汉坤法律评述

2025 年 6 月 26 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港 | 海口 | 武汉 | 新加坡 | 纽约 | 硅谷

数据安全事件频发，企业如何防御？（上）

作者：李珺 | 黄颖 | 赵思韵

近年来，国内外数据泄露事件频发，涉及医疗、金融、零售、酒店、教育等多个行业，数据安全问题屡屡成为公众关注的焦点。

随着全球数据监管要求日益趋严，企业一旦发生数据安全事件，不仅可能面临**运营中断、声誉受损等经营风险，还可能触发多重法律责任，包括监管约谈、强制开展个人信息保护合规审计[1]，甚至高额行政处罚**——例如，依据《个人信息保护法》，企业因违规造成数据安全事件可能面临高达 5,000 万元或企业上一年度营业额 5%的罚款[2]。

在企业推进数字化的当下，**数据安全事件的规模和频率持续上升，已由偶发事件演变为“新常态”，成为管理层和企业法务必须日常关注的重点**。结合近期的实务经验与观察，我们拟通过上下两篇，从事前防御与事后响应两个角度，为企业梳理应对数据安全事件的处置要点。本文为上篇，聚焦于事前防御工作。

一、高发风险场景：企业数据安全的“隐雷”在哪里？

数据安全的**最大挑战之一，是不少企业虽具备一定的合规意识，但缺乏足够的风险意识**。现实中，不少事故的根源，正是因为企业未能建立起有针对性的风险防控体系。遗憾的是，很多企业只有在经历了重大安全事件后才开始“亡羊补牢”，但此时往往已付出高昂代价。**风险防控的起点在于识别风险**。根据我们的观察，以下高发风险场景尤其值得关注：

（一）权限管理：被忽视的数据安全短板

尽管权限管理作为数据合规的基本要求，已逐渐成为企业共识，但在实际操作中仍存在诸多隐患。不少企业存在“权限越多越好”的误区，导致企业员工甚至外包人员申请的数据访问权限超出实际岗位所需，造成**权限配置与实际职责不匹配**的问题。同时，权限管理**缺乏动态调整机制，**既未定期审查权限配置，也未及时清理冗余权限，尤其在员工离职或岗位变动时，因未能同步冻结或解绑其原有访问权限，扩大了数据暴露范围。

另外，部分企业的**权限管理制度流于形式，**实际执行不到位，员工可较为自由地复制、下载敏感信息。与此同时，**日志记录不完整、审计机制缺失**，也使得行为追踪与事件溯源困难重重。一旦发生安全

1 《个人信息保护法》，第 64 条。

2 《个人信息保护法》，第 66 条。

事件，往往难以及时定位风险源头，显著增加了响应与追责难度。

（二）数据流转：信息共享下的安全隐患

数据共享虽已成为企业业务协同的重要基础，但在实际操作中，企业在部门间、集团内部或与外部合作伙伴的数据交互中，往往存在**数据披露范围失当**的问题，未区分不同数据的敏感等级，数据在超出业务必要性下被任意调取和使用。同时，**数据流转路径不清，**缺乏完整的流转记录和透明的流向管理，进一步加大了管控难度。

更值得关注的是**数据传输方式不规范**，实践中部分企业依然采用未经加密的明文邮件或即时通讯工具等非正式渠道传递敏感数据，使数据在流转过程中暴露于外部风险之下，极大增加了数据被滥用与泄露的可能性。

（三）外包服务：数据泄露高发地

随着数据处理链条日益复杂，企业对外包服务的依赖度不断提升，第三方供应商在系统运维、数据处理等环节的作用愈发关键。然而，实践中，企业在引入和管理外包服务过程中仍存在诸多风险点。例如，**数据接口管理不规范、访问权限设置过宽，**成为了数据安全的突破口。

同时，由于供应商服务对象多元化，易出现**数据混同处理、权限交叉共享**等情形。此外，部分**供应商安全管理薄弱**，在数据脱敏、加密、日志审计等方面的措施不到位，进一步增加了数据泄露的可能性。

二、精准防控：企业如何有效化解数据安全风险？

数据安全风险虽无处不在，但并非不可防控。**企业若能遵循“二八法则”，聚焦于高风险环节，采取有效的防护措施，可显著降低数据安全事件的发生概率和危害程度**，具体而言：

（一）实施数据分类分级管理

数据的分类分级不仅是企业数据合规的重要义务，更是防范安全事件的关键手段，还可以在数据泄露发生时有效降低事件危害程度。根据公开信息，在近期一起数据安全事件中，正因涉事企业对数据采取了存储隔离，避免部分敏感信息外泄，降低了事件造成的影响。

我们建议企业结合实际业务场景，**梳理数据和数据流、识别敏感程度、使用场景及潜在风险，完善数据分类分级管理策略**，并据此**建立数据隔离制度**，通过物理或逻辑隔离措施，规范不同层级数据的访问权限与流转路径。

（二）强化访问权限控制

访问权限管理不当是引发数据泄露事件的重要因素之一。我们建议企业基于“最小授权”原则和“职责分离”原则，**明确各部门/岗位对应的权限清单，合理划分不同系统和数据的访问级别、建立岗位与权限的对应关系，同时完善第三方访问的审批与监控机制。**

针对高风险操作，例如批量下载、数据导出、敏感数据访问等，应明确审批流程，落实**操作留痕与实时监控措施**。此外，企业还应建立权限的**定期复核和动态调整机制**，及时调整离职或岗位变动人员的访问权限，减少权限冗余带来的潜在隐患。

（三）构建供应链安全管理机制

我们建议企业从准入审查、合同约束与持续监管三方面着手，构建供应链管理机制，具体而言：

- 准入审查：在供应商引入阶段，企业应开展数据合规尽职调查，评估供应商的数据安全能力与合规意识。企业可**将尽职调查与 PIA（个人信息保护影响评估）流程结合，嵌入供应商准入流程**，从源头筛查并控制潜在风险。
- 合同约束：在合作协议中设置专门的数据处理条款，或与供应商签订数据处理附录，**明确数据访问的条件和要求，约定供应商须遵守企业的数据安全标准**。同时，应规定在数据安全事件发生时，**供应商有义务及时通知、积极配合调查和报告，并主动采取措施减轻危害。**
- 持续监管：第三方合规管理并非“一劳永逸”，对供应商的管理也不应止步于合同签署，而应建立动态监督机制。**通过定期对供应商进行 IT 系统与合规审计**，企业不仅能及时发现并纠正风险，也能在面对监管问询时证明企业已履行“监督义务”。

需要注意的是，供应链管理可采用差异化原则，并非所有的供应商均需同等强度的管控。企业可根据供应商的业务属性、数据处理范围及风险等级，制定分级管理策略，提升管理效率。

***

综上，尽管数据安全事件难以预见，但其防范并非无从着手。企业可通过梳理业务流程和数据流转路径，理清所涉数据资产及其映射关系，识别关键系统（包括内外部平台、云服务）和相关主体（包括内部员工、集团成员、外部供应商、合作伙伴），精准定位风险敞口，并通过优先完善关键环节的防控，将“被动应对”转变为“主动防御”，降低数据安全风险的发生概率。

然而，即便建立了完善的预防机制，数据安全事件仍难以完全避免。一旦事件发生，企业的响应方式将直接影响损失程度。在下篇中，我们将围绕事件响应机制，提出针对性建议，帮助企业在危机中最大限度地减少损失并降低影响。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

李珺

电话： +86 21 6080 0981
Email： jun.li@hankunlaw.com