

# 防患于未然：基于风险矩阵的 API 金融数据泄露风险管理

## （附录 2）

### 外审意见

文章从定量角度探讨 API 金融数据泄露风险管理问题，基于 API 数据收集、使用、传输、处理和储存环节构建风险矩阵。以下建议供参考：

**意见 1：**“二、相关文献综述”更像是引言，相关的部分内容是否可以和引言部分合并。引言部分“基于此...”写的是本文研究内容，文献综述部分第三段中也有本文研究内容，是否可以适当修改，避免重复。

“文献综述”部分，建议按照以下逻辑梳理：先写现有的关于 API 金融数据泄露风险及其管理领域的研究现状，接着，在综合分析现有研究不足，最后，突出本研究创新成果。

**意见 2：**进一步梳理文章逻辑，如“三、（一）”中概念性的部分感觉可以删掉，文章题目是 API 金融数据泄露风险管理，就只围绕 API 金融数据泄露风险管理进行，无关的内容尽量少罗列。

“（一）”中其他内容还有“（二）基于 API 应用过程风险节点”的内容是否可以揉到合适的对应章节中。

**意见 3：**“六、金融数据泄露风险应对”是否可以和最后“七”的建议部分合并。

**意见 4：**“七、结论和建议”部分，只有建议，没有结论。另外，在建议部分，可从 API 数据的收集、使用、传输、处理和储存各环节提出有针对性的建议。总之，就是前文文献综述、理论分析、实证分析和建议最好是有一定的逻辑对应关系，现在逻辑稍显松散，以上建议供参考。

### 作者回复

我们非常感谢审稿专家提出的宝贵修改意见，我们完全认可并努力按照修改意见对本文进行修改，您的建议让我们受益良多，对本文的完善有非常重要的启迪和指导作用。现在，我们针对审稿专家的中肯意见以及相关修改情况进行逐条回复。

#### 意见 1 修改说明：

1、原来的“二、相关文献综述”相关内容已和引言部分合并，并添加了一些参考文献重写了“二、文献综述”。

2、原来的引言和相关文献综述后都有本文研究内容，我们将引言部分的“本文研究内容”进行了完善，删除了文献综述后的“本文研究内容”，并在总结现有文献不足的基础上补充了本文创新点。

**意见 2 修改说明：**

文章原来的“三、风险识别路径”，有关风险可能存在环节的内容已融入到文章的引言部分，有关数据泄露风险因素的内容已融入到文章“API 数据泄露风险识别”部分，无关内容已删除。

**意见 3 修改说明：**

我们已将“七”的建议部分融入到了“六、金融数据泄露风险应对”，并补充了本文研究结论。原来的风险应对措施在文字表达上不太具有针对性，逻辑有些混乱，我们根据上述分析总结出的高风险、中风险、低风险，针对性提出应对措施和建议。

**意见 4 修改说明：**

除上述根据专家建议的针对性修改外，我们对文章表达进行了优化，使整体表达逻辑更为连贯，用词更为规范。

防患于未然：基于风险矩阵的 API 金融数据泄露风险管理

(附录 1)

表 4 A 银行 API 开放银行的风险矩阵

| 风险类别   | 风险因素         | 风险影响 | 风险概率 | 风险级别 | Borda 数 | Borda 序数值 |
|--------|--------------|------|------|------|---------|-----------|
| 数据收集环节 | 绕过身份验证       | 5    | 3    | 高    | 54      | 14        |
|        | 不法分子违规收集数据   | 4    | 3    | 中    | 43      | 18        |
|        | 内鬼暗地下载数据     | 3    | 4    | 中    | 43      | 18        |
|        | 黑市购买数据       | 2    | 3    | 中    | 17      | 32        |
|        | API 开发和部署漏洞  | 4    | 5    | 高    | 59      | 10        |
| 数据使用环节 | 登录接口盗取密码     | 5    | 5    | 高    | 80      | 0         |
|        | 接入耗时长        | 2    | 3    | 中    | 17      | 32        |
|        | 被植入恶意软件      | 3    | 2    | 中    | 19      | 31        |
|        | 利用动态代理 IP 攻击 | 3    | 4    | 中    | 29      | 27        |
|        | 数据风险标准不一     | 5    | 4    | 高    | 62      | 9         |
|        | 数据清洗成本过高     | 4    | 4    | 中    | 47      | 17        |
|        | API 管理无统一标准  | 3    | 2    | 中    | 16      | 34        |
|        | 非法篡改或错误修改数据  | 5    | 4    | 高    | 68      | 3         |
|        | 金融机构滥用个人数据   | 4    | 5    | 高    | 55      | 13        |
|        | 第三方金融机构不合规   | 2    | 2    | 低    | 6       | 38        |
| 数据传输环节 | 数据未加密        | 5    | 4    | 高    | 65      | 6         |
|        | 未授权访问        | 4    | 5    | 高    | 70      | 2         |
|        | 允许弱密码存在      | 5    | 5    | 高    | 78      | 1         |
|        | 数据传输途中被篡改    | 5    | 3    | 高    | 58      | 12        |
|        | 网络窃听         | 1    | 3    | 低    | 11      | 36        |
|        | 中间人攻击        | 3    | 2    | 中    | 15      | 35        |
|        | 不安全的传输协议     | 4    | 3    | 中    | 36      | 20        |
|        | 数据包重放        | 4    | 2    | 中    | 29      | 26        |
|        | 内部员工行为问题     | 4    | 5    | 高    | 59      | 10        |
|        | API 资产管理问题   | 2    | 2    | 低    | 8       | 37        |
| 数据处理环节 | 缺乏统一的数据处理标准  | 5    | 3    | 高    | 54      | 14        |
|        | 恶意计算代码       | 4    | 3    | 中    | 31      | 25        |
|        | 不正确的算法实现     | 3    | 2    | 中    | 22      | 30        |
|        | 侧信道攻击        | 4    | 2    | 中    | 24      | 28        |
|        | 格式转换出错       | 1    | 2    | 低    | 0       | 40        |
|        | 数据映射和重定向     | 4    | 3    | 中    | 33      | 23        |
|        | 数据脱敏不规范      | 4    | 5    | 高    | 66      | 4         |
|        | 人为失误和组织失误    | 3    | 4    | 中    | 35      | 21        |
|        | 风险信息沟通渠道不畅通  | 1    | 3    | 低    | 4       | 39        |
|        | 业务操作及工作习惯    | 2    | 4    | 中    | 24      | 28        |
|        | 伪装成正常流量请求    | 4    | 5    | 高    | 64      | 7         |

|            |           |   |   |   |    |    |
|------------|-----------|---|---|---|----|----|
| 数据储存<br>环节 | 储存数据价值较大  | 4 | 5 | 高 | 66 | 4  |
|            | 数据储存时间过长  | 3 | 4 | 中 | 34 | 22 |
|            | 储存渠道管理不规范 | 3 | 4 | 中 | 32 | 24 |
|            | 储存数据未分级分类 | 4 | 3 | 中 | 39 | 19 |
|            | 储存数据数量过多  | 4 | 5 | 高 | 64 | 7  |

注：作者计算得到。