

产品风险管理

你好，欢迎来到腾讯大学出品的《腾讯产品 18 讲》。

前几节课，我们聊到的几个运营思路，比如热点运营需要产品经理快速响应热点，唯快不破讲究小步快跑、快速迭代等等，都在体现运营之「快」的精髓；今天这一讲，我们希望产品经理能够「慢」下来，观察和思考日常奋起奔跑的过程中，经常无暇理会、容易忽视、却有可能带来致命一击的「灰犀牛」。

我们身边都有哪些「灰犀牛」？

「黑天鹅」一词近些年被很多人知晓，它比喻极小概率发生、却影响重大的事件；与它相关联的还有一个概念，叫「灰犀牛」，它是由来自纽约国际政策研究所的米歇尔·渥克提出来的，表示大概率会出现、且影响巨大的潜在危机。

灰犀牛体型笨重、反应迟缓，你能看见它在远处，却毫不在意；而一旦它向你狂奔而来，定会让你猝不及防，直接被扑倒在地，它并不神秘，却更危险。

那么回归到我们的产品工作中，都有哪些像灰犀牛一样的潜在风险项呢？



第一，信息泄漏风险。

互联网产品有一个特点，我们叫它「错觉的私密感」，为什么这样说呢？

现在，来想象一个画面，我们创造每一个科技产品，本质上都是在现实世界里，为用户打开一扇数字世界之窗，透过这扇窗户，用户可以获取到无尽的信息，足不出户与他人产生交流。

用户在真实世界中，绝大多数时候都是在独立使用科技产品，尤其是移动互联网时代，手机是每个用户的专属设备，小屏幕、随身性，更是强化了产品使用中的个性化与私密性。所以这个时候，用户会「错觉」地以为自己是一个人在使用产品，我所处的环境是安全的，往往忽略了那扇数字之窗，也记录着用户的各种信息和数据。

那构建这扇窗户背后的产品、人以及公司，就非常的关键。我们是否能够帮助用户保护好数据的私密性和安全性，对产品的长远发展起着非常重要的作用。一旦产生信息泄漏，我们将失去用户的信赖，而且这种失信，会像滚雪球一样危及到产品的立身之本。

两年前，轰动整个科技圈的 Facebook 信息泄漏事件，应该算一个典型案例了。美国 5000 万用户，通过一个性格测试的小应用，回答测试问题，领取奖金，在此过程中，授权应用可以获取 Facebook 的个人信息数据。一家名叫「剑桥分析」的公司，利用这些用户数据，建立分析模型，以个性化政治广告为目标，对用户投放可以产生共鸣的推送信息，从而达到影响选民的目的。

当时，5000 万用户占了 Facebook 整个北美地区活跃用户的三分之一，占了潜在美国选民数量的四分之一，可想而知，这次事件的影响之广，程度之严重。这个「灰犀牛」事件，最终给 Facebook 带了天价的罚款和一系列信任危机。

第二，人为操作风险。

人为操作风险可能是产品经理日常工作中最容易遇到的问题了。我们的一丁点小小的失误，都可能在产品应用范围内造成重大的影响。

腾讯也曾经吃过亏。比如在快讯消息的 Push 文案中，漏写了伤亡数字，导致「一场台风致全省死亡」这样的乌龙信息登上热搜，官方立即澄清致歉；

又比如在产品经理与开发同学的沟通中，由于双方各自对「12 点」这个时间概念的理解不同，产品经理定义的是当日结束的 12 点，开发同学理解的是当日凌晨开始的 12 点，从而导致产品逻辑中，用户使用时间有一天之差，整整 24 小时内可能产生的潜在收入，被拒之门外。

还有一些极端的「黑天鹅」事件，比如因员工的个人情绪或道德品质，而擅自触发的产品问题，像删除数据库、恶意串改数据等行为，更是可能会为公司带来不可挽回的损失和重大危机。

第三，资金风险。

资金风险一般容易发生在营销活动的场景中。我们需要推敲每一个资金消耗的细节逻辑与玩法规则，否则一个小小的规则漏洞或者边界 bug，都可能导致活动资金的大量无效流出，给公司带来直接的经济损失。

2018 年，魅族就发生过类似事件。为了配合一款新品的推出，公司策划了一次营销活动——前 100 名预购手机的用户，只需要花费 5 毛钱就可以购得手机；然而，活动推出后，却发现付款 5 毛钱就能下单的，远远不止前 100 名用户，有近千人都下单成功了！最后，公司追查发现了 bug 并进行了相关修复，但承诺已下单的用户，还是正常发货，这其中的损失，就由公司承担了。

这类「冤枉钱」不仅可能发生在官方的失误中，社会上还存在一波专门针对互联网产品的黑产集团，他们随时都在搜寻产品中可能存在的资金漏洞，从而加以利用、谋取暴利。2019 年初，就有黑产团伙利用拼多多一个过期优惠券的漏洞，盗取数千万元平台优惠券，进行不正当牟利，成为一场不小的风波事件，再次为互联网平台的资金安全与系统安全，敲响了警钟。

第四，合规风险。

一般来说，涉及内容、金融、民生的产品，需要重点关注合规风险。这里首先需要知道哪些政府部门或机构，会对我们的产品提出合规要求，再根据具体的合规准则，来评判产品是否在合规范围内。一旦越界，产品可能直接会面临被关停或整顿的风险。

像 2019 年，视觉中国这家在图片市场领域占据绝对优势的上市公司，由于给「人类首张黑洞照片」以及国旗、国徽等图片都标注了版权所有，导致公司陷入「版权门」事件，多次被政府有关部门约谈，整个网站暂停服务、全面整改，带来不可挽回的重大损失。

第五，公关风险。

公关风险，一般都发生在对外公关之时，由于一些言论不当、未及时回应等问题，导致公众信任和口碑危机。这里需要特别警惕，当已经出现危机，正在进行危机公关时，再次出现公关风险的话，会让之前的问题进一步恶化。

知名作家六六曾经在微博上吐槽，自己在京东上购买的天天果园水果是烂的，要求退款却被拒绝；事件舆论发酵后，天天果园和京东都主动联系六六和解退款，却被六六拒绝，接着她又发布了《我要的是公平》的文章，事件二次发酵，天天果园公开致歉，京东也转发了这条致歉微博。然而没想到事件还未平息，后续王思聪也转发了六六的微博，说自己也遇到过类似的情况，第二天，京东官方就给王思聪致歉，引来了更多质疑：为什么王思聪就能得到公开道歉？「看人下菜碟」的帽子，就这样戴在了京东的头上。

所以你看，不仅做产品需要站在用户的角度去考虑，做公关同样如此，需要首先考虑到用户的立场与利益，出现问题第一时间澄清事实，公开表达诚意，更容易获得用户的理解和谅解，避免让公司陷入舆论危机。

产品风险管理四步法



知道了产品工作中可能涉及到哪些「灰犀牛」，那么我们可以如何来规避这些风险呢？

这里，我们提出相对通用的产品风险管理四步法，不管是哪一类风险，我们都可以按照这样的准则，来规范我们的工作，让「灰犀牛」尽量远离我们。

1.时刻保持风险意识

风险管理的第一步，首先要知道我们会面临哪些风险。像上面提到的信息泄漏风险、人为操作风险、资金、合规与公关风险，都是我们可能会遇到的一些风险方向，除此之外，由于各个业务的特殊性，可能还有一些风险项是非常特殊且个性化的。这就需要我们深度理解业务，知道我们的风险来源，时刻保持应有的风险意识。

2.建立防范流程

知道了风险来源后，我们就可以根据每一个风险方向，来追溯风险可能产生的情况，反向推导出我们的防范流程。

比如防范信息泄漏风险，我们就需要特别关注用户隐私信息的严格评判和保护，要梳理清楚产品和技术上可能存在哪些漏洞，会对用户的数据安全造成威胁，要制定在数据存储、上报、治理上的各类规范流程等等；

又比如防范人为操作风险，我们可以建设多重审核机制，来规避单人出错带来的直接影响；

还比如防范合规安全风险，我们就需要在日常工作中多关注政府的监管政策，定期与监管部门进行沟通，了解合规准则的变化，随时调整产品策略。

3. 尽量采用系统化的保护机制

在防范流程方面，在资源允许的情况下，我们要尽量采用系统化、产品化的保护机制，把明确的质检逻辑、判定逻辑交给计算机，从而再次降低人为流程可能出现的二次错误，同时也降低人力成本，提升团队产出效能。

4. 合理妥善地应对危机

如果最终我们还是百密一疏，由于失误引发了危机，我们就需要立即投入应对危机的流程中，第一时间解决问题，特别是跟用户关联度比较高、程度严重的问题，更是需要团队全力补救；

其次，我们需要做好内部的信息传达，将出现的危机问题第一时间上升或暴露给相关团队，让大家知悉，并共同促进问题的解决；一定要警惕、避免把问题藏着掖着，最终导致问题进一步恶化；

再次，必要时，我们也需要开启公关处理机制，对外发布消息澄清事实、诚意致歉或解释缘由，合理妥善地应对危机。有时候，危机公关也可能变成一次机会，让用户或行业对产品有一个全新的认知。像之前提到的 Facebook 信息泄漏事件，虽然是公司的一次重大危机，但扎克伯格在美国政府组织的听证会上，完成了一场堪称教科书级别的危机公关，不仅为 Facebook

重新赢得了口碑和信任；同时，还使得 Facebook 的股价飙升回暖。可见，危机公关是团队弥补错失、拯救危机的一次至关重要的行动。

总结

今天这一讲，我们认识了产品工作中可能会遭遇的、类似「灰犀牛」事件一样的潜在风险——信息泄露风险、人为操作风险、资金风险、合规风险、公关风险；

也提出了产品风险管理的四步法——时刻保持风险意识、建立防范流程、采用系统化的保护机制、合理妥善应对危机。

课后分享

你在之前的产品实践中，又曾经遇到过哪些风险问题，它是怎么产生的，给你们团队带来了哪些启示呢？欢迎在课后评论区与我们分享。

悬念预告

到这里，「找-比-试」三步法中「试」这一模块，就要接近尾声了，下一讲，我们将带来这一模块的【避坑指南】。

恭喜你又学完一节课，如果你觉得有收获，别忘了分享给更多的朋友，共同成长进步。

