户的网络行为、喜好和各类媒体的投放价值，为客户定制针对目标用户的精准社会化广告营销及投放策略”。

2018 年 7 月 24 日，瑞智华胜曾发布公告称，公司法定代表人、董事周某某及监事黄某、梁某某因涉嫌非法获取计算机信息系统数据罪，已于 7 月 3 日被公安局刑拘。

根据网络公开报道中[1]办案警官的介绍，“他们先和运营商签订正规合同、拿到登录凭证，然后将非法程序置入用于自动采集用户 Cookie、手机号等信息。他们劫持数据后会进行爬取、还原等，为了不被发现，他们专门购买了 3 万多个 IP 地址用于频繁爬取”，“该公司自营微博和微信公号的粉丝、关注中，很大一部分是在用户未知的情况下，账号被非法操控后强行加粉或关注的，其中今年 1 月 24 日单日加粉数达到 109 万。针对不同的社交平台软件，该公司研发了不同用户信息提取、操控程序用于加粉”。

根据刑法第 285 条第 2 款，非法获取计算机信息系统数据、非法控制计算机信息系统罪是指违反国家规定，侵入国家事务、国防建设、尖端科学技术领域以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

瑞智华胜的商业模式是通过植入非法程序采集 Cookie 和手机号，之后又通过用户信息提取和操控程序进行加粉。该等操作至少涉嫌非法获取计算机信息系统数据、非法控制计算机信息系统罪以及侵犯公民个人信息罪。

对于互联网新媒体营销解决方案提供商，其微博、微信公众号等自媒体的粉丝数量对于其商业价值有巨大影响，但是如果通过不合规的方式“加粉”将导致重大的法律风险。

5.5. 增长黑客的法律风险

增长黑客的英文原文是“Growth Hacker”，这一概念是由美国互联网行业的传奇 Sean Ellis 在 2010 年提出。此后，由于互联网行业的爆发增长，Sean Ellis 关于增长黑客的理论和实践取得了巨大的成功，也对中国企业数字化转型造成了空前的影响。目前市场上除了 Sean Ellis 本人著作的《增长黑客 如何低成本实现爆发式成长》之外，还有很多其他作者的论述。很多商学院、企业家在讨论商业模式的时候都不可避免的受到了前述论述的影响。

增长黑客作为创新性的数据驱动策略可以有效的达到高效获取用户、激发活跃、提高留存度、增加营业收入以及病毒销售等商业目的。但这并不意味着增长黑客的策略一定合规。

[1] https://www.xianjichina.com/special/detail_352593.html

某关于增长黑客的论述提及了“借鸡下蛋”的策略。作者举例其曾经为了推广某个交友“APP”所需而抓取某 K 歌应用的用户头像照片。按照作者的说法，他们短时间下载了超过 1 万多张照片后虚拟成真实用户随机分布到地图上，作为给种子用户体验试玩的测试数据。

很明显照片属于个人信息，前述所谓“借鸡下蛋”策略事实上违反了《网络安全法》关于个人信息收集的规定，甚至有可能触犯刑法。

增长黑客的著作中还反复提及另外一个案例，即某世界领先旅游租房网站 A 在刚成立的时候为了引流，采用了如下的策略：（1）越过 C 的技术防御，通过机器人脚本将发布在 A 网站上的信息自动发到流量更大的 C 网站上；（2）A 定期扫描 C 的新房源，有新房源后会自动伪装成买家或新顾客，给卖家留言，内容大致是我对你的房源比较感兴趣，我建议你把它也发一份到 A 上。

对于中国的公司而言，如果简单粗暴地模仿前述 A 公司的策略将是极其危险的。任何一个公司的成功策略都有其时间、地域以及司法区域的特殊性，A 公司实施前述策略是在 2010 年，而且 A 公司是美国经营前述业务。即便如此，前述策略仍然充满争议，在 Quora 关于这个策略的问答中有人回答到，“虽然不知道为什么 C 没有起诉 A，但是 A 的行为违反了(1)C 当时的使用协议（terms of use）（譬如没有网络机器人/网络蜘蛛/网络爬虫/收集，没有假冒/假用户，没有误导性的电子邮件，没有垃圾邮件（no bots / spiders / crawlers / harvesting, no impersonation / fake users, no misleading emails, no spam））;(2) gmail 的使用协议; (3) 美国《2003 年垃圾邮件管制法》（The CAN-SPAM Act of 2003）以及（4）联邦和州关于广告的法律”[2]。

根据中国法律法规以及指导案例，如果在中国采取前述 A 的策略将很有可能构成非法侵入计算机系统罪并承担刑事责任。因此，数据化转型中的中国公司如果考虑增长黑客策略，那么首要应确保该策略合法合规。

5.6. 捆绑下载

捆绑下载是某些经营者利用其技术或者市场的优势，在用户下载安装某软件时未取得用户明示同意而下载另外一个软件的行为。从用户推广角度，捆绑下载不失为有效的方案，但是捆绑下载存在较大的违规风险。

2017 年搜狗诉百度案是典型的有关捆绑下载的案例，其树立了如下原则:

[2]https://www.quora.com/Did-Airbnb-get-sued-for-running-a-robot-on-craigslist-Where-are-they-breaking-the-law-anyways

- ✓ 反不正当竞争法语境下公认的商业道德的评判标准应当以特定商业领域普遍认同和接受的行为标准作为评判尺度。
- ✓ 公认的商业道德应当是特定行业的经营者普遍认同的、符合消费者利益和社会公共利益的经营规范和道德准则。
- ✓ 《规范互联网信息服务市场秩序若干规定》第八条第一项的规定，互联网信息服务提供者不得欺骗、误导或者强迫用户下载、安装、运行、升级、卸载软件。第九条规定，互联网信息服务终端软件捆绑其他软件的，应当以显著的方式提示用户，由用户主动选择是否安装或者使用，并提供独立的卸载或者关闭方式，不得附加不合理条件。
- ✓ 在用户通过百度搜索引擎搜索、下载搜狗软件时，通过技术设定使用户一并下载“百度杀毒”等软件或者下载目标软件前先行下载“百度手机助手”软件，本质上均属于《规范互联网信息服务市场秩序若干规定》第九条规定的软件捆绑行为。但百度公司并未以显著方式提示用户，以供用户自主选择是否安装或使用。
- ✓ 百度未尽到充分、明确提示与说明义务，其被诉行为导致网络用户在下载搜狗软件时，在毫无预期、不知情或无法充分研判的情况下，额外下载其原本并不希望或不需要下载的“百度杀毒”等软件。
- ✓ 百度因违反公认的商业道德而具有不正当性，且造成了对消费者利益和搜狗信息公司、搜狗科技公司利益以及竞争秩序的损害，不制止不足以维护公平竞争的秩序，故构成《反不正当竞争法》第二条所禁止的不正当竞争行为。

因此，如果某个公司的推广策略中包含捆绑下载时，必须考虑前述判决的影响以及相应的违规风险。

5.7. 关于商业模式的最佳实践

根据我们在网络安全以及数据合规领域的实践，就商业模式的最佳实践简单总结如下：

- ✓ 增长黑客的策略需要确保其在中国法下合规;
- ✓ “大数据杀熟”有违规风险但是个性化展示可在符合要求的前提下实施;
- ✓ 在与任何第三方进行有关数据的业务合作，确保己方和对方获取数据的范围在数据权利主体的授权范围内;

版权所有 翻印必究

- ✓ 在自己的网站或者 APP 上设置必要的反爬措施，并对数据的权属进行声明，譬如禁止 spider 访问特定目录；禁止访问网站中的特定页面；禁止抓取网站上的特定图片等。
- ✓ 不得通过模拟数据权利方客户请求的方式来获取数据;
- ✓ 不得突破对方的防屏蔽规则，特别是对方有封账号、封 IP、验证码等安全策略时不得用技术手段强行访问;
- ✓ 避免采用爬虫高频次访问要获取数据的服务器;
- ✓ 不得通过非法利用对方员工的账号、密码或权限获取数据;
- ✓ 不得植入钓鱼链接及利用钓鱼网站获取数据;
- ✓ 不得未经允许安装域名解析软件（用于显示计算机地址，例如“花生壳”）、多用户系统软件（远程控制计算机）、键盘记录软件（用于盗取账号和密码，例如“灰鸽子”）并利用其获取数据;
- ✓ 不得通过各种木马程序非法获取数据;
- ✓ 获取计算机信息系统数据时，不得对系统内的数据进行增加、删除、修改等操作，干扰信息系统的正常运行;
- ✓ 不得非法侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统。

6. 网络安全以及数据合规的最佳实践范例

网络突破了时空限制，由此带来的是更加复杂的安全环境。而数据由于其固有的高流动、无边界、易被复制、易被修改、高价值、高隐私附着以及泄露后可能造成巨大损失或者损害的特性，其合规应该是全生命周期统筹而非就某个阶段或者环节考虑。就数据全周期策略而言，对于数据的收集、保存、使用、委托、共享、转让、公开披露、出境以及并购等多个场景，需进行相应的合规设计，包括 data mapping、等级保护、供应商管理、安全事件处理等。

篇幅所限，我们仅讨论数据的收集、供应商管理、等级保护、数据出境以及涉及数据的并购等五个场景。其他的场景在之后会陆续和大家分享。

6.1. 数据收集的 12 个合规要点

在任何一个中国企业的数字化转型过程中，数据的收集是首要问题也是第一个合规风险敞口。

版权所有 翻印必究

6.1.1. 什么是数据的收集

根据《个人信息安全规范》，收集是指获得对个人信息控制权的行为，包括:

- ✓ 由个人信息主体主动提供
- ✓ 通过与个人信息主体交互或记录个人信息主体行为等自动采集
- ✓ 以及通过共享、转让、搜集公开信息间接获取等方式

如果产品或服务的提供者提供工具供个人信息主体使用，提供者不对个人信息进行访问的，则不属于本标准所称的收集行为。例如，离线导航软件在终端获取用户位置信息后，如不回传至软件提供者，则不属于个人信息收集行为。

简而言之，无论通过何种方式获取任何个人信息的行为均属于收集。值得注意的是，这只是狭义的数据收集，毕竟在商业环境中需要保护的除了个人信息之外还有重要数据以及其它数据。

6.1.2. 数据收集的法律以及规范要求

- ✓ 《网络安全法》第四十一条树立了收集个人信息最重要的原则。网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。
- ✓ 根据《个人信息安全规范》，个人信息控制者开展个人信息处理活动，应遵循以下基本原则。换言之，任何一个公司在就数据全生命周期中都应该遵循如下原则:
  - 权责一致原则——对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。
  - 目的明确原则——具有合法、正当、必要、明确的个人信息处理目的。
  - 选择同意原则——向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意。

版权所有 翻印必究

- 最少够用原则——除与个人信息主体另有约定外，只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时根据约定删除个人信息。
- 公开透明原则——以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。
- 确保安全原则——具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。
- 主体参与原则——向个人信息主体提供能够访问、更正、删除其个人信息，以及撤回同意、注销账户等方法。

6.1.3. 对收集个人信息的合法性要求

- ✓ 不得欺诈、诱骗、强迫个人信息主体提供其个人信息;
- ✓ 不得隐瞒产品或服务所具有的收集个人信息的功能;
- ✓ 不得从非法渠道获取个人信息;
- ✓ 不得收集法律法规明令禁止收集的个人信息。

6.1.4. 收集个人信息的最小化要求

- ✓ 收集的个人信息的类型应与实现产品或服务的业务功能有直接关联。直接关联是指没有该信息的参与，产品或服务的功能即无法实现;
- ✓ 自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率;
- ✓ 间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

6.1.5. 收集个人信息时的授权同意

- ✓ 收集个人信息前，应向个人信息主体明确告知所提供产品或服务的不同业务功能分别收集的个人信息类型，以及收集、使用个人信息的规则（例如收集和使用个人信息的目的、收集方式和频率、存放地域、存储期限、自身的数据安全能力、对外共享、转让、公开披露的有关情况等），并获得个人信息主体的授权同意;

6.1.6. 间接获取个人信息的要求

版权所有 翻印必究

- ✓ 应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；
- ✓ 应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露等。
- ✓ 如本组织开展业务需进行的个人信息处理活动超出该授权同意范围，应在获取个人信息后的合理期限内或处理个人信息前，征得个人信息主体的明示同意。

6.1.7. 使用个人信息无需征得个人信息主体的授权同意的情形：

- ✓ 与国家安全、国防安全直接相关的；
- ✓ 与公共安全、公共卫生、重大公共利益直接相关的；
- ✓ 与犯罪侦查、起诉、审判和判决执行等直接相关的；
- ✓ 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；
- ✓ 所收集的个人信息是个人信息主体自行向社会公众公开的；
- ✓ 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；
- ✓ 根据个人信息主体要求签订和履行合同所必需的；
- ✓ 用于维护所提供的产品或服务的安全稳定运行所必需的，例如发现、处置产品或服务的故障；
- ✓ 个人信息控制者为新闻单位且其开展合法的新闻报道所必需的；
- ✓ 个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的；
- ✓ 法律法规规定的其他情形。

6.1.8. 收集个人敏感信息时的明示同意

- ✓ 收集个人敏感信息时，应取得个人信息主体的明示同意。应确保个人信息主体的明示同意是其在完全知情的基础上自愿给出的、具体的、清晰明确的愿望表示；

版权所有 翻印必究

✓ 通过主动提供或自动采集方式收集个人敏感信息前，应：

- 向个人信息主体告知所提供产品或服务的基本业务功能及所必需收集的个人敏感信息，并明确告知拒绝提供或拒绝同意将带来的影响。应允许个人信息主体选择是否提供或同意自动采集；
- 产品或服务如提供其他扩展功能，需要收集个人敏感信息时，收集前应向个人信息主体逐一说明个人敏感信息为完成何种扩展功能所必需，并允许个人信息主体逐项选择是否提供或同意自动采集个人敏感信息。当个人信息主体拒绝时，可不提供相应的扩展功能，但不应以此为理由停止提供基本业务功能，并应保障相应的服务质量。根据《信息安全技术 个人信息安全规范（草案）》，如果产品或服务不提供基本业务功能，个人信息主体将不会选择使用该产品或服务。应根据个人信息主体选择、使用所提供产品或服务的根本期待和最主要的需求，划定产品或服务的基本业务功能。

6.1.9. 收集未成年人信息

收集年满 14 周岁的未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意。

6.1.10. 《个人信息安全规范》是否必须要遵守

从规范的效力位阶角度，《个人信息安全规范》不属于《立法法》所规定的宪法、法律、行政法规、地方性法规、行政条例及规章这些法律渊源中的任何一种，而且其自身也明确定性为推荐性的国家标准。其似乎没有强制性的效力。但是事实上，其具有重要的约束力。也即有学者提到的“《个人安全规范》不具有形式上的拘束力，具有事实上的拘束力。”[3]首先，《个人信息安全规范》由全国信息安全标准化技术委员会制定，《个人信息安全规范》已经成为监管机构进行监督检查的把握执法尺度的重要标准。如光明网 2018 年 01 月 10 日的报道，“国家互联网信息办公室网络安全协调局约谈‘支付宝年度账单事件’当事企业负责人”就提到网络安全协调局负责人指出，支付宝、芝麻信用收集使用个人信息的方式，不符合刚刚发布的《个人信息安全规范》国家标准的精神。而中央网信办、工业

[3] 许可著“《个人信息安全规范》的效力与功能“，载于微信公众号“网安寻路人”2019 年 4 月 30 日

和信息化部、公安部、市场监管总局四部委已经连续开展了两届“App违法违规收集使用个人信息专项治理”行动，其依据的主要标准也是《个人信息安全规范》中的大部分原则。进一步而言，虽然《个人信息安全规范》并不是法院办理案件的必须遵守的依据，但是这个领域目前没有细化的法律、行政法规，所以法院在审理案件过程中，在确定是否存在侵犯公民个人信息的行为时，大概率情况下，会参考《个人信息安全规范》确定的专业化的意见，甚至最高人民法院出台的司法解释中，也会充分考虑《个人信息安全规范》的规定，有其明显的影子。有鉴于此，《个人信息安全规范》对于行政执法和司法裁判都具有实质的重要影响，自然也应当成为需要被遵守的规范。所以才会被称为“软法”。

6.1.11. 朱烨诉百度案件是否意味着 Cookie 不属于个人信息，可自由收集？

Cookie 的定性是业内从业人员特别关心的问题。Cookie 是常见的自动数据收集工具中的一种，自动数据收集工具还包括脚本、Web 信标、FlashCookie、内嵌 Web 链接、本地存储器等。对于 Cookie 是否属于个人信息、是否可以自由收集，业内有个常见的错误理解就是在朱烨诉百度案件后法院已经认定 Cookie 不属于个人信息，因此可以自由收集。

在“北京百度网讯科技公司与朱烨隐私权纠纷案”中，百度网讯公司使用了 Cookie 技术记录和跟踪了原告所搜索的关键词，利用记录的关键词，对原告浏览的网页进行广告投放。原告起诉百度网讯公司的行为侵犯了其隐私权。终审法院认为，该 Cookie 关键词记录未能与原告的个人身份对应识别，不符合“个人信息”的可识别性要求;又因为百度网讯公司利用网络技术提供个性化推荐服务，并未直接将搜索引擎服务而产生的数据和 Cookie 信息向第三方或公众展示，没有任何的公开行为，因而不属于侵害个人隐私的行为。

值得注意的是，由于该案件发生在《网络安全法》及 2017 年《关于侵犯公民个人信息案件的解释》、《个人信息安全规范》等法律、规范性文件颁布和生效之前，该案件中认定的 Cookie 的性质已经不具有太多参考意义。此外，中国不是判例法国家，该案件的终审法院也不是最高院，从另外角度来说，这个案例不可能对任何一个后续案件构成有约束力的先例。

版权所有 翻印必究

在《个人信息安全规范》中，Cookie 规定在其附录的隐私政策模版中，其表述为“二、我们如何使用 Cookie 和同类技术:（一）Cookie 为确保网站正常运转，我们会在您的计算机或移动设备上存储名为 Cookie 的小数据文件。Cookie 通常包含标识符、站点名称以及一些号码和字符。借助于 Cookie，网站能够存储您的偏好或购物篮内的商品等数据。我们不会将 Cookie 用于本政策所述目的之外的任何用途。您可根据自己的偏好管理或删除 Cookie。有关详情，请参见 AboutCookies.org。您可以清除计算机上保存的所有 Cookie，大部分网络浏览器都设有阻止 Cookie 的功能。但如果您这么做，则需要在每一次访问我们的网站时亲自更改用户设置。如需详细了解如何更改浏览器设置，请访问以下链接:

<Internet Explorer>、<Google Chrome>、<Mozilla Firefox> 、<Safari>和<Opera>。（二）网站信标和像素标签 除 cCookie 外，我们还会在网站上使用网站信标和像素标签等其他同类技术。例如，我们向您发送的电子邮件可能含有链接至我们网站内容的点击 URL。如果您点击该链接，我们则会跟踪此次点击，帮助我们了解您的产品或服务偏好并改善客户服务。网站信标通常是一种嵌入到网站或电子邮件中的透明图像。借助于电子邮件中的像素标签，我们能够获知电子邮件是否被打开。如果您不希望自己的活动以这种方式被追踪，则可以随时从我们的寄信名单中退订。（三）Do Not Track（请勿追踪）很多网络浏览器均设有 Do Not Track 功能，该功能可向网站发布 Do Not Track 请求。目前，主要互联网标准组织尚未设立相关政策来规定网站应如何应对此类请求。但如果您的浏览器启用了 Do Not Track，那么我们的所有网站都会尊重您的选择。（四）……”

因此，目前对于 Cookie 必须在监管要求范围之内谨慎使用。如此前所分析，瑞智华胜的商业模式是通过植入非法程序采集 Cookie 和手机号，之后又通过用户信息提取和操控程序进行加粉。该等操作至少涉嫌非法获取计算机信息系统数据、非法控制计算机信息系统罪以及侵犯公民个人信息罪。

6.1.12. 关于信息收集合规的最佳实践

- ✓ 根据监管要求制订合规隐私政策
- ✓ 必须清楚地知道中国法规和规范中“个人信息”以及“个人敏感信息”的范围;

版权所有 翻印必究

- ✓ 收集个人敏感信息时，应取得个人信息主体的明示同意。应确保个人信息主体的明示同意是其在完全知情的基础上自愿给出的、具体的、清晰明确的愿望表示;
- ✓ 收集年满 14 周岁的未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意;
- ✓ 清楚界定自己服务的核心功能以及相关的必要信息范围;
- ✓ 最小够用原则，不应收集与业务功能无关的信息和权限，譬如美图软件没有必要访问手机通信录;
- ✓ 搜集信息必须通过告知和声明的前置程序;
- ✓ 搜集过程中必须真实、准确、完整的披露信息范围、使用范围，不得有欺诈、误导或者强迫;
- ✓ 需要根据具体情况而提供选择性加入 Opt-in，选择性退出 Opt-out 的机制;
- ✓ 拒绝非必要信息提供不能影响接受服务。例如淘宝网《法律声明及隐私权政策》中就说明“在注册会员过程中，如果您提供以下额外信息补全个人资料,将有助于我们给您提供如会员生日特权等更个性化的会员服务：您的真实姓名、性别、出生年月日、居住地、您本人的真实头像，但如果您不提供这些信息，将会影响到您使用个性化的会员服务,但不会影响使用淘宝网产品或服务的基本浏览、搜索、购买功能”;
- ✓ 用第三方 SDK 时，须对 SDK 做安全审查，确保充分了解 SDK 的搜集信息范围;
- ✓ 通过协议限制 SDK 过度搜集用户信息;
- ✓ 不得超过授权使用;
- ✓ 应当分项告诉用户功能或者服务收集个人信息详情;
- ✓ 收集内容、使用目的、方式、保护方式、共享等发生变更需要告知用户;

版权所有 翻印必究

- ✓ 如果通过 App 收集信息，须遵循包括《App 违法违规收集使用个人信息自评估指南》、《App 违法违规收集使用个人信息行为认定方法（征求意见稿）》等在内要求而相应合规整改。

6.2. 等级保护

根据《网络安全法》第二十一条，国家实行网络安全等级保护制度（下称“等保”）。网络运营者应当按照网络安全等级保护制度的要求，履行相应安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

6.2.1. 等保适用法规

《网络安全法》对等保仅做了原则性的规定。公安部和信安标委分别下发了两个征求意见稿，即《网络安全等级保护条例(征求意见稿)》（下称“《等保条例》”）和《信息安全技术网络安全等级保护定级指南（征求意见稿）》（下称“《定级指南》”）。在正式文件出台之前，目前适用的还是《中华人民共和国计算机信息系统安全保护条例》 (2011 年 1 月 8 日实施，国务院令第 588 号) 的安保体系。

6.2.2. 五个安全保护等级

根据网络在国家安全、经济建设、社会生活中的重要程度，以及其一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及相关公民、法人和其他组织的合法权益的危害程度等因素，《等保条例》将网络分成了五个安全保护等级，即:

- ✓ 第一级，一旦受到破坏会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社会秩序和公共利益的一般网络。
- ✓ 第二级，一旦受到破坏会对相关公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全的一般网络。
- ✓ 第三级，一旦受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害，或者会对社会秩序和社会公共利益造成严重危害，或者对国家安全造成危害的重要网络。
- ✓ 第四级，一旦受到破坏会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害的特别重要网络。

版权所有 翻印必究

- ✓ 第五级，一旦受到破坏后会对国家安全造成特别严重危害的极其重要网络。

6.2.3. 特定对象的安保等级

对于大数据，应综合考虑数据规模、数据价值等因素，根据数据资源（完整性、保密性、可用性）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侵害程度等因素确定其安全保护等级。原则上，大数据安全保护等级不低于第三级。

对于确定为关键信息基础设施的，原则上其安全保护等级不低于第三级。

6.2.4. 安保三级的意义

如果一个公司其安保等级被评定为三级或者三级以上，则意味着其应当承担特殊安全保护义务，那么在如下方面，其都将适用更加严格的标准:

- ✓ 上线检测
- ✓ 等级测评
- ✓ 网络服务提供者的选择
- ✓ 产品服务采购使用的安全要求
- ✓ 技术维护，三级以上网络应在境内实施技术维护，不得境外远程技术维护
- ✓ 监测预警和信息通报
- ✓ 应急处置要求
- ✓ 非涉密网络密码保护
- ✓ 安全监督管理
- ✓ 安全检查
- ✓ 关键人员管理
- ✓ 违反安全保护义务后果
- ✓ 违反技术维护要求后果

6.3. 供应商管理

版权所有 翻印必究

6.3.1. 为什么需要管理供应商

我们注意到，由于数据的易复制性、高流动性，此前发生的多起数据安全事件都和供应商有关，譬如:

- ✓ 2015 年 10 月，Experian（信用报告机构）为 T-Mobile 提供处理信贷申请时的客户信用检查服务。由于 Experian 的一个包含 T-Mobile 客户信息的服务器被入侵，造成约 1500 万 T-Mobile 用户的个人信息暴露。[4]
- ✓ 2017 年 3 月，Dun&Bradstreet（邓白氏，世界著名商业信息服务机构）一个大小为 52GB 的数据库意外在线泄露，被泄露信息包括 AT&T、沃尔玛、Wells Fargo、美国邮政，甚至美国国防部等在内的 3300 多万员工的信息和联系方式等。[5]
- ✓ 2017 年 7 月，浙江苍南警方在侦查中发现，有苹果国内公司员工涉嫌以非法手段获取苹果手机关联的公民个人信息，并在网上大量出售，涉案金额巨大。随即，苍南警方开展侦破工作，共抓获主要犯罪嫌疑人 22 人，其中涉及苹果国内直销公司及苹果外包公司员工 20 人。[6]
- ✓ 2017 年 7 月，Verizon（美国本土电信公司）由于与 NICE Systems（一家以色列的公司）合作，导致超过 1.4 亿的美国用户个人信息暴露在网上，这些信息被存储在不受保护的亚马逊 S3 云服务器上，任何人都可以访问并且下载这些数据。被暴露的信息中包含众多敏感信息，包括用户姓名、电话号码、账户 PIN 码（个人识别码）。[7]
- ✓ 由于 Inbenta Technologie（软件开发服务商）所提供的软件中含有恶意代码，导致 Ticketmaster（活动票务巨头公司）发生了数据泄露事件，影响了近 5%的全球用户，泄露数据包含用户个人信息和银行卡数据等。[8]
- ✓ Level One Robotics 公司是百余家车厂共同的服务器提供商。该公司在一个可公开访问的服务器中使用了一种用于备份大型数据集的通用文件传输协议 rsync，但却没有设定任何安全密码保护措施。通过该传输协议，任何用户都可无障碍访问其中的隐私数据，因此造成

[4] https://blog.csdn.net/yoyoyoyo000/article/details/48883137
[5] https://www.sohu.com/a/215090624_682308
[6] http://tech.qq.com/a/20170607/035410.html
[7] http://www.sohu.com/a/157044936_257305
[8] http://mini.eastday.com/a/181126092156993.htm

版权所有 翻印必究

100 多家车厂的机密数据被泄露，其中包括通用汽车、菲亚特克莱斯勒、福特、特斯拉、丰田、蒂森克虏伯及大众等。[9]

6.3.2. 网络运营者与供应商相关的保护数据安全义务

在中国法下，无论是网络运营者还是供应商只要被认定为《网络安全法》下的“网络运营者”，均有法定的保护数据安全的义务。

根据《网络安全法》，网络运营者有如下基本义务：（1）采取技术措施和其他必要措施，保障网络安全，维护数据安全。（扩展性义务）（2）对其收集的用户信息严格保密，并建立健全用户信息保护制度。（第一责任主体）

首先，任何一个供应商均须根据网络安全等保制度履行下述网络安全义务：

- ✓ 安全制度和安全负责人
- ✓ 技术措施
- ✓ 监控并至少留存六个月网络日志
- ✓ 数据分类，重要数据备份和加密
- ✓ 安全应急预案
- ✓ 安全事件发生时启动应急预案、采取补救措施并报告
- ✓ 产品、服务应当符合国标的强制性要求
- ✓ 不得设置恶意程序
- ✓ 发现存在安全缺陷时，应当立即补救，告知用户并报告
- ✓ 应当为其产品、服务持续提供安全维护

而对于关键信息基础设施运营者而言，则需要承担更多义务：

- ✓ 确保支持业务稳定、持续运行的性能——安全措施“三同时”
- ✓ 设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查
- ✓ 技术措施
- ✓ 监控并至少留存六个月网络日志

[9] http://www.qdaily.com/articles/55510.html

- ✓ 数据分类，重要数据备份和加密
- ✓ 应急预案，定期演练
- ✓ 定期进行安全教育，技术培训和技能考核
- ✓ 重要系统和数据库容灾备份
- ✓ 采购产品和服务，通过国家安全审查，签订安全保密协议
- ✓ 每年对网络安全和风险进行一次检测评估，并将结果和改进报送相关部门
- ✓ 个人数据和重要数据境内存储

6.3.3. 管理供应商的最佳实践——引进供应商前的准备工作

作为管理供应商的第一步，在引进供应商之前要做如下的准备工作：

- ✓ 双向 Data Mapping，即需要了解自己公司以及对方公司的数据全生命周期的流向并绘制数据流图表（Data Flow Diagram）；
- ✓ 数据流图表（Data Flow Diagram）所涉及的数据应包括存储在服务器、网络、第三方数据中心以及云、办公设备（台式机、笔记本电脑、U 盘、移动硬盘、手机以及其他设备），联网设备以及工业控制系统中的数据等任何与公司业务相关的数据；
- ✓ 确认前述数据中是否包含个人信息；
- ✓ 确认前述数据中是否包括敏感个人信息；
- ✓ 确认数据是否包括重要数据；
- ✓ 确认在本次合作中供应商将从公司获得哪些数据；
- ✓ 与供应商的合作涉及开放哪些系统的权限？权限的内容和级别是？
- ✓ 公司生效的隐私政策以及用户协议是否允许本次与供应商的合作；
- ✓ 公司与本次供应商的合作是否违反任何适用的法律；
- ✓ 公司与本次供应商的合作是否会违反任何一方在先的生效协议，如是，是否取得相应的豁免。

版权所有 翻印必究

6.3.4. 管理供应商的最佳实践——对供应商做网络安全与数字合规的尽职调查

从网络安全与数字合规的角度，任何一个公司在引进供应商的时候须对供应商做网络安全合规的专项尽职调查。尽职调查应主要关注如下方面：

- ✓ 供应商是否通过等保，如是，等保几级？
- ✓ 供应商是否有完全符合中国以及其他适用法律的网络安全制度？
- ✓ 前述制度如何被执行？
- ✓ 供应商的数据来源是否合法？
- ✓ 供应商是否符合信任链（Chain of Trust）原则？
- ✓ 供应商是否采用加密技术处理其数据？
- ✓ 供应商是否有网络安全保险（cyber security insurance）？
- ✓ 供应商此前是否签署过任何限制本次合作的协议？
- ✓ 供应商是否有任何网络安全以及数据方面的不良记录

6.3.5. 管理供应商的最佳实践——如何与供应商合作

- ✓ 合作之前对自己以及对方进行双向的 data mapping;
- ✓ 确保自己收集数据的流程合规;
- ✓ 确保对方收集数据的流程合规;
- ✓ 确保任何数据在处理之后无法识别特定个人且不能复原后才可以流转;
- ✓ 在协议中要求对方不能采用任何手段重新识别特定个人身份;
- ✓ 三重授权原则;
- ✓ 限制供应商的转委托（sub-license）;
- ✓ 所有的授权许可都应该有兜底的条款，即“本协议未注明的一切权利，归属于本公司所有”;

版权所有 翻印必究

- ✓ 规定供应商对数据库的使用权限仅限于经过匿名化处理的数据集;
- ✓ 严禁供应商将数据集用于未经授权的用途。

6.4. 数据出境

全球经济一体化进程中，越来越多的企业面临着数据出境的现实需要，譬如跨国银行就某客户的全球范围的账户信息查询系统、国际酒店品牌对于持有白金会员的住宿消费记录、航空联盟对于乘客里程记录、汽车自动驾驶与全球技术中心的数据交换等。

6.4.1. 何谓“数据出境”

针对数据出境，网信办会同相关部门起草的《个人信息和重要数据出境安全评估办法（征求意见稿）》和信安标委公布的《信息安全技术 数据出境安全评估指南(征求意见稿)》均作出了界定。后者规定更为细致：数据出境（data cross-border transfer）是指网络运营者（即网络的所有者、管理者和网络服务提供者）通过网络等方式，将其在中华人民共和国境内运营中收集和产生的个人信息和重要数据，通过直接提供或开展业务、提供服务、产品等方式提供给境外的机构、组织或个人的一次性活动或连续性活动。

此外，《信息安全技术 数据出境安全评估指南(征求意见稿)》还强调以下三种情形也属于数据出境:

- ✓ 向本国境内但不属于本国司法管辖或未在境内注册的主体提供个人信息和重要数据;
- ✓ 数据未转移存储至本国以外的地方，但被境外的机构、组织、个人访问查看的（公开信息、网页访问除外）;
- ✓ 网络运营者集团内部数据由境内转移至境外,涉及其在境内运营中收集和产生的个人信息和重要数据的。

同时，非在境内运营中收集和产生的个人信息和重要数据，经由本国出境且未经任何变动或加工处理的，或虽在境内存储、加工处理后出境，但不涉及境内运营中收集和产生的个人信息和重要数据的，不属于数据出境。

6.4.2. 何谓“境内运营”

版权所有 翻印必究

依据《个人信息和重要数据出境安全评估办法（征求意见稿）》，境内运营(domestic operation)是指网络运营者在中华人民共和国境内开展业务，提供产品或服务的活动。《信息安全技术 数据出境安全评估指南(征求意见稿)》进一步阐释，未在中华人民共和国境内注册的网络运营者，但在中华人民共和国境内开展业务，或向中华人民共和境内提供产品或服务的，属于境内运营。判断网络运营者是否在中华人民共和国境内开展业务，或向中华人民共和境内提供产品或服务的参考因素包括但不限于使用中文、以人民币作为结算货币、向中国境内配送物流等。

中华人民共和国境内的网络运营者仅向境外机构、组织或个人开展业务、提供商品或服务，且不涉及境内公民个人信息和重要数据的，不视为境内运营。

6.4.3. 数据出境评估的要点内容

数据出境评估的要点主要集中在出境目的和安全风险两个方面。前者需满足合法性、正当性和必要性的要求；后者应综合考虑出境数据的属性（根据数据的类别是个人信息还是重要数据评估要点，评估各有侧重）和数据出境发生安全事件的可能性及影响程度。

值得注意的是，数据出境涉及多方主体的，如云服务、转包服务等，根据数据出境发起方，确定安全自评估责任主体。如：云服务客户主动要求云服务提供商进行数据出境的，由云服务提供商配合云服务客户开展安全自评估，且由云服务客户承担相应责任。如云服务提供商主动要求进行出具出境的，由云服务客户配合云服务提供商开展安全自评估，且由云服务提供商承担相应责任。

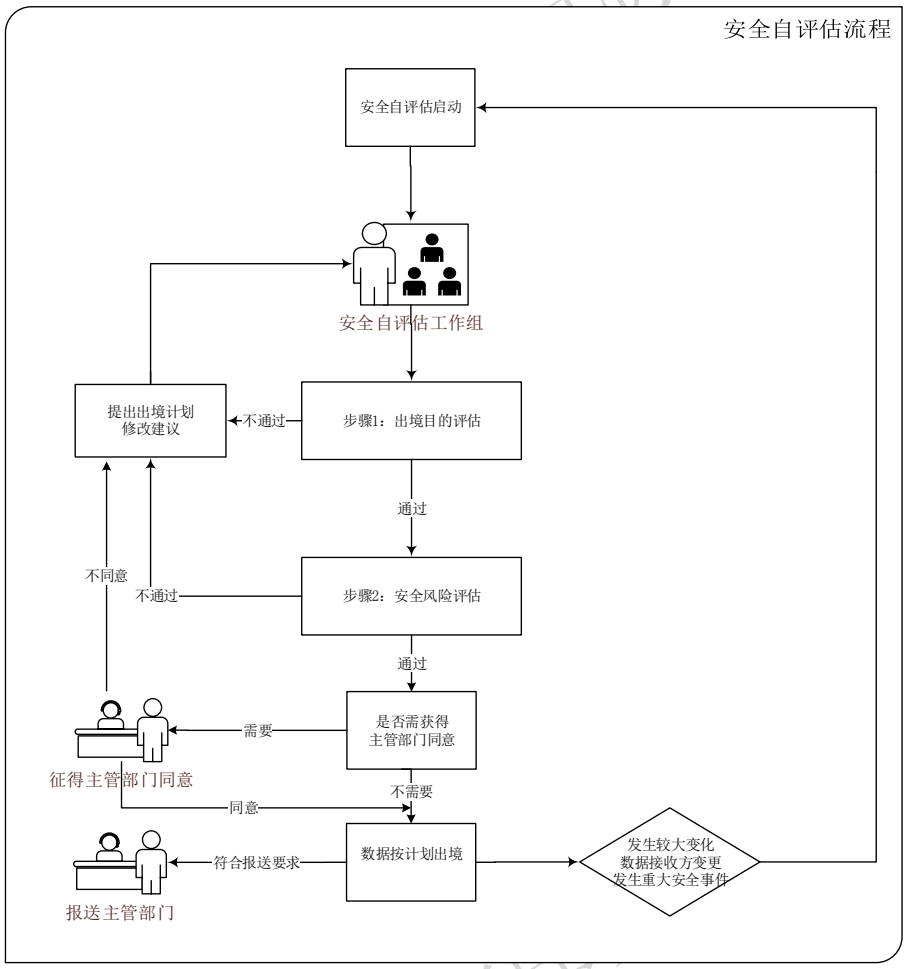
6.4.4. 数据出境的评估

数据出境评估可以分为“安全自评”和“主管部门评估”。依据《个人信息和重要数据出境安全评估办法（征求意见稿）》，网络运营者应在数据出境前，自行组织对数据出境进行安全评估，并对评估结果负责；而在特定情况下，如关键信息基础设施运营者数据出境等情形，需要由网络运营者报请行业主管或监管部门组织安全评估。

需特别注意的是，《关键信息基础设施安全保护条例(征求意见稿)》规定 CII 的运行维护应当在境内实施。因业务需要，确需进行境外远程维护的，应事先报国家行业主管或监管部门和国务院公安部门。《个人信息和重要数据出境安全评估办法（征求意见稿）》规定，

CII 的系统漏洞、安全防护等网络安全信息，以及 CIIO 向境外提供个人信息和重要数据都必须报请行业主管或监管部门组织安全评估。这体现了国家对于关键数据出境的严格控制。

6.4.5. 数据出境自评估的具体流程如下图:



6.4.6. 禁止出境的情形

《评估办法》还规定了几种禁止出境的情形，包括:

- ✓ 个人信息出境未经个人信息主体同意，或可能侵害个人利益;
- ✓ 数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益;
- ✓ 其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。

6.5. 并购中如何控制网络安全以及数据风险

版权所有 翻印必究

随着企业数据化的转型和大数据的广泛应用，企业存储和使用着大量的个人数据和用户信息。虽然目前国内相关法律并未明确将数据与现金、知识产权等作为公司财产的一种，并且由于数据生态的复杂性和数据权利的多样性，数据权属目前仍然存在较多争议。但毋庸置疑，数据已成为重要的新兴资产类别。例如，在收购以电商、社交、硬件、互联网金融、物联网等数据驱动型公司股权或资产时，数据往往是买家看重的核心资产。随之而来，在数据驱动型的并购交易中，对与数据有关的商业模式的网络安全、数据合规和隐私保护，亦逐渐成为并购交易关注的重点。

6.5.1. 对于收购双方的重要性

对于收购方而言，标的公司的数据合规是重要的风险管控内容，它直接决定了所收购资产的价值（是否可实现资本溢出和业务协同的效应，抑或带来重大的违规成本）。此外，在尽职调查阶段，获得目标公司的客户、用户、员工等数据也有助于收购方有效判断标的公司的各项经营、盈利、人力等指标的状况。

对于被收购方而言，在收购期间，向收购方提供数据和个人信息，构成数据处理。应如何在遵守相关法律和其数据合规制度、隐私保护政策的前提下，以合规方式向收购方及相关第三方（并购交易的参与方）进行披露和传输，是收购方应重点关注的问题。

6.5.2. 在并购各阶段应关注的要点

数据合规不仅是尽职调查的重点内容，在并购战略、标的公司估值、合同谈判、交割后的整合等各阶段，也应引起高度重视。以收购方为例：

首先，在收购方收购以数据为核心资产的标的时，应评估数据资产对于交易的重要性、收购后在数据相关业务的商业目的是否可以实现、数据资产在估值（模型）中的权重和影响，这些都有助于收购方形成科学和清晰的收购战略。

其次，数据合规的尽调作为一种新型的尽职调查，主要包括：

- ✓ 标的公司是否属于关键信息基础设施运营者；
- ✓ 标的公司的数据规模和数据梳理；
- ✓ 标的公司现行有效的隐私政策如何；

版权所有 翻印必究

- ✓ 标的公司如何收集、使用、存储、加密、共享、披露、销毁数据;
- ✓ 标的公司的第三方供应商管理状况;
- ✓ 标的公司是否存在数据泄漏或其它违规的历史问题;
- ✓ 标的公司目前或未来是否存在数据违规的潜在风险;
- ✓ 此外有别于传统尽职调查,此类尽调还涉及网络安全技术层面的尽职调查，即 IT（软硬件）的安全审查，例如对关键资产的漏洞扫描（vulnerability scans）和渗透测试（penetration test），因此也需要聘请技术专家进行评估。

由此可见，并购中关于数据合规的尽调，主要在于帮助收购方筛查和甄别标的公司是否存在数据泄漏等违规情形，从而避免因此承担目标公司的历史遗留的法律责任和风险，或通过估值调整、协议明晰责任分担等方式进行调整。

未能进行全面的数据合规尽调的后果可能会非常严重。例如，2014 年美国在线旅游网站 TripAdvisor 以 2 亿美金收购了旅行预订网站 Viator，交割后大约两周，Viator 宣布发生数据泄漏，该泄漏事件危及 140 万用户的信用卡等个人信息，TripAdvisor 股价应声下跌 5%。

6.5.3. 并购交易过程中的数据合规

在并购交易过程中，无一例外都会涉及到数据的披露或交换，包括交易对手方的用户、客户、雇员等的个人信息。

而在一宗并购成功交割之前，尤其在尽调过程中，任何的数据披露或交换，都可能导致数据披露方违反网络安全法规、隐私保护法规和其根据隐私政策所负有的隐私保护义务，轻则触发民事侵权赔偿责任，重则触发刑事责任。例如，在尽职调查中，标的公司将向交易对手方以及双方的投行、律师、顾问、第三方供应商等等交易参与方披露大量的用户个人信息、敏感信息、保密信息等。即便通过虚拟数据室以及各类隐私保护措施，仍存在数据泄漏的风险。当标的公司对收购方进行反向尽调时，收购方同样面临以上风险。

因此，这一阶段的数据合规和隐私保护也尤为重要，并购交易中的任何一方在获取或使用个人信息时，均应采取适当安保措施，签署保密协议，并以仅供满足交易需求为限度进行。

6.5.4. 并购交割后的数据整合以及商业目的实现

Mergermarket 2017 年的调查报告显示，在数据为核心资产的行业并购中，半数以上的受访者表示在交割后发现数据合规问题，对数据合规的尽调不满意度达 16%。同时，导致交易失败的两大元凶之一，就包括数据合规问题。报告显示，有近 1/4 的收购因为数据合规出现问题而失败，这一比例和因财务、税务问题导致交易失败的比例一样多。

美国电信巨头 Verizon 收购 Yahoo 就是一个收购后数据资产整合失败的反面教材。Verizon 的收购尚未完成，Yahoo 已发出声明称曾在 2013 年 8 月被黑客袭击，导致超过 10 亿用户信息泄露，之后又披露，在 2014 年还有 5 亿用户数据被黑客窃取，交易几乎流产。最终 Verizon 的收购对价由 48.3 亿美金减至 44.8 亿美金，Verizon 同意和 Yahoo 平分两次数据泄露事件带来的成本。2017 年 6 月完成收购后，Verizon 没有采纳雅虎提交的报告，在外部安全专家的帮助下重新调查雅虎之前的数据泄露，最终发现 Yahoo 超过 30 亿的用户信息无一幸免全被泄露，Yahoo 面临着多起集体诉讼。此后，Yahoo 和美国在线（AOL）资产整合为 Oath，但这一整合显然是失败的，截止 2018 年底，Verizon 宣布 Oath 资产减至 46 亿美金。由此可见，“有毒”的数据资产，其历史遗留问题将持续存在相当长一段时间，并收购方造成重大的经济损失。

2018 年 4 月，美团全资收购摩拜，100%控股摩拜。据报道，美团认为城市中的所有生活场景都将涉及到出行需求，其预期摩拜所掌握的超短途出行市场数据，与美团的生活场景结合，将发挥一定的业务协同效应。2019 年 1 月，摩拜全面接入美团 App，双方通过一封“账号融合用户确认函”，告知用户将实现账号互通，允许美团共享用户在摩拜端的各类数据。企业发生收购等重大变更时，通过 app 弹窗获得用户确认数据融合的做法，可谓一种创新性的解决方案。

在数据驱动型的并购交易中，对于收购方而言，收购的终极目的是最大限度的发挥目标公司的数据价值，这就意味着，收购方应尽早对交割后的数据整合进行筹划，在收购完成后，由技术团队、法律团队以及业务团队通力合作，对交割后的过渡期及数据融合进行合规操作。

6.5.5. 并购涉及到的数据跨境问题

版权所有，翻印必究

经济全球一体化下，中国企业出海并购和外国（含外资）企业境内并购（合称“跨境并购”）时，境内（外）母公司和被并购的境外（内）公司不可避免会发生大量的数据跨境传输。

在跨境并购中，收购方与标的公司均需考虑在收购交割前数据交换是否符合其各自所在司法辖区的相关法规，收购方同时亦应提前对交割后标的公司开展业务时的相关数据合规和隐私保护的合规进行安排，如数据融合为收购之目的，则收购后的过渡期安排以及最终的数据整合的合规也是交割后的重中之重。

例如，我国通过《个人信息和重要数据出境安全评估办法（征求意见稿）》和《信息安全技术 数据出境安全评估指南(征求意见稿)》均对数据跨境传输作出了界定。2018 年 5 月施行的 GDPR，则限制从欧洲经济区向第三国跨境传输个人数据的行为，但欧洲委员会认定该第三国具有充分数据保护水平的除外，同时允许采取某些方式合法跨境传输数据。

此外，如数据资产涉及到国家安全，则会在政府监管部门对交易审批的环节折戟。以蚂蚁金服收购速汇金为例：2017 年 1 月，蚂蚁金服曾宣布拟收购美国上市公司、世界第二大汇款服务公司速汇金（MoneyGram），速汇金的汇款业务遍布全球，拥有 35 万个网点，直达全球 24 亿用户。并购速汇金不仅将美国划入蚂蚁金服业务全球推进的战略版图，而且将进一步助力蚂蚁金服在全球跨境支付的市场进行大举扩张。虽然为达成交易，蚂蚁金服此前已表示，速汇金的数据基础设施将会保留在美国，且用户信息将被加密或保存在美国安全的设施内，但最终仍未能获得美国外国投资委员会(CFIUS)的批准。速汇金与蚂蚁金服放弃合并计划，根据收购协议，蚂蚁金服还需要向速汇金支付 3000 万美金的“分手费”。虽然收购未获审批的原因未予公开，但 CFIUS 对于这一并购可能对美国金融关键信息基础设施安全的考虑不言而喻[10]。

版权所有 翻印必究

[10]https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial/u-s-blocks-moneygram-sale-to-chinas-ant-financial-on-national-security-concerns-idUSKBN1ER1R7

7. PRIVACY AND CYBERSECURITY ISSUES AND RISKS: EUROPEAN AND US PERSPECTIVE 隐私和网络安全问题和风险：以欧洲和美国为视角

本章作者：Antony Kim, Kolvin Stone, Aravind Swaminathan, Xiang Wang（王翔）, Jeff Zhang （张劲松）and Betty Louie（吕丽明）

7.1. INTRODUCTION 介绍

The EU is generally considered to be at the forefront in setting a high standard with regard to data privacy and the regulation of handling personal information. The latest EU-wide law regulating the collection and use of personal data is the General Data Protection Regulation 2016/679 ("GDPR").

欧盟通常被认为是在数据隐私和处理个人信息的监管方面树立高标准的最前沿地区。规范个人数据收集和使用的最新欧盟法律是《通用数据保护条例》（2016/679 号）（“GDPR”）。

Outside the EU, data privacy laws have been implemented in many jurisdictions that follow the European approach to privacy regulation. Some of these are directly modelled on the GDPR. Notably, the US, with the California Consumer Privacy Act ("CCPA"), has introduced sweeping changes to its privacy landscape which historically has taken a less comprehensive stance to privacy regulation, favoring a more limited, sectoral approach.

在欧盟之外，许多司法管辖区都实施了数据隐私法，这些法律都遵循欧洲的隐私监管方法。其中一些是直接在 GDPR 上建模的。值得注意的是，美国通过《加利福尼亚州消费者隐私法案》（“CCPA”）对其隐私领域监管进行了全面的改革，历史上，美国对隐私监管的态度曾不够全面，更偏向于采用更有限的部门监管方法。

Section A of this article describes the European approach to data privacy in more detail, specifically the requirements of the GDPR, and in this context details what organizations operating internationally should be doing in practice to improve their data privacy compliance posture.

本文的第一部分更详细地描述了欧洲数据隐私保护方式，特别是 GDPR 的要求，并在此背景下详细说明了在国际上运营的企业应该在实践中如何改进其数据隐私合规性。

Though there are clear overlaps between data privacy and cybersecurity, the latter is an increasingly important subject and should be considered a standalone topic in its own right. The United States is widely considered to be the leader with regard to cybersecurity maturity and sophistication – both

in terms of regulation and enforcement and in terms of organizations' approach, preparedness and risk management efforts.

虽然数据隐私和网络安全之间存在明显的重叠,但后者是一个越来越重要的主题，应该被视为一个独立的主题。无论是在监管和执法方面，还是在企业采用的方式、准备和风险管理方面，美国都被广泛认为是网络安全成熟度和复杂程度方面的领先国家。

Section B of this article discusses some practical steps that organizations can take to reduce the risk of incurring cyber-enforcement. While these are written from a US-perspective, the general concepts are applicable globally.

本文的第二部分讨论了企业可以采取的一些实际步骤,以降低引发网络执法的风险。虽然这些是从美国的角度编写的，但一般概念在全球范围内适用。

As a practical matter, any Chinese business operating internationally should therefore look at a privacy compliance programme that is orientated around EU concepts and cybersecurity programme that leans towards US principles. In this way, businesses in China will be well placed to meet best practice and in a better position to comply with applicable laws in all the markets which they are active.

实际上,任何在国际上经营的中国企业都应该考虑一个以欧盟概念和网络安全计划为导向的隐私合规计划，同时该计划应倾向于美国的原则。通过这种方式，中国企业将能够很好地达到最佳实践标准，并能够更好地遵守他们所活跃的所有市场的适用法律。

7.2. DATA PRIVACY 数据隐私

The GDPR came into force in May 2018 and represented a major overhaul of the EU data protection landscape.

GDPR 于 2018 年 5 月生效，代表了对欧盟数据保护格局的重大改革。

Many of the GDPR requirements (described below) complement good data governance. They help organizations to more systematically plan, track, and manage the various types of data collected, where data is stored, how data is shared, and how data is processed. This is important as organisations are increasingly data-driven, relying on processing large amounts of data using innovative technologies that transform, augment, and transfer data around the world.

许多 GDPR 要求（如下所述）共同组成了良好的数据管理方式。它们可以帮助企业更系统地规划，跟踪和管理收集各种类型的数据，以及数据存储，数据共享方式和数据处理方式。这一点非常重要，因为企业越来越倾向于数据导向的运营方式，依赖于使用创新技术处理大量数据，这些技术可以在全球范围内转换，扩充和传输数据。

版权所有 翻印必究

Perhaps more fundamentally, compliance with GDPR will be mandated by EU-based customers, business partners, and regulators. Therefore, as a practical matter, any company that does any amount of business in the EU must assess, calibrate and implement GDPR-compliance measures to mitigate against disruption to its European business endeavors.

也许更根本的是，欧盟客户，业务合作伙伴和监管机构将要求企业遵守GDPR。因此，作为一个实际问题，任何在欧盟开展业务的公司都必须评估、实施 GDPR 合规措施并使其标准化，以减少对其欧洲业务活动的干扰。

7.2.1. Main features of the GDPR GDPR 的主要特征

- *Principle-based.* The GDPR is largely principle-based. There are several core principles that "controllers" (organizations that decide how data is used) must abide by when collecting or handling personal data (meaning any information relating to an identifiable individual, which includes but is not limited to, employees, customers, shareholders, service providers and business partners).

- *以原则为基础。*GDPR 主要以原则为基础。收集或处理个人数据（即与可识别个人有关的任何信息，包括但不限于员工，客户，股东，服务供应商和商业伙伴）时，“控制者”（决定如何使用数据的组织）必须遵守几项核心原则。

  The principles dictate that personal data must be: processed fairly and transparently; collected and used for specifically disclosed purposes; accurate and kept up to date; processed securely; and not stored for longer than is necessary.

- *原则规定个人数据必须:* 公平，透明地处理;收集并用于特定公开的目的;准确并保持是最新的;安全处理;并且没有储存超过必须要的时间。

- *Extraterritorial effect.* The GDPR considerably expands the territorial reach of EU data protection law such that it will apply to organizations outside the EU where (i) an EU resident’s personal data is processed in connection with goods/services offered to them; or (ii) the behavior of individuals within the EU is monitored.

- *域外效力。*GDPR 大大扩展了欧盟数据保护法的地域范围，使其适用于欧盟以外的组织，即（i）向欧盟居民提供商品/服务从而收集信息的企业；或（ii）监督欧盟境内个人行为的企业。

- *Increased scope.* While the previous data protection rules applied exclusively to controllers, the GDPR applies to controllers and, in relation to certain compliance requirements, "processors" (organizations that process personal data on behalf of a controller).

- *扩大范围。*虽然以前的数据保护规则仅适用于控制者，但 GDPR 在适用于控制者的同时，就某些合规性要求而言，也适用于“处理者”（代表控制者处理个人数据的组织）。

- *Higher sanctions.* Potential sanctions are considerable under the GDPR. For certain breaches, organizations could be subject to fines of up to €20 million or 4% of worldwide revenue. In addition, collective actions filed by, for example, consumer associations, will be facilitated which will significantly increase data protection-related litigation.

- *更严重的处罚。*根据 GDPR，可能发生的处罚金额是很高。对于某些违规行为，企业可能会被处以高达 2000 万欧元的罚款或全球收入的 4％。此外，GDPR 还将促进由消费者协会提出的集体诉讼，这将大大增加与数据保护相关的诉讼。

- *New and enhanced rights for individuals.* The GDPR extends rights of individuals that existed under the previous data protection rules and grants new rights, namely the right to be forgotten, the right to restriction of processing and the right to data portability.

- *新的和强化的个人权利。*GDPR 扩展了先前数据保护规则下存在的个人权利，并赋予了个人新的权利，即被遗忘的权利，限制处理的权利和数据可移植性的权利。

- *Increased compliance obligations for controllers and processors.* In addition to the data protection principles set out above, there are specific obligations that organizations must comply with. These obligations and typical remediation activities are set out below.

- *控制者和处理者更高的合规义务。*除上述数据保护原则外，企业还必须遵守具体义务。这些义务和典型的弥补措施如下。

7.2.2. Key compliance obligations and typical remediation activities 核心合规义务和典型的弥补措施

- *Transparency requirements*. Controllers are required to provide certain information to individuals at the time their data is collected. This includes information on how the data will be processed, with whom it will be shared, how long it will be retained and the relevant legal basis.

- *透明度要求。*控制者需要在收集数据时向个人提供某些信息，包括有关如何处理数据，与谁共享数据，保留数据以及相关法律依据的信息。

  Generally, this requires a degree of information-gathering to ascertain the categories of data being processed and to determine the legal basis for processing, etc., as well as drafting and updates to customer-facing and employee-facing privacy policies.

通常，这需要一定程度的信息收集，以确定正在处理的数据类别，确定处理的法律依据等，并且起草和更新面向客户和面向员工的隐私政策。

- *International transfer rules*. Transfers of personal data from the EU to certain countries outside of the EU are generally restricted. This is subject to various exemptions, e.g., the use of EU Model Clauses (special contracts approved by the EU Commission).

- *跨境转移规则*。从欧盟向欧盟以外的某些国家/地区转移个人数据通常受到限制。但也有很多豁免规则，例如欧盟示范条款（EU Model Clauses，欧盟委员会批准的特殊合同）的使用。

  Typically, this obligation requires a level of information gathering to identify internal and external international transfers taking place and putting in place appropriate safeguards. Note that an "international transfer" in this context includes the mere viewing of personal data from a country outside the EU, for example, through a cloud-based service.

  通常，这项义务需要收集一定程度的信息，以确定正在进行的内部和外部国际转移并实施适当的保障措施。请注意，在此提到的“国际转移”包括仅从欧盟以外的国家查看个人数据，例如，通过基于云服务查看个人数据。

- *Compliance and accountability*. The GDPR concept of "accountability" means that controllers must be able to demonstrate they are in compliance with the data protection principles (described above).

- *合规性和问责制*。GDPR 的“问责”概念意味着控制者必须能够证明它们符合数据保护原则（如上所述）。

  In practice, this means organizations should have in place a data governance framework, a suite of privacy and related policies and procedures, and mechanisms for training/audit/enforcement so as to document their ongoing compliance.

  在实践中，这意味着组织应该建立数据治理框架，一套隐私和相关政策和程序，以及培训/审计/执行机制，以记录其持续的合规性。

- *Security and breach notification*. Both controllers and data processors must protect personal data using appropriate technical and organizational security measures. If a data breach occurs involving personal data, in certain circumstances, data controllers must notify the relevant EU data protection regulator and the affected individuals within a very short time frame (72 hours). There is a corresponding obligation on data processors to notify the data controller.

版权所有 翻印必究

- *安全和泄露通知*。控制者和数据处理者都必须使用适当的技术和组织安全措施来保护个人数据。如果发生个人数据的数据泄露，在某些情况下，数据控制者必须在很短的时间内（72 小时）通知相关的欧盟数据保护监管机构和受影响的个人。数据处理者也有相应的义务通知数据控制者。

  Organizations may need to implement more sophisticated systems for detecting breaches and establish / update policies and procedures (e.g., Incident Response Plans) to ensure reporting is completed within the strict time limit.

  企业可能需要实施更复杂的系统来检测违规行为并建立/更新政策和程序（例如，事件响应计划），以确保在严格的时间限制内完成报告。

- *Service providers*. The GDPR imposes certain requirements on data controllers that wish to appoint service providers to process personal data on their behalf. Essentially, controllers must only use service providers providing sufficient guarantees as to their security.

- *服务供应商*。GDPR 对希望指定服务供应商代表他们处理个人数据的数据控制者提出了某些要求。从本质上讲，控制者仅能够使用服务供应商以提供足够的安全保障。

  Compliance with this requirement is usually achieved by implementing an appropriate vendor risk assessment procedure – which typically involves, at a minimum, upfront due diligence, contracting, periodic review/assessment/audit, and termination procedures. The GDPR is also prescriptive as to certain clauses that must be contained in the written agreement between the controller and service provider (processor); customer and vendor standard contracts usually need to be updated to reflect this.

  达到该等要求通常通过实施适当的供应商风险评估程序来实现——该程序通常至少包括前期尽职调查，合同制定，定期审查/评估/审计和终止程序。GDPR 还规定了控制者和服务提供者（处理者）之间的书面协议中必须包含的某些条款，客户和供应商标准合同通常需要更新以反映这一点。

- *Records of processing activities*. Under the GDPR, data controllers and data processors in certain circumstances will be required to develop and maintain detailed records of their data processing activities, and such records must be provided to EU data protection regulators on request.

- *收集行为记录*。根据 GDPR，数据控制者和数据处理者在某些情况下将需要开发和维护其数据处理活动的详细记录，并且必须根据要求向欧盟数据保护监管机构提供此类记录。

版权所有 翻印必究

This obligation likely requires data mapping and related information gathering activities, as well as potential technology/tools to assist in recordkeeping.

这项义务可能需要数据映射和相关的信息收集活动，以及协助记录保存的潜在技术/工具。

- *Governance and appointing a Data Protection Officer*. Depending on the type of processing being undertaken, controllers and processors may have to appoint a statutory Data Protection Officer ("DPO"). DPOs have specific duties under the GDPR which include contributing to data protection audits and conducting employee training.

- *管理和指定数据保护官*。根据正在进行的数据处理类型，控制者和处理者可能必须指定一名法定数据保护官（“DPO”）。DPO 在 GDPR 下具有特定的职责，包括参与数据保护审计和进行员工培训。

Typically, analysis is undertaken to determine and document whether a DPO is required and, if so, whether a single DPO can be appointed for the entire group where the organization is a multinational.

通常来说，企业需要进行分析以确定和记录是否需要 DPO，以及如果需要 DPO，是否可以为跨国组织整体指定同一个 DPO。

* * *

The specific activities an organization will need to undertake with a view to GDPR compliance will depend on a number of factors, including: its exposure to the GDPR; and the nature and volume of personal data that is handled by the organization and the corresponding risk.

企业为了遵守 GDPR 而需要开展的具体活动将取决于多种因素，包括：其接受 GDPR 规制的程度;以及企业处理的个人数据的性质和数量以及相应的风险。

The starting point for most companies, however, is to assess the changes it will be required to make to its present approach to privacy. This should involve an initial high-level assessment of:

然而，大多数公司的出发点是评估其目前隐私政策所需的变化。这应包括对以下方面的初步高层面评估：

- whether and which of its operations are going to be subject to the GDPR;

- 其运营是否以及哪些业务将受 GDPR 的约束;

- reviewing the data the organization collects, how it uses that data and with whom it is shared; and
- 审查企业收集的数据，如何使用该数据以及与谁共享数据；和
- its current maturity as regards its privacy compliance in order to identify gaps and remediation activities.
- 目前其在隐私合规方面的成熟度，以确定差距和补救措施。

Undertaking this assessment and embarking on remediation activities typically requires input from various business functions – individuals from legal, compliance, risk, IT and IT security and marketing are often good candidates to be involved.

进行此评估并着手进行补救措施通常需要来自各种业务职能部门的投入——包括法律，合规，风险控制，IT 和 IT 安全以及市场部门，这些都是应该包括在内的合适的参与者。

Finally, bear in mind that the GDPR may require significant changes to IT systems and business processes. Companies will therefore need support and sponsorship from senior management that should be involved as early as possible.

最后，请记住，GDPR 可能要求对 IT 系统和业务流程进行重大更改。因此，公司需要尽可能早地获得高级管理层的支持和帮助。

7.3. CYBERSECURITY 网络安全

In the cybersecurity realm, the core risk management issue is typically around calibrating investments in security to align with properly identified threats and vulnerabilities. This requires a holistic view drawn from key stakeholders across departments and disciplines. It also warrants tough debate on enterprise priorities and resources. Companies rarely get it 100% right. But they enhance their chances of doing so through structures and processes that account for the critical interplay between Governance (input and accountability), Operations (practical business considerations and capabilities), and Controls (technical, physical and administrative) – in that order.

在网络安全领域，核心风险管理问题通常围绕着校正安全方面的投入，以应对经适当识别的风险和漏洞。这需要从跨部门和跨学科的核心利益相关者那里获得全面的观点，还需要就企业的优先事项和资源展开激烈讨论。企业很少能做到 100%正确，但他们通过管理（输入和责任）、运营（实际业务和能力）和控制（技术、实体和管理）之间相互作用的结构和流程来提高实现这一目标的机会。

版权所有 翻印必究

Ultimately, the goal is clear: to appropriately assess and mitigate risk to the enterprise and its key stakeholders. Unfortunately, that risk increasingly includes the potential for enforcement by a regulatory agency and/or a private action. Nearly every US state and federal agency has cybersecurity at the top of its agenda. And statutes such as the California Consumer Privacy Act of 2018[11]portend a next-generation of laws that will inject *statutory* breach damages into the mix – ostensibly eliminating the need to show any actual harm to consumers, similar to other statutes with unbalanced punitive consequences like the TCPA.[12]

最终，目标很明确：适当评估和降低企业及其核心利益相关者的风险。不幸的是，这种风险越来越多地包括潜在的监管机构执法和/或私人诉讼风险。几乎每个美国州和联邦机构都将网络安全置于首位。诸如 2018 年《加利福尼亚州消费者隐私法案》等法规预示着下一代法律将会把法定违约赔偿金纳入 - 表面上消除了消费者需要证明任何实际伤害的必要性，类似于其它具有不平衡惩罚性后果的法规，如 TCPA。

Substantial fines and penalties, brand and reputational damage, and a host of other liabilities, including for directors and officers, are squarely on the table for the foreseeable future.

在可预见的将来，大量罚款和处罚、品牌和名誉损害以及包括董事和高管在内的许多其它责任将会出现。

Against this backdrop, while there is no such thing as perfect security, there are some steps that make perfect sense. We have set out below seven actions that can help an organization.

在此背景下，尽管没有绝对的安全，但是一些步骤非常有意义。下面我们列举了可以帮助企业的七项行动。

7.3.1. Effective Vendor Management 有效的供应商管理

It has never been more important to diligently vet, onboard, monitor and audit critical third-party service providers and vendors. These third parties exist to make life easier, more efficient and more innovative and to help businesses better serve their customers. To do so, they often have access to, ingest and store tremendous amounts of data for various processing purposes. Given this reality, it is hardly surprising

[11] The CCPA provides that any consumer whose non-encrypted or non-redacted personal information is subject to unauthorized access and exfiltration, theft or disclosure due to security failures on the company's part can sue "to recover damages in an amount not less than $100 and not greater than $750 per incident or actual damages, whichever is greater." Cal. Civ. Code § 1798.100, *et seq.*
CCPA 规定，任何未加密或未编辑的个人信息由于公司安全故障受到未经授权的访问和泄露、被盗或泄露的消费者可以起诉"就每一个事件获得两者孰高者的赔偿：（1）不低于 100 美元、不高于 750 美元；或者（2）实际损害。"加州民法典第 1798.100 条等。

[12] The Telephone Consumer Protection Act (TCPA) provides a private right of action for "actual monetary loss from such a violation [or] $500 in damages for each such violation, whichever is greater." 47 U.S.C. § 227(b)(3) (also providing for trebling of damages if a court finds willful or knowing violations).
《电话消费者保护法（TCPA）》规定了"违法行为的实际金钱损失，或每次违法 500 美元的损失，以较高者为准"的私权救济权利。美国法典 47 款第 227(b)(3)条（也规定了如果法院认定故意或明知违法行为，则为三倍赔偿）。

that vendor-attributed data breaches are increasingly common. A recent study by Soha Systems found that 63 percent of data breaches may be directly or indirectly related to third-party access by contractors and suppliers.[13] And while there are certainly examples of bad press and enforcement activity against a service provider who suffers a data breach, by far, the rule is that the company bears the brunt of its service provider's cyber-mistakes and mishaps. Continued corporate migration to the cloud, and the growth in outsourcing generally, set the stage for significant third-party risk going forward.

对重要的第三方服务商和供应商进行尽职调查、跟踪、监督和审计非常重要。这些第三方的存在是为了让生活更简便、高效，更具创新性，并帮助企业更好地服务客户。要做到这一点，他们通常为各种处理目的访问、摄取并存储大量数据。考虑到这一现实，归咎于供应商的数据泄露越来越普遍。Soha System 最近的一项研究发现，63%的数据泄露都可能与第三方承包商和供应商直接或间接相关。尽管确实有针对数据泄露的服务供应商的负面新闻和执法活动，但是到目前为止，公司首当其冲地承受着因服务供应商网络错误和事故产生的影响。企业不断向云端迁移以及外包业务的增长，为重大第三方风险埋下了隐患。

Vendor management can impose significant costs, and we are not advocating the outsourcing of vendor management to yet another service provider (e.g., companies that offer website/online scanning technology). Rather, we offer three tips on less notorious, but (in our experience) effective risk mitigation moves that counsel might consider vis-à-vis third parties:

供应商管理可能会带来巨大的成本，我们并不主张将供应商管理外包给另外一个服务提供商（例如，提供网站/在线扫描技术的公司）。相反，我们提供了三条不那么令人厌恶但（根据我们的经验）律师可能会考虑的应对第三方的有效降低风险的建议：

- *Define "Breach" Strategically, Address Cooperation, and Seek a No-Past-Breach Rep*: In the US, the scope of notifiable data breaches is actually quite narrow as only certain types of data and certain circumstances trigger mandatory notification regimes. In vendor contracts, companies should consider what types of cyber security events or incidents matter in terms of managing their risk, and negotiate for definitions consistent therewith. Moreover, in our experience, companies and their vendors must cooperate with each other when a cybersecurity incident occurs that affects them both. When third-party breaches happen, regulators not only look at the security commitments

[13] Soha Systems, "Third Party Access Is A Major Source of Data Breaches, Yet Not An IT Priority," (April 2016) (online survey of over 219 IT and Security C-Level Executives, Directors and Managers). Soha Systems，"第三方接触是数据泄露的主要来源，但仍然还没有成为 IT 的重点工作"，（2016 年 4 月）（对 219 家 IT 和 C-安全级别公司的高管、董事和经理的在线调查）。

that a company obtained from the vendor, but also the speed and quality of information and cooperation that the company obtains from the vendor to help more quickly and effectively mitigate harm to any impacted consumers. Finally, we have found that it can be very helpful to include a draft contractual rep that the vendor is not aware of facts or circumstances suggesting a past "breach" (defined, as discussed above). This type of rep has two benefits. First, it usually prompts a discussion with the vendor around different types of incidents that the vendor has experienced, and whether or not they are covered by the rep. Second, because many breaches trace back to hacks and other events that occurred many months or even years ago, a no-past-breach rep can provide significant leverage should the rep turn out to be untrue.

- *从战略上定义"泄露"，解决合作问题，获得"无数据泄露历史"的陈述：*在美国，需通知的数据泄露范围实际上相当狭窄，因为只有某些类型的数据和某些情况会触发强制通知制度。在供应商合同中，各公司应考虑哪些类型的网络安全事件对风险管理很重要，并就与之一致的定义进行协商。此外，根据我们的经验，当发生影响公司和供应商双方的网络安全事件时，他们必须相互合作。当第三方数据泄露行为发生时，监管机构不仅要查看公司从供应商处获得的安全承诺，还要查看公司从供应商处获得的信息和合作的速度和质量，以帮助更快、更有效地减轻对任何受影响消费者的伤害。最后，我们发现合同草案中的陈述条款——表明供应商不知道过去"数据泄露"的事实或情况（定义见上文讨论）非常有帮助。这种类型的陈述有两个好处。首先，它通常会提示与供应商讨论供应商遇到的不同类型的事件，以及它们是否被陈述条款覆盖。其次，由于许多漏洞可追溯到几个月甚至几年前发生的黑客和其他事件，因此，如果陈述是不真实的，"无数据泄露历史"的陈述可对公司提供重要的筹码。

- *When Bargaining Power is Unequal, Implement Compensating Controls*: In many situations, a service provider is so large, powerful and essential, that companies are unable to negotiate for customized contractual protections. In these situations, counsel are well advised to work with their clients to identify and implement compensating controls. This can be as simple as turning on a multi-factor authentication option that the vendor offers, or as complex as implementing supplemental encryption strategies.

- *当谈判能力不平等时，实施补偿控制：*在许多情况下，服务供应商是十分强大和重要的，公司无法与其谈判特别定制的合同保护。 在这些情况下，建议律师与客户合作，以确定并实施补偿控制。 这可以像打开供应商提供的多因素验证选项一样简单，也可以像实现补充加密策略一样复杂。

- *Exercise Your Audit Rights*: In our experience, when regulators investigate a breach attributable to a service provider, the fact that the

company had a contractual *right* to audit compliance, is becoming less and less acceptable. Regulators want to see more. Counsel should take time to identify critical vendors and to the extent no audit process is in place, consider the possibility of some (any) checks on whether vendors are living up to their security commitments. And as regulatory requirements and expectations evolve, they should be reflected in both vendor management practices as well as in updated contractual provisions.

- *行使您的审计权利：*根据我们的经验，当监管机构调查可归因于服务供应商的违规行为时，公司拥有审计合规的合同*权利*的事实正变得越来越难被接受。 监管机构希望看到更多。 律师应该花时间确定关键供应商，并且在没有审计程序的情况下，考虑是否可以对供应商是否履行其安全承诺进行一些（任何）检查。 随着监管要求和期望的发展，它们应该反映在供应商管理实践以及更新的合同条款中。

7.3.2. Cyber Diligence and Corporate Transactions 网络安全尽调与公司交易

According to a 2016 New York Stock Exchange and Veracode survey,[14] 22% of directors said that they would *not* acquire a company that had experienced a high-profile data breach.

根据 2016 年纽约证券交易所和 Veracode 调查结果，22%的董事表示，他们不会收购曾高调遭受数据泄露的公司。

It is important to note that comprehensive diligence on all aspects of cybersecurity is often impractical and unrealistic. M&A transactions, for example, typically involve multiple suitors competing for the same target. Compromises and concessions are part of negotiating a complex deal. Timeframes are tight. Resources are limited. It is also exceedingly difficult to find an opening, or willingness, to perform the type of technical penetration tests and compromise assessments, and compliance reviews, that a buyer might otherwise pursue.

值得注意的是，对网络安全的各个方面进行全面尽调往往是不切实际的。 例如，并购交易通常涉及竞争同一目标的多个竞争者。 妥协和让步是谈判复杂交易的一部分。 时间紧迫。 资源有限。 找到买方追求的开放或愿意进行技术渗透测试和折衷评估以及合规性审查也是非常困难的。

Below, we offer some insights from the buyer's perspective that, in our experience, have helped to get at the heart of the issue:

[14] NYSE/Veracode, *Cybersecurity and the M&A Due Diligence Process*, Survey Report (2016).
纽约证券交易所/Veracode，*网络安全和并购交易尽职调查程序*，调查报告（2016）。

下面，我们从买方的角度提供一些见解，根据我们的经验，这有助于解决问题的核心：

- *Non-Public Cyber Incidents*: Because most cyber-attacks and data breaches do not trigger mandatory notification rules, as with the vendor discussion above, it is important to understand whether the target has experienced broadly-defined data "incidents" (e.g., ransomware, DDOS, data corruption/loss, theft of proprietary information or trade secrets) and the associated remediation strategy and results. Equally important is assessing any history of non-compliance fines or penalties that are not public, such as those involving the card brands and PCI.

- *非公共性的网络事件：*由于大多数网络攻击和数据泄露不会触发强制通知规则，如上面的供应商讨论所述，了解目标公司是否经历了广泛定义的数据"事件"（例如，勒索软件，DDOS，数据损坏/丢失，专有信息或商业机密被盗）以及相关的补救策略和结果。同样重要的是评估任何非公开的违规罚款或处罚历史，例如涉及信用卡品牌和支付卡行业（PCI）等。

- *Validating Publicly Made Representations*: As discussed further below, what a company publicly says about cybersecurity in its Privacy Policy, Terms of Use, or even marketing materials, is classic fodder for regulator and class action complaints. Opposing parties point to allegedly "deceptive" statements that customers and consumers relied on to their detriment. These are low hanging fruit for enforcement cases and can be challenging to defend.

- *验证公开做出的陈述：*正如下面进一步讨论的那样，公司在其隐私政策、使用条款甚至营销材料中公开谈论的网络安全内容，是监管机构和集体诉讼投诉的经典素材。反对者指出客户和消费者依赖了对他们不利的"欺骗性"言论。这些都是垂手可得的执法案件，并且可能难以抗辩。

- *Reverse Vendor Management*: Where the target is a service provider/vendor, the buyer should assess whether and how the target anticipates and addresses (including through contractual protections) its own customers' compliance requirements. This is particularly important where the target's customer base or data-types are highly regulated – e.g., financial services; healthcare; defense contracting; PCI/payment card data; children's data; data subject to prescriptive rules such as the GDPR.

- *反向供应商管理：*如果标的公司是服务商/供应商，买方应评估目标是否以及如何预测和解决（包括通过合同保护）其自身客户的合规性要求。 在目标客户群或数据类型受到高度监管的情况下（例如金融服务、卫生保健、国防承包、PCI /支付卡数据、儿童数据、受制于 GDPR 等规范性规则的数据），这一点尤其重要。

7.3.3. Deploying Privilege where Appropriate 适当使用律师-客户特权保护

Legal counsel's role in cybersecurity has evolved significantly over the past 10-15 years. While lawyers traditionally were called in to reactively handle lawsuits and regulatory actions, they now contribute to shaping proactive cyber planning, assessment and resiliency efforts, including incident response.

在过去 10-15 年间，法律顾问在网络安全方面的作用发生了重大变化。虽然传统上律师被要求反应性地处理诉讼和监管行动，但现在他们有助于制定主动性的网络安全规划、评估和防灾工作，包括事件响应。

The fact that case law is now developing on the issue of cyber-related privilege, makes clear that lawyers are increasingly playing a meaningful role in this space. However, there are some key lessons learned that should be considered for both in-house and outside lawyers:

判例法目前正在发展与网络安全相关的律师-客户特权问题，这表明律师在这一领域的作用越来越重要。但是，内部律师和外部律师都应考虑一些重要的经验教训：

- *Non-Breach Cybersecurity Audits or Assessments*: Counsel should carefully manage client expectations and differentiate between audits or assessments that are routine "normal business functions" versus those that are truly directed by counsel for purposes of rendering legal advice. Proactive (pre-breach) work always involve tradeoffs between remediation and resources (i.e., tough choices are made about what to do now versus put-off until later). Debates like these can generate prejudicial documents. Counsel should seek to shield them from potential discovery to the extent they are properly subject to the privilege.

- *未泄露网络安全审计或评估*：律师应认真管理客户期望，并区分日常"正常业务职能"的审计或评估与法律顾问为提供法律咨询而真正指导的审计或评估。主动（泄露前）工作总是涉及补救和资源之间的权衡（即，对现在要做到事情和推迟到以后做的事情做出艰难选择）。像这样的讨论会产生不利影响的文件。律师应设法在适当受到律师-客户特权保护的情况下，从潜在的证据开示程序中保护它们。

- *Deploy Privilege Through "Drafts"*: Even if a cyber audit or assessment might not qualify for attorney client privilege or work product protections, there are strategies to shield the debate and decision-making from disclosure. For example, emails to counsel that discuss the pros/cons of an audit, items to investigate or focus on,

tradeoffs and compromises, priorities and key risks are legitimately privileged. Another practice is to conduct oral read-outs before things are reduced to writing.

- *通过“草案”设置特权保护:* 即使网络审计或评估可能不符合律师-客户特权或工作成果保护的条件，也仍然有屏蔽该等讨论和决策而不被泄露的策略。例如，向律师发送电子邮件，讨论审计的利弊、调查或关注的事项、权衡和妥协、优先事项和核心风险都是合法的受到律师-客户特权保护的。另一种做法是在上述事项成为书面文件之前进行口头陈述。

- *Engaging Public Relations (PR) Firms*: The typical incident response playbook contemplates PR/crises communications teams being engaged through counsel for privilege purposes. However, in the US there is mixed case law on this point. For example, some courts have distinguished between "standard" public relations services aimed at preserving a public image or reputation versus PR firm communications or work product that are directly related to legal advice or litigation strategy.[15]

- *聘用公关（PR）公司:* 为获得律师-客户特权目的，典型的事件响应手册考虑了通过律师引入公关/危机沟通团队。 但是，在美国，关于这一点的案例法不一。 例如，一些法院区分了旨在保护公众形象或声誉的“标准”公共关系服务与公关公司与律师就法律咨询或诉讼策略直接相关的通讯或者工作成果。

7.3.4. Focus on Communications 关注沟通

In the wake of a data breach, companies must navigate a host of legal, risk and reputational landmines. However, perhaps nothing influences liability – and drives the appetite of public and private enforcers – more than the first *external communication* that a company makes about a cyber incident.

在数据泄露之后，公司必须处理大量法律、风险和声誉隐患。然而，也许没有什么比公司就网络事件的第一次*外部沟通*更能影响责任归置和推动公共和私人执法者的胃口。

In our experience, early brainstorming and coordination can help to reduce the risk that breach notifications catch company stakeholders by surprise when they are later quoted in legal briefs and court orders. In addition, we offer the following lessons learned that can be

[15] *Compare McNamee v. Clemens* (E.D.N.Y. 2013) (no privilege; PR firm only provided standard services not necessary in order to provide legal advice, and therefore disclosing documents to firm resulted in waiver) *and King Drug Co. v. Cephalon, Inc.* (E.D. Pa. 2013) (privilege applied; consultants preparing business and marketing plans were the client's "functional equivalent").
Compare McNamee 诉 Clemens (纽约东部地区法院 E.D.N.Y. 2013 年)（没有律师-客户特权；公关公司只提供了不是为提供法律咨询而必要的标准服务，因此公司向公关公司提供文件豁免掉了律师-客户特权）和 *King Drug Co. 诉 Cephalon, Inc.* (宾州东部地区法院 E.D. Pa. 2013 年)（可适用律师-客户特权；顾问准备业务和市场计划是其客户的“功能性相同工作”）。

included in every lawyer's next discussion with their communications colleagues:

根据我们的经验，早期的头脑风暴和协调有助于降低泄露通知在随后的法律简报和法院命令中被引用时，使公司利益相关者感到意外。此外，我们还提供了以下经验教训，可以包含在每个律师与其传播部门同事的下一次讨论中：

- *Early Announcements Can Be Risky*: To the extent that reputational and other considerations (e.g., leaks) demand early communications, organizations should be very careful in disseminating information too broadly (e.g., sending an e-mail alert to all employees about a potential security incident) or in over-disclosing to external stakeholders.

- *提前公告可能存在风险：*在声誉和其他因素（如走漏风声）要求提前沟通的情况下，企业应谨慎过度传播信息（例如，向所有员工发送有关潜在安全事件的电子邮件警报），或者过度向外部利益相关者披露信息。

- *One-Size-May-Not-Fit-All for Precautionary Messages*: It is critical to understand the nuances of the US state-specific notification requirements. Many states (including Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia and Wyoming) explicitly require that the reporting company include specific recommendations to consumers on risk mitigation, including encouragement to monitor credit reports. However, notwithstanding variations across state rules, a commonly accepted practice is for organizations to issue a standard notification that complies with substantially all of the states' various requirements (except Massachusetts), and supplement certain notifications based on state-specific requirements (e.g., instructions on contacting a specified state agency/regulator). This means that all of the various state-required language and disclosures are often provided to all individuals, even if not entirely applicable. Although they often reflect sound security practices that consumers should follow in any circumstance, organizations should recognize the risk in making risk mitigation recommendations, and consider whether to provide them only to consumers whose states' law explicitly requires it.

- *对于预防信息，一种标准可能不适用所有情况：*了解美国州法的特定通知要求的细微差别至关重要。许多州（包括夏威夷、密歇根、密苏里、北卡罗来纳、佛蒙特、弗吉尼亚和怀俄明州）明确要求报告公司向消费者提供有关减轻风险的具体建议，包括鼓励监测信用报告。然而，尽管各州的规则有所不同，一个普遍接受的做法是，企业发布一份基本上符合所有州的各种要求（马萨诸塞州除外）的标准通知，并根据州的具体要求补充某些通知（例如，关于联系指定的州政府机构/监管机构的说明）。这意味着，即使不完全适用，不同州要求的语言和披露通常都提供给所有人。尽管它们通常反应

消费者在任何情况下都应遵循的良好安全措施，但企业应认识到提出减轻风险建议的风险，并考虑是否只向特定州法律明确要求的消费者提供这些建议。

- *Carefully Describe Protective Measures*: Certain US state statutes require disclosure of the measures taken to contain, mitigate or minimize the incident. For example, Michigan directs that notifications "generally describe what the [company] providing the notice has done to protect data from further security breaches." Wyoming requires a description in general terms of "the actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches." Similar requirements exist in North Carolina, Vermont, Virginia and elsewhere. However, these types of statements have been used to infer the scope of individuals who were affected. Thus, although statutorily required, these cases demonstrate why organizations should thoughtfully articulate the containment/remedial measures taken in response to an incident.

- *认真描述保护措施：*美国某些州法规要求对所采取的控制、减轻和最小化事故的措施进行披露。 例如，密歇根州要求该通知"通常需要描述提供通知的[公司]为了保护数据免受安全漏洞进一步影响都做了哪些工作。"怀俄明州要求该通知一般性地描述"个人或商业实体为保护包含个人识别信息的系统免受进一步泄露而采取的行动。"北卡罗来纳州、佛蒙特州、弗吉尼亚州和其它州存在类似的要求。然而，人们已经可以通过这些声明的类型来推断事故中受影响个人的范围。 因此，尽管法律做出了这些要求，这些例子仍然显示了为何组织机构应该仔细地阐明为应对事故而采取的遏制/补救措施。

  - *Rigorously Analyze Voluntary Notifications*: In our experience, even if a cyber incident does not technically trigger a notification requirement, companies often "voluntary" notify affected parties. They do for a host of different reasons. We see counsel's role as helping stakeholders to assess the pros/cons of voluntary notification through decision trees that account for downside and upside (e.g., the likelihood that voluntary notice will enable customers to take meaningful self-help steps).

  - *严格地分析自愿通知：*根据我们的经验，即使网络事故从严格法律角度来讲不会触发通知要求，公司也经常"自愿"通知受影响的各方。他们这样做是出于很多不同的原因。我们认为律师的角色是帮助利益相关者通过可解释优缺点的决策树来评估自愿通知的利弊（其优点例如自愿通知使客户可能能够采取有意义的自助步骤）。

7.3.5. Don't forget about Privacy 别忽略隐私

A few years ago, the Federal Trade Commission wrote a blog post that highlighted key issues companies should expect to be asked about in cyber investigations. Among other things, the FTC explained that the agency looks at "privacy policies and any other promises the company has made to consumers about its security."[16] Indeed, most FTC cyber enforcement cases turn on allegations that a company made misleading statements regarding the type, strength, or even presence of, security measures associated with its product or services. Offending statements can appear in a variety of contexts, including privacy policies, terms of service, marketing materials, and even investor relations materials, just to name a few.

几年前，联邦贸易委员会（FTC）写了一篇博文，强调了公司在网络调查中应该被问及的关键问题。 据 FCT 解释，除其它事项外，FTC 着眼于"隐私政策以及该公司向消费者提供的有关其安全性的任何其它承诺。"事实上，大多数 FTC 网络执法案件的指控原因都是某公司就其产品或服务相关的安全措施的类型、强度甚至是否存在安全措施做出了误导性陈述。仅举几例，这些不合规的言论包括隐私政策、服务条款、营销材料、甚至投资者关系材料。

We offer the following tips for identifying potential privacy-related cyber exposure points:

我们提供以下提示以供识别可能导致隐私泄露的潜在风险点:

- *Check What Your Company Publicly States About Security*: Be thoughtful about the fine line between transparency that informs customers on the ways in which you collect, use, share, store and transfer data, and vague language or catch phrases, such as "industry standard security," "bank-level encryption" or "we do everything we can do to secure your data" that can land a company in hot water. Decide whether detailed statements about your plans, protocols, processes and tools are necessary and generate any value. Avoid overstating your security practices, or implying that a high level of security is applied across the board, if in fact it is applied in more limited circumstances (e.g., subsets of data; data in-transit versus at-rest; applied by the company but unknown for service providers).

- *检查公司就其网络安全性做出的公开声明:* 仔细考虑这个微妙的区别-即坦诚告知客户您收集、使用、共享、存储和传输数据的方式，还是用可将公司置于水深火热之中的模糊的语言或短语对其进行描述，例如"行业安全标准"，"银行级加密"或"我们尽最大努

[16] M. Eichorn, "If the FTC comes to call," Blog Post, *available at,* https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call (May 25, 2015).
M. Eichorn，"如果联邦贸易委员会 FTC 打电话来"，博客文章，在 https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call (2015 年 5 月 25 日).

力来保护您的数据”。您要确定是否需要详细陈述您的计划、方案、流程和工具和其是否会产生任何价值。避免夸大您的安全实践或暗示全面应用高级别安全性的措施（实际只应用在更有限的情况下）（例如数据子集;传输中的数据与静止的数据;由公司应用；但对服务提供商而言是未知的）

- *Regularly Refresh Assessments of Publicly Made Statements*: All external (consumer) facing representations should be reviewed no less than twice per year. Reviews should be accelerated as part of privacy-by-design processes any time new products or services will be deployed. Counsel should conduct these reviews as group exercises with mandatory participation by IT/InfoSec and Marketing/e-commerce (who often have first line-of-sight to new tools and technology being considered and deployed).

- *定期对公开声明进行更新评估：*所有面向外部（消费者）的陈述每年应评审不少于两次。作为隐私设计流程的一部分，当部署新产品或服务时，审核应该进行加速。律师以小组检查的方式进行这些审查，并必须要求有 IT /InfoSec 和市场营销/电子商务（这些员工经常对拟适用的新工具和新技术有第一手的想法）进行参与。

- *Consider Reasonable Security Disclaimers*: We regularly see privacy policies that trumpet claims like “Security Guaranteed” and “Bank Level Security” (often by non-financial services entities!). Given the shifting cyber threat landscape, virtually any assurance regarding security is susceptible to legitimate scrutiny. This is why many companies include blanket disclaimers that security measures may change, be unavailable from time to time, or even circumvented by sophisticated actors (e.g., “We cannot guarantee 100% security. No security is fail proof”). Competent judgment is required to strike a thoughtful balance: any legal benefits that disclaimer language may provide should be weighed against the PR/business impact of being viewed as shifting risk to the consumer. And even though disclaimers are not a panacea, they can at least provide arguments regarding what consumers should reasonably expect.

- *考虑合理的安全免责声明：*我们经常看到隐私政策宣称“安全有保障”和“银行级安全”（而这些声称通常由非金融服务实体做出！）。鉴于网络威胁的格局不断变化，几乎任何有关安全性的保证都容易受到合法性的审查。这就是为什么许多公司包括声称安全措施可能会改变的一揽子免责声明不时会无法使用，甚至被富有经验的参与者规避（例如，“我们不能保证 100％的安全性。没有完美无懈的绝对安全性”）。 需要有足够的判断才能达到一个深思熟虑的平衡: 免责声明可能提供的任何法律利益应该与将风险转移到消费者身上产生的公关/业务影响进行权衡。 尽管免责声明不是灵丹妙药，但它们至少可以提供关于消费者应该合理期望的论据。

7.3.6. Mind Your Directors and Officers 注意您的董事和高级职员

In-house counsel, and outside counsel who work with them, technically represent the company. They are fiduciaries to the corporate entity, which has as its highest authority, the Board of Directors. Accordingly, an important part of the general counsel's role is to provide sound legal compliance and legal risk mitigation advice to the Board.

内部法律顾问和与其合作的外部法律顾问严格来说是代表公司的。他们是公司实体的受托人。公司实体拥有最高权力机构即董事会。因此，总法律顾问工作的一个重要部分是为董事会提供合理的法律合规和减低法律风险建议。

While it is a new risk, cybersecurity falls squarely within the traditional "risk oversight" obligations of corporate Directors. Directors have fiduciary duties to act in good faith, and with care and loyalty, which, in the cyber context, includes directing Management to design, implement and enforce a robust cybersecurity compliance program. To effectively do so, Directors must be educated and informed about the company's risk profile, threat actors, and strategies to address that risk; they must receive regular briefings from Management and metrics to understand progress toward the desired state.

虽然网络安全是一种新风险，但它完全属于公司董事的传统"风险监督"义务。董事承担信义义务，以诚信、谨慎和忠诚行事。在网络语境中，这包括指导管理层设计、实施和执行强大的网络安全合规计划。为了有效地执行，董事必须接受培训并了解公司的风险状况、威胁行为者和应对风险的策略;他们必须定期收到管理层的简报，和以了解为达所需状态的进展情况的相关指标。

We offer three insights from the frontlines of governance work that we believe has the dual benefit of not only helping to mitigate risk for the company, but also helping directors and officers to fulfill their cyber-fiduciary duties:

我们从治理工作的前沿提供三个见解。我们认为这些见解这不仅有助于降低公司风险，还具有有助于董事和高级职员履行其网络安全信托义务的双重好处:

- *Practice with Your InfoSec Team*: While cyber risk is not "new," its high level of Board attention is certainly new. InfoSec teams, often for the very first time, are in the Board room, and responsible for educating the Board on the company's risk profile, vulnerabilities, current security state, and roadmap for remediation and sustained risk management. Accordingly, they need practice and guidance from

counsel (e.g., regulatory and litigation perspectives) to be most effective in communicating with the Board. Counsel's early involvement is particularly important when the Board will assume a more active role – for example, where InfoSec conducts a Board-level incident response tabletop, or discusses ransomware attacks and the issue of who in the company decides whether to pay.

- *和 InfoSec 团队一起练习：*虽然网络风险已经不是一个新话题，但董事会对其关注的高水平程度肯定是新的。 InfoSec 团队通常是第一次参加董事会会议，负责向董事会提供有关公司风险概况、漏洞、当前安全状态以及补救和持续风险管理路线图的培训。 因此，他们需要律师的实践和指导（例如，监管和诉讼的观点）才能最有效地与董事会沟通。 当董事会将扮演更积极的角色时，律师的早期参与就尤为重要 - 例如，当 InfoSec 设立董事会级别的事件响应桌面，或者讨论勒索软件攻击以及公司里谁来决定是否支付的问题。

- *Vertically Integrate InfoSec with the Governance/Disclosures Team*: From a governance perspective, many companies do not involve their InfoSec teams in the risk disclosures process and committee. Especially for public companies, lawyers can help to establish a channel for reporting cyber events, and the appropriate Board committee (whether the Audit, Risk, of even Cybersecurity Committee) can thereby gain experience around assessing events for disclosure filing purposes.

- *将 InfoSec 与治理/披露团队垂直整合：*从管理的角度来看，许多公司不会让他们的 InfoSec 团队参加到风险披露流程和委员会。特别是对于上市公司，律师可以帮助建立报告网络事件的渠道，相应的董事会委员会（无论是审计、风险甚至是网络安全委员会）都可以因此获得有关评估披露提交目的的事件的经验。

- *Implement Trading Blackout Protocol for Cyber Events*: Based on the 2018 SEC cyber guidance, lawyers should assess whether procedures are in place to determine whether implementing a trading blackout period while the company investigates and assesses the significance of a cyber incident is appropriate, and review insider trading policies to ensure they prohibit insiders from trading when in possession of material nonpublic information relating to cyber risks or incidents.

- *为网络事件实施交易暂停协议：*根据 2018 年美国证券交易委员会的网络安全指南，律师应评估是否有程序来确定在公司调查和评估网络事件的重要性时是否实施交易暂停期是适当的，并审查内幕交易政策，以确保他们在获知与网络风险或事件有关的重大非公开信息时禁止内部人员进行交易。

7.3.7. Assess Your Risk Assessments 评估您的风险评估

Cyber risk assessments come in dozens of flavors. They can involve enterprise or product level analyses, focus on people, processes, or technology (or all three), be limited to certain systems or all of them, and relate to the company or its service providers (or both). But what *all* risk assessments have in common is that they identify lots of "opportunities" for improvement. For that reason, both regulators and private plaintiffs demand them in discovery.

网络风险评估可以有几十种不同特点评估。 它们可以涉及企业或产品级别分析，关注人员、流程或技术（或全部三种），或仅限于某些系统或所有系统，并且与公司或其服务提供商（或两者）相关。 但*所有*风险评估的共同点是，它们确定了许多改进的“机会”。 出于这个原因，监管机构和私人原告都要求他们在证据开示阶段提供该等网络风险评估的证据。

For legal counsel, risk assessments are relevant and useful in a number of respects. For example, risk assessments can play a key role in helping to evaluate the vendor management program, as well as helping to assess the vendors' own security programs. They can also be leveraged to evaluate cyber or privacy issues related to an acquisition target; or leveraged by a target company to ready itself for acquisition or other major transaction (or even a cyber insurance underwriting). Risk assessments can also be used to benchmark a company's overall security program or elements of its (e.g., incident response) against regulatory requirements, industry standards/best practices, or customer requirements. In some cases, an enforcement agency may request a risk assessment in the aftermath of a breach, or as part of a settlement. Having a recent assessment already done in the ordinary course can go a long way in demonstrating diligence and mitigating regulatory scrutiny.

对于法律顾问而言，风险评估在许多方面都具有相关性和实用性。例如，风险评估可以在帮助评估供应商管理计划以及帮助评估供应商自己的安全计划方面发挥关键作用。 它们还可用于评估与收购目标公司相关的网络或隐私问题；或由目标公司利用以准备被收购或其它主要交易（甚至是网络安全保险承销）。 风险评估还可用于根据法规要求、行业标准/最佳实践或客户要求对公司的整体安全计划或其要素（例如事件响应）进行基准测试。 在某些情况下，执法机构可能会在企业违规后或作为和解的一部分要求其进行风险评估。 拥有一个最近依据正规流程进行的评估可以在很大程度上证明尽职程度和减轻监管审查。

As with any audit or assessment, the challenge for companies is prioritizing and executing on the remediation plan. While some companies have robust processes for identifying corrective actions, road-maps, milestones, and funding requirements, many companies

struggle – and thereby, unintentionally create an unfavorable paper trail and precedent.

与任何审计或评估一样，公司面临的挑战是对补救计划进行优先排序和执行。虽然一些公司拥有强大的流程来识别纠正措施、路线图、里程碑和资金需求，但许多公司都在还在为此挣扎——从而无意中产生了一个不甚有利的纸质证据和先例。

While it is certainly easy for outsiders to critique in hindsight, the tone and tenor of the allegations clearly set forth a roadmap for identifying key exposure points. We offer three thoughts on how lawyers might leverage cyber assessments to help proactively manage enterprise risk:

虽然外人很容易在事后进行批评，但指控的基调和大意清楚地提出了可以识别关键风险点的路线图。 我们就律师如何利用网络安全评估来帮助企业前瞻性地管理风险提出三点看法:

- *Focus on Repeat Items*: Lawyers should hone in on documented weaknesses, warnings and action items that continue to show up from audit to audit or assessment to assessment, particularly those that map to non-compliance with a specific law, regulation, or contractual requirement (e.g., PCI). Depending on their criticality and remedial potential (e.g., if fixes are reasonably available), these repeat items can form the basis for serious regulatory and private liability – particularly if any even arguably contribute to a future data breach. Of course, context is always relevant to assessing liability exposure. For example, remediation recommendations must be viewed in the context of whether the risk item was deemed "accepted risk" by the company; the probability of the risk event occurring is also relevant; and counsel should probe whether compensating controls exist to mitigate the risk item's criticality for prioritization purposes.

- *关注重复出现的事项:* 律师应该深入了解从审计到审计或评估到评估继续出现的记录在案的弱点、警告和任务项，特别是那些不遵守特定法律、法规或合同要求的案例 （例如 PCI）。根据其重要性和补救潜力（例如如果可以合理地获得修复），这些重复事项可能构成严重的监管和私权诉讼的基础——特别是如果有任何导致未来数据泄露可能的话。当然，背景总是与评估责任风险相关。 例如，必须在风险项是否被公司视为"可接受的风险"的背景下查看补救建议；风险事件发生的概率也是相关的；并且为了确定优先次序，律师应该调查是否存在降低风险项目的关键性的补偿性控制措施。

- *Deploy Privilege Via Emails and "Drafts"*: As discussed above, risk assessments are a double-edged sword – helping to *identify* security risks while simultaneously *creating* remediation risks for the enterprise.

Thus, it bears repeating that even if a cyber audit or assessment might not qualify for privilege or work product protections, there are strategies to shield legitimate debate and decision-making. Lawyers should be consulted *precisely* in situations where tradeoffs must be made between remediation and resources – as these choices often carry significant legal compliance, regulatory and litigation risk repercussions. Drafts of reports sent to counsel for legal advice, as well as emails and conversations that occur outside the four corners of an assessment, are almost always covered by the attorney client privilege.

- *通过电子邮件和"草稿"部署律师-客户特权信息:* 如上所述，风险评估是一把双刃剑——有助于*识别*安全风险，同时却又为企业*制造*补救风险。 因此需要重申的是，即使网络审计或评估可能不符合律师-客户特权或工作成果保护的资格，也仍然有用律师-客户特权保护合法讨论和决策的策略。 在必须在补救和资源之间进行权衡时，应该*准确地*在适时情况下咨询律师——因为这些选择通常对重大的法律合规性、监管和诉讼风险上产生后果。 律师-客户特权几乎总是涵盖向律师请求提供法律建议的报告草稿，以及在评估范围之外发生的电子邮件和对话。

- *Focus on Assessments That Are Tightly Linked to Strict Legal Requirements*: In our experience, risk assessments produce broad recommendations that cover a lot of ground, including actions that range from necessary to advisable to nice-to-have. Counsel should work with business and security teams to develop a defined schedule on the corporate calendar for conducting risk assessments in areas like Health Insurance Portability and Accountability Act ("HIPAA") and PCI that produce specific, targeted remediation recommendations. In addition to being able to identify specific issues, there is value in being able to demonstrate a culture of compliance should the company experience a public breach or regulator investigation.

- *着重于与法律要求紧密相关的评估*: 根据我们的经验，风险评估会提出广泛的建议，涵盖了包括从必要到可取以及"有了也好"的行动的很多方面。 律师应与业务和安全团队合作，在公司日历上制定明确的时间表以便在《健康保险可携性及责任法案》（"HIPAA"）和 PCI 等领域进行风险评估，从而可以制定具体的且有针对性的补救建议。 除了能够识别具体问题之外，在公司经历公共违规或监管机构调查时，能够证明合规文化是有价值的。

* * *

Cyber risk is constantly evolving and intensifying the enforcement risk that companies face from both regulators and private litigants. As lawyers are increasingly involved in proactive risk management, our hope is that at least some of the "easier" wins discussed in this

article allow counsel to add value to the process. Of course, there is never enough time, enough money or people to do everything. But prioritized, targeted work holds the best potential for mitigating cyber risk for the enterprise and its stakeholders.

网络风险不断发展，并加剧了公司面临监管机构和私人诉讼的执法风险。 随着律师越来越多地参与到主动风险管理中，我们希望至少在本文中讨论的一些“更容易”胜利的情形允许律师为风险管理的流程增加价值。 当然，企业从来没有足够的时间、金钱或人手来完成所有的事情。但优先且有针对性的工作对于减轻企业及其利益相关者的网络风险无疑是具有最大潜力的。

8. 企业应当采取哪些措施保障数据安全

本章作者：Kelvin Gao

8.1. 企业数据安全保护理念

每当我们与企业董事及高级管理人员交流时，越来越多的机会会谈及数据安全保护方面话题。他们通常会问：我们企业的数据安全保护措施是否有效？我们的工作思路和方向与目标是否一致？他们为能拨出足够的预算，从而建立拥有所需技能的团队以跟上最新的技术发展而殚精竭虑。尤其是当他们已经尽其所能地做好防范工作，他们依然担心会发生重大数据安全事件。但事实是，没有人可以独善其身，外部攻击窃取及内部恶意泄漏是我们时时面对的数据安全风险。随着企业数字化变革的不断快速推进，在数据价值迅速提升的同时，企业重要数据资产所面临的攻击面也在不断扩展，并延伸到了企业业务乃至企业生态链的方方面面。从而急剧加大了企业级数据保护的难度。传统的、被动式的数据安全防范通常以事后补救措施为主，已无法满足管理层对于企业数据安全的保护要求。数字化变革下的企业，需要建立一套“弹性”的数据安全防御机制，从事前“感知”，未雨绸缪，事中“抵御”，见招拆招，到事后“应对”，及时补救，全方位立体化地提升企业级数据安全防范水平。

版权所有 翻印必究

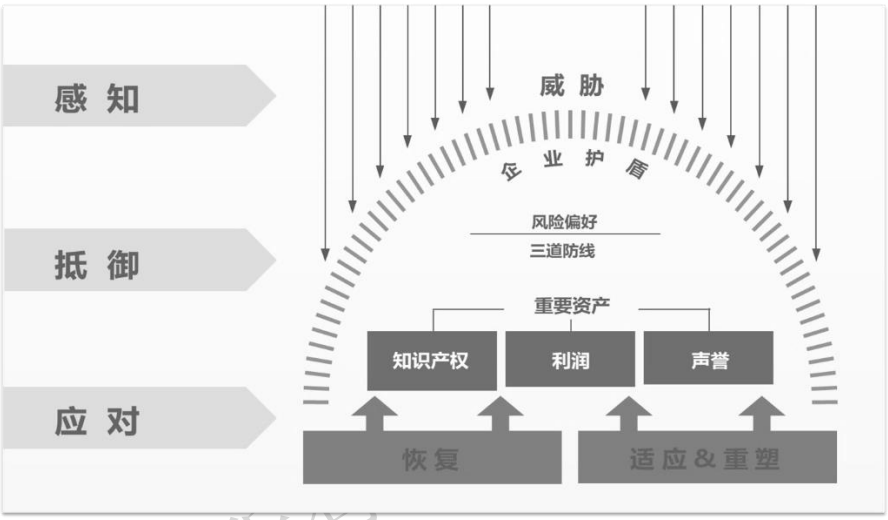


图 8.1 摘录自《安永第 19 届全球信息安全调研报告》

- 感知 - 首先，擦亮您的眼睛。您是否能看见正在向您网络防护边界靠近的外部攻击者？您的边界是否依然存在？如果您的防御体系开始受到破坏，或者遭受攻击，您是否会察觉？若有攻击者藏在您内部的某个角落，您是否会发现？感知是企业预测并发现内外部威胁的能力。企业需要通过网络威胁情报和主动防御来预测向其逼近的威胁或攻击，在内外部恶意行为成功实施前将其发现。企业必须知道可能会发生的事，同时采取分析来精准获取数据安全事件的风险预警。

- 抵御 - 其次，升级您抵御攻击的能力。如果攻击来自于您从未接触过的、全新且更为复杂的技术，您会怎么办？您的防御系统是否有能力抵御更为强大的、新的攻击？抵御机制就是企业护盾。建立防御机制首先需要了解企业整个生态系统所能承受的风险，然后在此基础上建立三道防线：

✓ 第一道防线：在日常操作中采取控制措施；

✓ 第二道防线：部署监控职能部门，如内部控制、法务部门、风险管理与网络安全部门；

✓ 第三道防线：实施强有力的内部审计。

- 应对 - 再者，增强应对能力。当受到外部攻击窃取或内部恶意泄漏时，您的企业有怎样的应对计划，您在其中的角色是怎样的？您会采取怎样的措施，是集中精力快速定位泄漏渠道还是不遗余力收集证据，诉诸法律？您的当务之急会是什么？如果感知失效（企业没能察觉逼近的威胁），抵御机制也出现问题（控制措施的效力不足），那么企

版权所有 翻印必究

业便需要为相关数据安全事件响应措施以及危机管理做好准备。同时企业也需要开始保留有力的法律证据，并对数据安全事件进行调查以安抚关键利益关联方——客户、监管机构、投资者、执法机关及公众，因为其中任意一方都可能发起诉讼，要求企业对其损失或不合规行为进行赔偿。而恶意事件的责任主体一经确认，企业则可以对之进行诉讼索赔。最后，企业需要以最快的速度恢复日常业务，从中学习经验，并调整与重塑以逐步加强数据安全保护的“弹性”。

具备“弹性”的数据安全防御机制的企业通常具有以下的特点：

了解业务

“弹性”的数据安全防御机制需要“整个企业”做出回应。为此，企业首先需要对业务和运营状况有深入了，才能知道在企业级的重要数据资产是什么，承载重要数据资产的流程及系统分别是什么。

了解网络生态

规划并评估企业在网络生态中的生态关系，识别存在的风险。评估网络生态中企业所面临的风险，确定影响企业对其生态控制能力的因素。

确定重要资产——王冠上的宝石

大部分企业对一些资产保护过度，但却忽略了另外一些重要数据资产。

确定风险因素

对于风险和威胁状况的不全面了解会导致数据安全保护职能无法发挥其全部作用。在所有能够提高意识、增加情报和识别风险的技术和工具中，合作意识才是最重要的。将所有业务职能中的风险和威胁状况分享出来才能够使企业了解其风险全貌，以及暴露出来的不足。这种分享与合作可以惠及处于同一生态中的其他企业（合作伙伴和供应商）。

用卓越的领导力管理人力因素

和所有混乱的局面一样，在企业遭受数据安全事件以后，员工应准备好且被训练好如何做出反应和行动。由于整个企业的运行都由技术支撑，所以每个员工都会受到影响。领导层明确的沟通、指导和示范是必不可少的，同时，员工明确的角色职责和能力所及的任务分工也能够帮助企业再次运转起来。

构建一个应变自如的企业文化

快速对数据安全事件做出反应的能力会最小化产生长期实质影响的可能性。优越、统一且自动化的响应能力能够帮助企业激活非常规的领导能力、危机管理能力以及全企业范围内的资源配置能力。企业在演练的时候可以考验现有的危机管理、现行操作以及风险状况以确保它们与企业的经营战略和风险偏好相一致。同时，企业也应开发并实施与自身状况相适应的对抗演习，将所有指挥和控制中心、“弹性”数据安全防御方针及计划纳入评估范围。

开展正式调查，准备应对诉讼

为了在重大数据安全事件中保护企业的利益，首席信息官和首席信息安全官应准备好联合企业中负责安全的最高层管理人员、企业法律总顾问、外部法律顾问、调查机构以及合规机构。

版权所有 翻印必究

版权所有 翻印必究

8.2. 数据安全保护原则与模型

企业管理层往往会担心数据安全保护工作不够全面，总有被遗漏疏忽的点最终成为重大数据安全隐患。和企业业务发展的长板理论不同，企业数据安全保护更要关注“短板效应”。因此，全面审视企业数据安全保护能力是至关重要的，需覆盖企业数据的全生命周期，即产生/创建/收集、流转、使用、分享/外发、归档到最终销毁的各个环节。

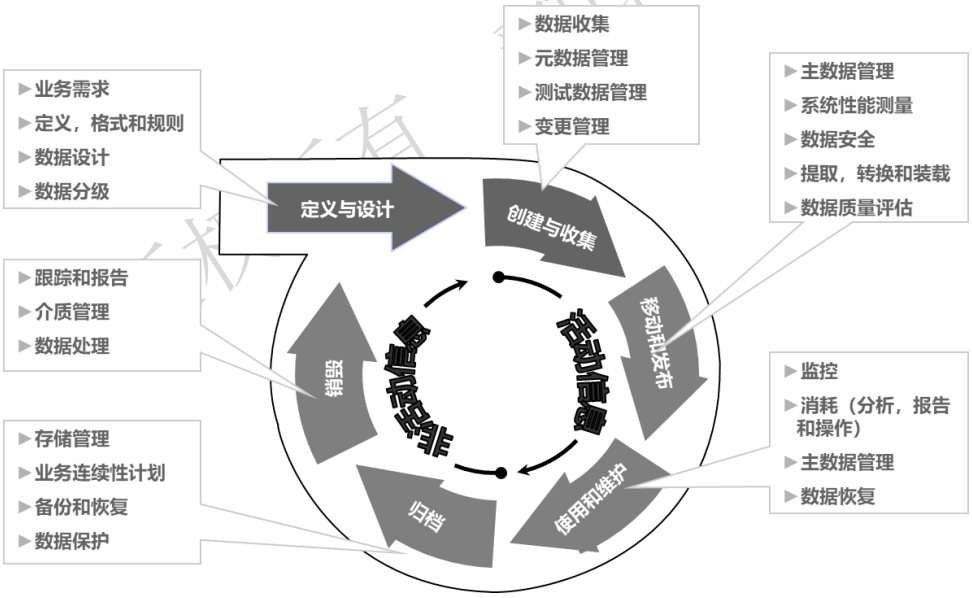


图 8.2 数据全生命周期

数据安全保护的方式多种多样，也有许多可遵循的法律法规及行业最佳实践标准，汇总起来大体有以下一些通用的原则。

普适性的数据安全原则：

- 最小权限原则 – 只授予处理者能够实现处理目的的最小权限和最少信息，达到处理目的后，应及时在限定时间内删除相关信息；
- 安全保障原则 - 采取适当的并与数据资产重要性相适应的管理措施和技术手段，确保数据安全，防止未经授权的检索、披露及丢失、泄露、损毁和篡改；
- 质量一致原则 - 保证处理过程中的数据资产保密、完整、可用，并确保数据质量，检验数据处于有效和更新状态；
- 可审计性原则 - 明确各项数据处理活动的责任，采取相应的措施落实监控、记录和审计，并对数据处理过程进行记录以便于追溯；

版权所有 翻印必究

针对个人信息的一些通用原则:

- 目的明确原则：处理个人信息具有特定、明确、合理的目的，不扩大使用范围，不在个人信息主体不知情的情况下改变处理个人信息的目的;
- 个人同意原则 - 处理个人信息需要要征得个人信息主体的同意;
- 公开告知原则 - 对个人信息主体要尽到告知、说明和警示的义务。以明确、易懂和适宜的方式如实向个人信息主体告知处理个人信息的目的、个人信息的收集和使用范围、个人信息保护措施等信息;
- 诚信履行原则 - 按照收集时的承诺，或基于法定事由处理个人信息，在达到既定目的后不再继续处理个人信息。

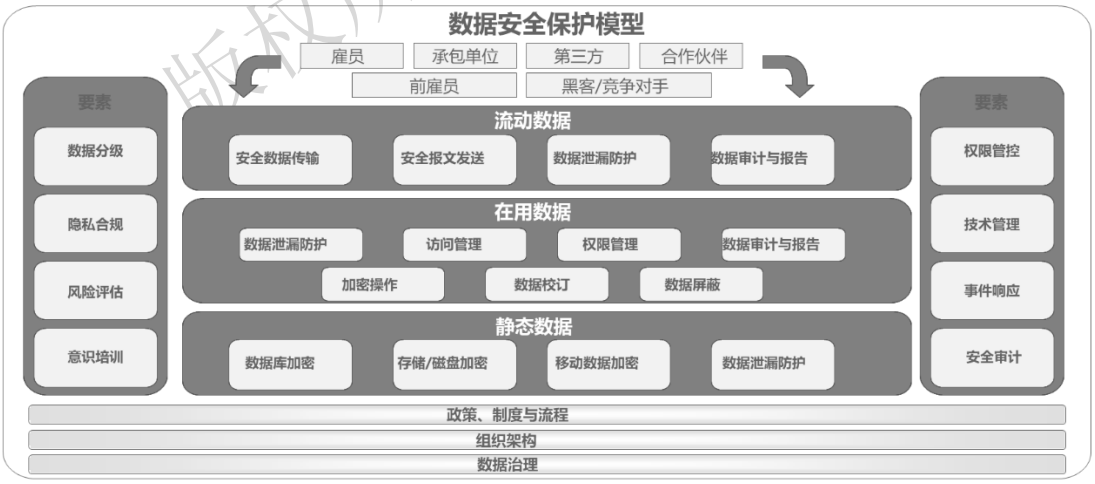


图 8.3 数据安全保护模型

企业级数据安全保护究竟需要哪些要素和组成部分呢？通过图 8.3 数据安全保护模型我们可以进一步清晰了解数据安全保护的组成部分。首先，我们需要了解企业数据安全的内/外部威胁生态有哪些，其中包含内部的雇员（恶意的/无意识的）以及外部的第三方合作伙伴、恶意黑客/竞争对手、前雇员等。只有了解了内/外部威胁生态，才能在风险分析过程中用攻击者的视角去分析，从而更全面的了解攻击面及手段。其次，有一系列的管控要素，这些要素正式回应了前面章节关于感知、抵御和应对的理念，其中包含了事前、事中及事后的一系列管控要素，协助企业建立“弹性”的数据安全保护机制。再次，数据资产在全生命周期中，通常存在于三种状态，即流动数据，使用数据及静态数据，在数据三种状态中实施不同的安全管控，包含管理流程类和技术类的管控，即可全面覆盖数据全生命周期的安全管控。最后，也是最重要的基石，即上层建筑的落实，包含高级管理层的支持，企业级整体数据安全治理架构，策略流程及人员组织架构和职责分配，这些都是确保上述管控要素和措施可以落实到位的先决条件。

版权所有 翻印必究

8.3. 数据安全保护方法及思路

我们从“公司治理层面”，“流程与数据层面”，“支持层面”三个不同的层面建立自上而下的全面数据安全防护体系，全盘地解决数据安全问题。建立治理机制，定义角色及其职责，以求有效地管理和维护体系架构；在流程层面，根据全面的数据安全风险评估所发现的差距，加强所有支持性 IT 流程；在 IT 支撑层面，采用涵盖全部三个领域（人员、流程、技术）的解决方案，有效地监控、防止、和响应所有潜在的数据安全风险。

图 8.4 多层次的数据安全保护架构

那企业将如何开展数据安全保护工作呢？聚焦实务，通常通过三步走的方式，逐步推进相关工作。

- 步骤一：数据资产识别 – 企业所要保护的数据资产需有针对性，在数据安全保护投入有限的前提下，并考虑到管控和业务效率的平衡，我们必须先关注企业重要的数据资产，从而将最大限度的投入到对重要数据资产的保护中，并佐证其管控措施的必要性，为管控与效率平衡决策提供依据。如上文所述，这个过程不单单是 IT 部门或信息安全部门的事情，要想识别出企业最重要的数据资产应从业务视角切入，了解企业业务流程，了解企业业务价值，从中识别出重要的数据资产，并进一步分析数据资产所承载的业务流程及信息系统，为下一步风险评估做好充分的准备；

- 步骤二：风险分析 – 选取识别出的重要数据资产进行风险分析。在这个步骤中首先要确定分析客体，不能面面俱到进行全量数据的风险分析，不然得出的结果将是海量的，且工作量无法控制。必须聚焦最重要的数

翻印必究 版权所有 翻印必究

据资产，结合业务场景及信息系统，“自上而下”进行数据动态流转分析，并“自下而上”进行数据静态系统分布分析，从而绘制出所选取的重要数据流转图。基于数据流图就能进行流程层面及系统层面的风险评估。这样评估的意义在于，可以将单点上发现的问题串联起来识别出更具结果导向的，直观的数据安全风险场景;

- 步骤三：数据保护 – 在识别出了数据安全风险场景以后，针对场景中的流程及信息系统层面上的管控薄弱环节设计并实施数据安全保护措施。因此管控措施分为管理和技术两方面。管理方面，通过流程机制的建立，在关键节点设立检查点或审批点。在技术方面，通过在数据存储，数据流转及数据使用不同数据形态下实施技术管控手段，如身份访问控制、数据加密、数据脱敏、数据防泄漏、数据安全监控审计等技术产品及手段，确保数据保护措施落地到位。

图 8.5 数据安全保护工作思路

8.4. 数据安全保护主流技术简介

前文叙述了数据安全保护的理念，模型以及工作开展思路，最终数据安全保护落地的主流技术及解决方案有哪些，如何有效地且针对性地选取其中的相关技术为企业数据安全保护助力，在本节内我们将针对目前主流的数据安全保护技术做一简介。结合前文提出的“感知”、“抵御”和“应对”的理念，我们会分别标注相关技术的适用理念属性，便于更好地理解和后续选用。

8.4.1. DCAP 技术（标签：抵御、应对）

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

版权所有 翻印必究

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。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。

8.4.2. 脱敏技术（标签：抵御）

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。其核心功能包含数据和关系发现，数据脱敏规则定义，数据脱敏操作和管理及报告合规性。

8.4.3. 数据防泄漏技术（标签：抵御）

数据防泄漏技术是一款相对较成熟的数据保护技术，其功能是协助企业数据安全保护人员解决以下几个问题，即企业重要数据存储在哪里？企业重要数据使用情况如何？如何保护企业重要数据？根据部署位置和功能的不同，大致可以分为以下这些相关技术，即网络监控 DLP，终端防护 DLP，邮件防护 DLP，网络防护 DLP，文件存储设备 DLP，数据库 DLP 等。

8.4.4. CASB 技术（标签：抵御）

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。

8.4.5. 身份访问控制技术 IAM（标签：抵御）

身份访问控制技术是企业 IT 服与系统实施中最最基础的安全管控，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。

8.4.6. UEBA（标签：感知、抵御）

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。

8.4.7. 数据透明加密保护技术（标签：抵御）

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。

8.4.8. 数据库防勒索技术（标签：抵御）

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。

从以上主流数据安全保护技术介绍中可以看出，绝大部分技术解决方案依旧专注于传统的“抵御”环节，这也很好的反应了目前市场需求，企业数据安全保护成熟度以及厂商的方案侧重点。但是，随着“弹性”数据安全保护理念的不断普及和深入，“感知”和“应对”的市场需求及相关技术方案必将不断增加和提升。

版权所有 翻印必究

附件一.

关键信息基础设施业务判定表

行业		关键业务
能源	电力	● 电力生产（含火电、水电、核电等） ● 电力传输 ● 电力配送
	石油石化	● 油气开采 ● 炼化加工 ● 油气输送 ● 油气储存
	煤炭	● 煤炭开采 ● 煤化工
金融		● 银行运营 ● 证券期货交易 ● 清算支付 ● 保险运营
交通	铁路	● 客运服务 ● 货运服务 ● 运输生产 ● 车站运行
	民航	● 空运交通管控 ● 机场运行 ● 订票、离港及飞行调度检查安排 ● 航空公司运营
	公路	● 公路交通管控 ● 智能交通系统（一卡通、ETC 收费等）
	水运	● 水运公司运营（含客运、货运） ● 港口管理运营 ● 航运交通管控

版权所有 翻印必究

水利	● 水利枢纽运行及管控 ● 长距离输水管控 ● 城市水源地管控
医疗卫生	● 医院等卫生机构运行 ● 疾病控制 ● 急救中心运行
环境保护	● 环境监测及预警（水、空气、土壤、核辐射等）
工业制造 （原材料、装备、消费品、电子制造）	● 企业运营管理 ● 智能制造系统（工业互联网、物联网、智能装备等） ● 危化品生产加工和存储管控(化学、核等) ● 高风险工业设施运行管控
市政	● 水、暖、气供应管理 ● 城市轨道交通 ● 污水处理 ● 智慧城市运行及管控
电信与互联网	● 语音、数据、互联网基础网络及枢纽 ● 域名解析服务和国家顶级域注册管理 ● 数据中心/云服务
广播电视	● 电视播出管控 ● 广播播出管控
政府部门	● 信息公开 ● 面向公众服务 ● 办公业务系统

版权所有 翻印必究
版权所有 翻印必究

Things turn out best for the people who make the best of the way things turn out.

——John Wooden

版权所有 翻印必究

版权所有 翻印必究

作者介绍

北京植德律师事务所

王伟 合伙人

电话：185 6663 2717

邮箱：wei.wang@meritsandtree.com

微信：

朱宣烨 合伙人

电话：159 1067 2037

邮箱：xuanye.zhu@meritsandtree.com

微信：

曾雯雯 合伙人

电话：155 0104 7466

邮箱：wenwen.zeng@meritsandtree.com

微信：

植德律师事务所隐私保护、网络安全和数据创新团队是国内最早关注并从事该领域法律服务的团队之一。我们曾为多家互联网公司、高新科技公司、网络安全公司、数字媒体公司、社交网络公司、智能汽车公司、医疗大数据公司、云计算公司、区块链技术公司的数据管理、合规计划和审查、网络突发事件和网络犯罪的防范和应对、最佳实践提供快速、创新的法律咨询服务。

版权所有 翻印必究
版权所有 翻印必究

Orrick, Herrington & Sutcliffe LLP 美国奥睿律师事务所

Antony Kim
奥睿华盛顿办公室合伙人
全球网络／联邦贸易委员会(FTC)业务主管

电话：+1 202 339 8493

邮箱：akim@orrick.com

Kolvin Stone
奥睿伦敦办公室合伙人
全球隐私保护业务主管

电话：+44 20 7862 4701

邮箱：kstone@orrick.com

Aravind Swaminathan
奥睿西雅图、波士顿办公室合伙人
网络，隐私和数据创新/集体诉讼辩护

电话：+1 206 839 4340

邮箱：aswaminathan@orrick.com

Xiang Wang 王翔
奥睿北京和纽约办公室合伙人
中国隐私保护／网络业务主管

电话：+86 10 8595 5600

邮箱：xiangwang@orrick.com

Jeff Zhang 张劲松
奥睿北京、纽约办公室合伙人
企业，并购和私募股权

电话：+1 212 506 5363

邮箱：jeffzhang@orrick.com

版权所有 翻印必究

Betty Louie 吕丽明
奥睿北京办公室合伙人
技术公司集团/并购和私募股权

电话：+86 10 8595 5618

邮箱：blouie@orrick.com

美国奥睿律师事务所于 1863 年在加州创立，在亚洲、欧洲和北美各地的主要商业中心设有超过 25 家办事处，是一家专注于为科技业、能源与基础设施行业和金融服务行业提供全方位法律服务的大型国际律所。奥睿的业务遍布全球主要经济体，包括美国、中国、日本、欧盟、拉丁美洲以及非洲。

2018 年美国奥睿律师事务所连续第六年入选《美国律师》杂志 A 级律所名单（A-List），这也是奥睿第十次获此殊荣，本所在此 2018 年最新名单上排名全美第四。《美国律师》杂志将此名单上的律所形容为“全美最全面的精英律所”。2019 年《财富》连续第四年将本所列入最适宜工作的 100 家公司榜单，是少数几家上榜的律所之一; 而《金融时报》在过去三年将奥睿评为最具创新精神的北美律所。

版权所有 翻印必究
版权所有 翻印必究

高轶峰 Kelvin Gao
安永咨询合伙人

电话：183 2198 0561

邮箱： kelvin.gao@cn.ey.com

高轶峰先生是安永风险咨询服务部的合伙人。拥有超过 17 年从事信息科技风险及信息安全相关工作经验，对信息科技风险治理、信息安全治理、云计算安全管理、数据安全、隐私保护等均有深入研究。高先生的任职及荣誉如下：

- 云安全联盟（CSA）上海分会理事
- 中国云安全联盟（C-CSA）特聘专家
- ISACA 华北志愿者社区负责人
- 国际注册隐私保护专家（IAPP - CIPT）
- 国际注册信息安全经理（CISM）
- 国际注册信息系统审计师（CISA）
- 国际 APMG CISA/CISM 认证讲师
- 国际注册业务连续性专家（CBCP）
- 云安全联盟认证讲师（CSACT）
- 国际注册云计算安全专家（CCSK）
- 云计算系统安全专家（CCSSP）
- 信息安全管理体系主任审计员（ISO27001LA）
- 国际注册项目管理专家（PMP）
- 微软认证技术专家（MCITP）
- Oracle 认证技术专家（OCP）

版权所有 翻印必究
版权所有 翻印必究

本白皮书起草得到若干助力，在此一并致谢。感谢董芊，周泱，高阳，王明志、刘少华、汪子健、王丹阳、赵紫晗，卢苗苗，南灵芝，赵晓彧，以及其他同事和朋友。

版权所有 翻印必究
版权所有 翻印必究

版权与免责

本白皮书仅供业内人士参考，不构成任何意义上的法律意见或建议。未经事先同意，本白皮书不可被用于任何其他目的，如需转载，请注明出处。本白皮书中原始资料可能来源于网络，如有问题，请联系我们。

版权所有 翻印必究

版权所有 翻印必究