汉坤法律评述
2026 年 2 月 13 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？（下）

作者：李珺 | 黄颖 | 赵思韵

新年伊始，上海网信办发布 2025 年执法典型案例，首类案件即聚焦企业未履行安全主体责任引发的泄露事件，涉事企业均遭处罚。在《*数据安全事件频发，企业如何防御？（上）*》中，我们解析了**权限管理**、**数据流转**与**外包服务**等高风险场景，提出以“主动防御”为核心的事前防控策略。然而，面对复杂的安全形势，企业难以做到“零风险”。当防线被突破时，快速响应与有效处置即成为止损的关键。本篇将聚焦事后响应阶段，从**预案建设**到**跨国应对**，探讨企业如何构建高效的处置机制。

一、法定义务底线：数据安全事件中的“规定行动”

数据安全事件的响应不仅是技术层面的止损，更是法律层面的合规义务。根据“数据三法”的要求，一旦发生安全事件，企业应同步推进“技术止损”（例如隔离系统、修复漏洞、阻断访问等）和“合规履责”（例如报告监管、通知个人等）。

（一）事件报告：向监管部门履行告知义务

根据事件性质及影响范围，企业需在规定时限内向相关监管部门报告，通常包括**公安机关**、**网信部门**及**行业主管部门**等，这不仅是法定义务，也是获取监管指导、避免“迟报漏报”责任的关键。

依据 2025 年 11 月生效的《国家网络安全事件报告管理办法》，发生“较大、重大或特别重大网络安全事件”[1]的，**4 小时即为初步报告的时限**[2]；对于金融等**强监管行业**，这一窗口期可能进一步被缩减到 **1 小时**[3]。此外，若事件涉及非法侵入计算机信息系统等**违法犯罪行为**，需在 **24 小时**内向当地公安机关报告[4]；若事件涉及网络产品安全漏洞的，则应在 **2 日**内向工业和信息化部网络安全威胁和漏洞信息共享平台报送[5]。

[1] 根据《国家网络安全事件报告管理办法》附件，例如泄露 1 亿人以上公民个人信息的事件属于“特别重大网络安全事件”，泄露 1,000 万人以上公民个人信息的事件属于“重大网络安全事件”，泄露 100 万人以上公民个人信息的事件属于“较大网络安全事件”。

[2] 《国家网络安全事件报告管理办法》，第 4 条。

[3] 例如《中国人民银行业务领域网络安全事件报告管理办法》，第 15 条。

[4] 《计算机信息系统安全保护条例》，第 14 条。

[5] 《网络产品安全漏洞管理规定》，第 7 条。

为应对前述紧迫的报告时限，我们建议企业建立“**内外协同**”响应机制，对内，打通直达决策层的汇报通道，确保信息即时同步；对外，通过协议明确供应商的协助与通知义务，防止因第三方迟报导致合规责任传导。实践中，“个人信息泄露 100 万条”和“直接经济损失 500 万”是企业相对容易触碰的“较大事件”红线，一旦触及，即触发报告程序。因此，**建议企业预先完成红线数据盘点和定损标准确立，确保紧急状态下快速定性，避免漏报或者过度报告。**

（二）风险告知：向个人信息主体履行通知义务

若涉及个人信息泄露，企业还应通知受影响的个人，值得注意的是，法律也设定了豁免情形 — 即采取有效措施已消除风险的前提下，可免除通知义务。

基于此，实践中，“是否通知个人”已成为企业处理数据安全事件中最为棘手的决策之一。发出通知，可能引爆舆情，甚至在未报备监管的情况下招致监管问询；不通知或延迟通知，一旦后续被认定为“风险未消除”或被用户曝光，则面临更严厉的处罚与信任危机。尤其在跨国事件场景中，若海外已通知，国内却未同步，容易引发“双标”的舆情危机，导致合规风险与声誉危机的双重叠加。

因此，数据安全事件发生后，企业应**组织技术、法律、业务与公关团队的联合指挥部，进行多维度研判，包括是否启动通知程序、如何把握通知时机（特别是与监管报告的节奏协调）、如何统筹其他法域的披露进程、如何设定对外披露的颗粒度与口径**等，在守住合规底线的同时，保住品牌声誉，把事件的负面影响降到最低。

二、应急预案：打造一套真正“能用”的响应体系

妥善履行数据安全事件中的合规义务，前提在于建立一份**全面且具有操作性**的应急预案，涵盖从**发现、评估、报告**到**响应、处理**及**复盘**的全流程机制。遗憾的是，实践中不少企业直接套用模板文件，与自身的业务实际脱节，成了形式合规的“空架子”。因此，要让预案真正有用，企业应结合具体的业务场景（例如独立处理、委托处理、跨境传输等）厘清责任，针对不同等级的风险制定差异化策略，避免“一刀切”。同时，高效的响应不能依赖单一部门，而应建立**涵盖技术、法律、业务和公关等多维度的联动机制**。一旦危机触发，联动机制即刻启动：技术团队负责阻断攻击并留存日志，法务团队主导监管上报与证据保全，业务团队聚焦恢复服务运行，公关团队统筹内外发声，通过多方并行协作，最大程度降低事件冲击。

当然，再完美的预案如果不经实战检验，终究只是“纸上谈兵”。**定期演练不是为了走过场，而是验证预案是否管用、提升团队反应速度的关键。**建议企业避免粗放全面式的全面铺开，而是聚焦高频高风险场景（如勒索病毒、用户信息泄露）。应急响应本质上是一场跨部门的“团战”，因此演练须覆盖所有相关团队，一方面通过全链路推演，理顺指挥链和协同性；另一方面通过流程实测，检验技术阻断、通知发送等关键环节的有效性。演练结束后及时复盘修正，确保预案能从静态的“文档”变成关键时刻可用的“实战指南”。

三、跨国协同：全球框架下的“本地化”适配

对于开展跨国运营的企业而言，数据安全事件往往牵动多个法域，在此背景下，企业往往会建立**统一的全球响应框架**，在集团层面形成较为成熟的应急机制。然而，不同司法辖区在**事件报告、通知义务、响应时限**等方面存在监管差异。在实际落地中，若简单将全球预案“复制粘贴”到中国，往往会因水土不服而触碰红线。**我们建议企业从“响应时效”与“沟通策略”两个维度进行本地化适配。**

不同司法辖区对事件报告的时限要求不同。例如，根据《欧盟通用数据保护条例》（GDPR），企业应在

发现数据泄露事件后的 **72 小时**内进行报告，但数据泄露不会对个人权利和自由造成风险的情况除外[6]；然而根据前述《国家网络安全事件报告管理办法》，涉事企业可能需在**更短时间内（例如 4 小时内）**向监管部门报告，远短于 GDPR 的时限要求，且往往存在“边处置、边报告”的情况。

实践中，集团层面的应急组织架构通常由总部主导，存在许多跨国企业习惯于“先报总部、再等批复”的折返跑模式，当总部还在评估“是否触发 GDPR 披露要求”时，中国区可能已经面临迟报的合规风险。因此，**预案应建立“本地处置决策机制”，授权国内团队在特定紧急情形下，可依据中国法律直接启动程序，而非被动等待总部指令。**

另一方面，海外的应急预案往往以“防御”为核心，最小化信息披露，强调技术层面的原因，以防范集体诉讼和巨额罚款。然而，在国内的语境下，更看重企业的主动配合和过程透明。若完全照搬总部的防御性沟通策略，容易被监管认为是推诿责任。因此，**预案应根据合规语境的转换，给予国内团队适度的“策略适配权”，在总部的技术复盘分析基础上，补充完善本地监管关注的合规整改，确保对外沟通既符合集团统一要求，又能精准回应本地监管的重点。**

******

在 AI 与数字化加速的当下，绝对的安全已不存在。企业只有将“事前防御”与“事后响应”深度融入数据治理，把应急机制转化为组织的“肌肉记忆”，方能在危机中掌握主动，保障业务稳定运行与合规安全。

[6] 《欧盟通用数据保护条例》，第 33 条。

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