### **小规模团队如何开展信息安全工作？**

# **一、小规模信息安全团队的特征**

**1、人数少，专职少，编制少**

不算可支配的外包人员，专职信息安全总人数少于等于3人，或占企业人员比例小于千分之二（经验数据；IBM很久以前给出的建议比例是千分之2.7，但现在也找不到可类比的数据了）。据了解，甚至会存在1个人的 “信息安全团队”。

**2、企业年信息安全投入少**

（不含人力投入）少于200万，或占企业年营业额比例少于千分之一。（经验数据：金融企业IT年投入通常是年营业额的1-3%，安全类投入通常是IT投入的10%左右。）

**3、没有独立的实体部门或行政编制。**

大概率是IT部门的几个人，更大可能落在IT运维部门。

1. **团队成员普遍身兼多职，或多个岗位的工作内容。**

有可能是一人兼多个信息安全岗位的工作内容，有可能还会兼任合规、风控、运维等岗位，甚至还可能干文员的活。

# **二、小规模信息安全团队常见的困境**

****1、有短期、明确需要解决的信息安全问题，但缺乏长远的信息安全路线图。****

既然有专职信息安全人员，说明企业管理层已经意识到了信息安全风险的重要性，或者曾经出过事，所以通常短期之内有明确需要解决的信息安全问题。但是由于工作职责（组织架构相关）不清晰、资源能力不足等问题，对于信息安全人员（或团队）未来应该干什么、解决什么问题，要么不清晰、要么缺少一个路线图，导致信息安全工作总体上偏被动，属于事件驱动型或合规驱动型。

****2、资源少。****

“事多人少钱难要”是典型特征之一，有时也仅仅是“人少”，有时仅仅是“事多”。究其原因，可能

（1）信息安全在企业业务中的重要性还不够突出，伤的还不够痛，领导的专业能力不足，导致领导认知不到位、投入不够；

（2）金融行业由于监管或编制原因，往往有专职的安全人员，但是正编较少、外包人员多；据称很多城商行、互金企业都存在“1人信息安全团队”的情况。这时管理外包商、内外部的沟通可能就会耗费大量精力，反而无法集中精力开展建设，有可能会出现供应商管理风险，或者是核心能力丧失的问题。

（3）企业经营和盈利能力不强，虽然领导重视、但是手里能花的钱都得精打细算，但凡花点钱都想一分钱掰成2分钱用。比如这些年的互金行业、游戏行业活的其实挺艰难，除了几个巨头之外，其他企业能活下来都挺不容易，在安全上的投入是真的紧张。

（4）信息安全人员和领导对于“资源”一词的认知不一致。在我以前的文章中提到，信息安全人员往往把“资源”等同于“人、钱”，但实际上资源还包括“物、政策，内部支持者、供应商&合作商资源以及管理层在信息安全事务上投入的时间精力”；

（5）信息安全人员自身追求职业发展和企业经营需要之间的落差。作为一个摸爬滚打了十几年的业内人士，我深刻理解一个专职人员希望年年做事、做新鲜事情的感受，于是不断地发现新风险、期望做新项目、希望扩大团队，但是管理层需要的只是把风险控制在可接受程度、而不是彻底消灭，这时往往就会产生落差；

（6）监管部门这些年逐步加强了互金、游戏行业的监管力度，从等保、客户信息保护、网络舆情安全等等各种传达要求、开会、检查、整改，从银保监、央行到网监、网信办，虽说确实提高了行业的安全水平、控制了行业风险，却也给这些企业带来不小的管理成本，相比就容易感觉到资源不足。

****3、人员流动大、留人难。****

如果是大公司、小团队，有一个较好的事业平台或薪资待遇支撑，那可能这个问题还不够突出。如果是小公司、小团队，本身的平台和事业空间有限，薪资待遇很大可能也就中等水平，做几年估计就差不多了，想留住人非常困难。

****4、自己能力不够，或者面临挑战多、漏洞多、问题复杂。****

基于问题3，小规模团队大概率就会遇到人员能力不足或者人数不够，“事多人少钱难要”；或者由于信息安全工作在内部的职责、定位、协作关系不清晰，手里也缺乏足够的资源使得话语权不够，看上去就会挑战多、问题复杂。

大概率的情况下，一个公司设立专职信息安全人员之前，其实信息安全并非从0起步，多少还是推行过一些信息安全要求、部署了一些工具，但一定在执行中遇到这样那样的问题。那么，设立专职人员之后，如何整合、优化这些信息安全要求和工具，如何解决这些问题，如何保障内外部用户体验的前提下有效控制风险，也使得问题更加复杂。如果公司的信息安全是从0做起的，那么从哪里入手呢？

# **三、小规模信息安全团队的工作思路**

问题分析完了，那么如何解决这些问题？谈谈我的思路。

****1、挑个好的团队带头人。****

不管是1个人的团队，还是2-3个人的团队，事以人成，这个带头人极其重要。兵熊熊一个，将熊熊一窝的道理大家都懂。这个带头人必须（1）热爱信息安全，承压能力强或者热爱接受挑战；（2）具备信息安全专业领域资深经验，在行业内有较好的人脉资源；（3）既能向上沟通，也能向下管理；有全局视野；（4）具备动手能力，毕竟小团队工作的时候，不能只动口、不动手。在金融、互金、游戏行业里面，我觉得还必须具备一定的技术能力，虽然不一定要很专业，但像CISSP/CISP那样的知识宽度还是要有的，至少可以保证不会被忽悠。

****2、做个规划，明确2-3年内重点解决的问题、架构、路线图。****

如我以前的文章所述，这是我解决问题的一贯套路，先从全局着眼、把整体布局做好。规划中要明确信息安全工作的价值、定位、目标，和2-3年内需要重点解决的问题（风险）、信息安全架构和路线图。尤其是小规模信息安全团队的工作，尤其在金融、互金、游戏行业里面，安全团队极大可能就是IT团队的补一份，因此就整个公司IT基础设施的架构达成一致就非常非常重要。推荐采用EA的方法论去分析和搭建，这样可以保证安全项目的实施效果不会偏差太远。如果自身能力还不足以做这个架构和路线图，可以找大牛或咨询公司。

这当中尤其需要注意和IT部门、人力资源、行政部门达成目标、分工合作机制的一致，IT部门与IT基础设施的建设和运营相关，人力资源和员工培训、奖惩相关，行政部门和物理安全管控相关。必要的话，可以采用联席会议（温和的沟通机制）、绩效考核（强硬的保障机制）等手段保证目标一致。如果这样还是做不到，可以争取在公司现有的管理机制（比如经营例会、风险例会）上争取一个议题，每次都能讲十几分钟、半个小时，通过不断地宣讲来统一思想、统一目标。

如果领导的想法特别多，但是又不太愿意（或不能）投入更多的资源，其实这时蛮考验团队负责人的沟通能力。常规的做法，就是把信息安全风险仔细做个风险评估，可以自己做，也可以请外部咨询公司、安全公司做（大部分时候外面的人说话管用），或者是带着领导去参观学习同行标杆企业，然后跟领导一起把最重要的风险识别出来、定下来。

****3、以合规驱动为主，提纲挈领地解决核心问题****

虽然大家都说新官上任三把火，但是感觉不适用于信息安全小团队的运作。我们的第一件事情是站稳脚跟。如何站稳？就是首要解决管理层关注的重点问题、紧迫问题（我称为“核心问题”）。如何解决呢？我的观点是****以合规驱动为主，一边解决核心问题、一边搭建架构****。当然，做起来肯定不是面面俱到，而是要提纲挈领。具体怎么做呢？

就“合规驱动”而言，就是利用监管机构出具的各项指引，或等保测评标准，从制度体系、IT基础架构到安全组织、人员意识逐步、从虚到实地做起来。这些“规”都非常体系化，所以合规的过程本身就是一个体系化的建设过程；同时由于“合规”这个动作对于金融、互金、游戏行业来说也是一个强制性要求、必须要被满足，因此可以在这个阶段，借助合规驱动的机会，顺带着把架构性的问题基本解决，还能获得资源支持。

那么什么叫“提纲挈领”呢？还是围绕前面提到的“管理层关注的重点问题、紧迫问题”这些核心问题，在解决问题的过程中逐步地实现整体架构的改进。比如要优先解决“保护客户数据不泄漏”的问题，那可能就需要实现终端安全的基础防护+数据防泄漏+准入控制，网络要划分安全域并设置访问控制策略，互联网边界先做到可以应对普通攻击，应用要分级、隔离、做到数据不落地，这几个大方面的改进完成了，基本上整个架构就搭起来了，即便在推进过程中遇到阻力，也会因为这些任务是为“核心问题”服务而化解。做完之后，再逐步推进数据分类分级脱敏审计、应用系统开发标准和代码审计、NTA分析、应对APT、攻防对抗、部署蜜罐、态势感知等高阶动作。

这当中有几个注意点：

****（1）总体上遵循架构。****这里主要说的是IT基础架构，这样可以保证安全控制措施的协调性、有效性；但是各个部分的推进可以根据实际情况、尤其是IT部门自身的业务规划来调整。

****（2）可以先把制度体系建立起来，完成立法。****为什么这么说呢？因为首先需要合规、满足监管要求；同时也可以在建立制度体系的过程中，对照业内标杆或者最佳实践，把企业自身的差距识别出来，形成后续改进的依据。对于工作推动所需的资源抓手（比如硬性的培训要求，对员工的奖惩权），务必在这个过程中搞定。当然，制度体系的落地需要较长的时间，这个下面再说。建制度体系这个事情，可以请咨询公司做，也可以花点小钱买一套再改改，先保证有东西。

****（3）协调好业务需求跟合规需求。****金融、互联网金融、游戏等强监管的行业的合规需求和业务需求到底谁轻谁重？我没有实际经验、说不好。但是如果企业经营形势一般，似乎还是应该优先满足业务需求，先使得企业在大体合规的状态下生存下去，这时就需要和管理层、监管机构建立良好的沟通。

****（4）与核心干系人保持密切沟通，获得管理层和业务部门的支持。****与核心干系人保持密切沟通、汇报进展，不但可以展现成绩、暴露问题、推动问题的解决，还可以持续对管理层和业务部门主管进行意识教育。很多安全工程师往往只顾埋头做事、不管业绩展现，是导致“缺乏资源”的根本原因，也是我一直强调的安全人员要有管理技能和管理视角的原因。与核心干系人保持良好的关系，也为后续的信息安全工作开展找到了更加有力的支持者，而这也是我所说的“资源”之一，而且是重要资源。

****（5）做到PDCA。****凡事要闭环、要PDCA转起来，这是信息安全管理体系最重要所在。风险是否得到控制，要通过运营、检查、审计等综合措施运行一个阶段（一般是半年到一年），以实现闭环。这样既可以保证问题真正得到解决，又可以让老板、业务主管等核心干系人放心，他们会觉得你靠谱，后续对信息安全工作的支持力度也会更好。

****4、关于应用安全、业务安全****

互金、游戏行业的业务开展非常依赖互联网，因此往往对应用安全、业务安全（比如第三方非法接入、薅羊毛、借贷欺诈、内容安全等直接影响企业利益的问题）看的很重，而内部的IT基础设施、办公应用反而比较初级：要么用SaaS服务搞定，要么用大厂的企业邮箱，或者基于企业微信、钉钉满足绝大部分办公业务；金融行业也越来越加大互联网应用的投入。在这种局面下，小团队应该如何开展这方面工作？我提几个想法：

（1）能花钱解决的问题，就不要自己干。从App安全、应用系统安全、抗DDoS攻击、内容安全，安全厂家都有成熟解决方案，拉过来用就可以。如果有精力就货比三家，没精力也可以全包给一家。

（2）如果应用是自研的，那么就要和测试团队、质量控制团队合作，在测试或QA环节把风险控制住。该定标准定标准，该用自动化代码审计工具就用。

（3）如果管理层确实对应用安全、业务安全重视，可以把这个作为短期内的“核心问题”，按照等保或者ISO27001的要求，先制度标准、工具平台、意识教育等几个领域做起，容易看到效果、也容易得到资源支持；然后再解决内部的终端管理、网络架构、服务器管理、数据流管理等。这是一个切入点、突破口选择的问题。

（4）用好事件营销。一方面及时响应、处理事件，一方面用事件驱动体系化的建设，但对团队在这个阶段的数据分析能力、风控能力、响应能力有较高的要求。

****5、用好事件驱动，逐步补全信息安全管理体系的短板。****

刚才提到了核心的“点”的问题，下面谈谈如何解决“面”上的问题。一般来说，除了核心问题之外，多少还是有其他一些信息安全风险需要面对和控制。资源投入还是要关注，但不建议超过20%；从解决方式来看，我认为这些问题用“事件驱动型”方式来解决，效果和效率更好。还有一种情况，就是企业已经大体上满足合规要求了，如何做的更好更深入，往往还需要事件驱动。

以我所见，即便是对信息安全很重视的领导，也通常是优先解决能看到的风险、已经发生了安全事件的漏洞，毕竟资源都是有限的。因此，通过持续的事件驱动一个一个问题的解决，或者是更加深化地解决。逐步积累之后，就会连点成面，有点类似“农村包围城市”、“积小胜为大胜”的套路；同时，通过一个一个事件的处理和改进，不断地对员工、主管进行安全意识的教育，也是非常有效果的。再反过来想，如果信息安全工作的上级领导要去驱动同级的其他部门领导，他是不是也需要“事件”这个武器？你给领导提供资源，领导才能给你支持嘛。那么，如何才能获得这些事件呢？

（1）专项审计，包括调研访谈、现场查验。这不是审计部的活，是安全团队应该干的；

（2）运营和巡检。别看是日常工作，“安全无小事、出事必然都是大事”，如果在小的地方持续出问题，那说明一定是运行机制或人员意识上出了问题，需要立即纠正；

（3）渗透测试。比如可以策划模拟真实的钓鱼邮件等社会工程学的攻击，看看到底有多少人中招，然后把数据摆在领导面前，让领导真实感受到触目惊心的结果；比如可以集中资源抓2个月的上网数据分析，把互联网出口造成的信息泄露结果呈现在管理层面前。

（4）接收外部的漏洞报告、威胁情报。接收、评估并解决一个漏洞，并向管理层汇报，既是成果展现，也是意识提升。

（5）搜集并展现同行案例。同行案例、身边人的故事，对老板、主管最有说服力，所以要和圈子里的同行多交流。监管机构也会经常通报一些案例，也要用好。

以上“事件”应该保持至少每季度一次的频度，太频繁了就会“风险疲劳”。通过每一次事件触发的安全改进，逐步地把信息安全管理体系的短板补足，把PDCA的循环转起来，把“虚”的制度转变为“实”的执行，把“书面的控制项”变为“有保障的控制点”，减少事件的发生、减少重复事件的发生，进而实现螺旋式上升。在本文编写过程中中，谢涛提出****“小团队的安全从来就不是技术问题”****的观点，发人深省。

****6、组建团队、用好外部专业力量。****

组建团队不能太着急，要持续关注、找合适的人。小团队的人，我认为要招喜欢信息安全的、学习能力强的，经验不一定要太多，这样相对稳定、有忠诚度；校招也是一个非常不错的途径。对于金融、互金和游戏行业来说，招聘次序上来说建议先招运营，做策略、技术、意识宣传的按需补充，最后招审计人员。

建议小团队就不要招渗透测试的人了，还是用外部专业力量好。如果遇到疑难杂症需要解决，找咨询公司或者大牛咨询一下，其实基本就解决了，不必招大牛。说到大牛，我有个不成熟的想法，下一篇讲讲。

团队负责人平时要特别注重团队建设，总得在事业平台、团队氛围、薪资待遇的某个方面让员工有成长和收获吧？平时还要注意学习业务知识，让团队成员逐步树立“信息安全要为业务服务”的意识。特别还想说的，团队负责人一定要学会如何与90后相处、沟通，既能更好地管理团队，也能够让自己保持年轻的状态。

团队成员要多交一些圈子里面的朋友，一来有问题可以寻求咨询和指导，二来也可以让自己多一些解决问题的选择、或者掌握更多的信息。

这里有一个问题就必须讨论到：很多金融企业正编非常少，必须依赖供应商的外包人员，且人数还不少，随之而来的问题就是（1）外包人员是否可信；（2）如何让外包人员尽责；（3）自身团队人员长期只做外包商的协调管理，核心运营能力丧失，容易人走茶凉。对此我的建议如下：（1）与外包公司前述保密协议、落实责任；（2）对接触核心业务的外包人员要有背景调查；（3）将外包人员的KPI与团队成员的KPI保持一致，并建立激励机制（比如在合同中约定：完成日常任务拿100%收入，有突出表现可以多拿20%）；（4）从生意、技能、帮助外包公司的成长，双方结合成长期的伙伴关系，提升互信；（5）如果始终认为外包只是外包，那就设定一个可行的计划，让团队成员逐步负责安全策略、安全运营等核心工作，将外包的安全能力内化。

****7、尽量用标准化、商业化的技术产品和服务，尽量自动化。****

小团队在信息安全建设过程中，尽量采用标准化、商业化的技术和产品，少定制化、少自己开发，少用开源工具。大量经验表明，把工具用足用好最重要，不要想着买最好的工具。对于小团队来说，实用是第一位的，应尽量选择架构简单、学习成本低的工具，那种需要投人进去琢磨、研究的工具平台看着美好，但不适用小团队。开源工具虽然免费，但是需要时间琢磨研究、非标准化的做法也会带来架构上的风险漏洞，搞不好还会引入供应链风险。

不要一开始搭太多工具平台，成本高、项目多，效果还不一定好。我建议在团队初创期间，人均负责运营的工具平台不超过2个。但同时，我认为也要敢于打破旧的束缚，如果以前上过一些工具、平台，在保证投资收益比的前提下，该废止就要废止，能利旧还是要利旧，千万不要在这方面有束缚。如果团队人员规模始终控制在2-3人，一定要想办法整一套运营或监控工具（至于它叫SIEM、SOC、态势感知还是大数据分析平台，就是萝卜白菜各有所爱了），起码要达到“事中及时响应、事后快速回溯”的效果。

能快速用起来的、自动化的工具，只要能够满足当下关键需求就先上，切记多头出击还都是手工活。自动化的好处就是团队可以把更多的精力放在沟通汇报、协调资源、救火上。

****8、中后期的团队管理****

等到团队成员达到4个人左右的规模，就可以逐步形成这样的分工：团队负责人主管向上沟通协调、资源协调和团队管理，同时可以负责数据安全、业务安全等需要高端资源协调的工作；A负责项目管理、制度文件管理、意识教育，B负责IT基础架构的建设、项目评审、SDLC，C负责审计、应急响应和调查，运营的工作可以根据实际情况让每个人都承担一部分。ABC的工作还要注意形成互相备份，这样不至于在人员流失的时候耽误工作。同时想办法把琐碎、低价值的工作交给外包人员去做，或者交给公司内部的低价值岗位（比如文员、行政前台），或者尝试利用一些工具、改进一些工作流程来提升这些琐碎工作的处理效率、降低对团队人员的时间精力占比。

时间久了之后，团队成员不免面临流失的风险，因此仍要保持对可用人才的关注，可通过校招等途径适当补充。随着团队人员价值的逐步实现，在安全专业平台上的发展空间已经不大，可以考虑这几种方式（1）公司内部轮岗，安全的人去干运维，运维的人来干安全，横向扩展团队成员的技能和视野；（2）努力提升团队成员的薪酬待遇水平，以保更好地留人员。经验数据表明，安全人员的薪酬上限和公司的人均产出是基本相当的，这时就需要团队负责人多想想办法了；（3）对于团队负责人来说，去从事和安全相关的工作内容（比如合规，比如业务风控），可能也是一个选择。

如果团队成员+外包人员规模应该要增加、但始终上不去，一方面要找找自身原因、看如何改进，一方面其实也可以琢磨琢磨是不是应该动一动了。

****9、逐步地过渡到关注和解决业务安全问题，找到更大的价值空间。****

当信息安全团队的短期目标实现，就要考虑下一步发展的问题。从情理上来说，都希望扩大团队、争取更多的资源、实现更大的价值，但我还是建议团队负责人能够以务实的态度看待这件事情，毕竟这个必须建立在企业大规模发展和盈利的基础上，不要盲目追求扩大团队和资源。

如果希望找到更大的价值空间，那必须要结合行业发展趋势、企业经营战略和对未来风险的认知，在与安全密切相关的方向上整合资源和能力，做一些技能、工具或外部资源的调研储备，或着力帮助公司业务的提升，比如合规、风控。但其核心思想依然是我之前提到的，“保企业增长，保企业核心竞争力”。至少在需要你灭火的时候能顶上去，也就为团队打开了一片新的天空。如果找不到，该功成身退也就退吧，把机会留给其他人。

****10、向上管理、以及对监管的驱动****

金融、互金、游戏行业的小规模安全团队，大概率在IT部门，也容易面临级别不够、跨部门推动困难等困难。在和几位业内人士沟通的时候，都不约而同提到了这一点，同时提到了目前最大的难题就是“数据安全”推不动。

为啥推不动？1自身级别不够；2就是虽然别人出了很多事，但企业管理层还不够痛，外力不够强；3企业管理层认知不够，或者企业经营顾不上这个事情。但是“数据安全”这个事情真的不敢出事，一旦出事很可能就是灭顶之灾（这个说法可能有点夸张，但安全从业人员应该有这样的意识和责任感）。那怎么办？考虑到金融、互金、游戏行业有很强的合规驱动性，也必然需要和监管机构保持良好的沟通，我的建议是：

（1）安全团队成员应坚持向上管理和沟通。积极地、在不同场合向管理层沟通和灌输数据安全的重要性。如果是我，会在恰当时机安排对管理层的个人信息利用的渗透测试。

（2）业内同行应该形成合力，持之以恒、想法设法驱动监管机构对“数据安全”的重视，以监管的力量（合规、奖惩、排名措施都可以）来促进“数据安全”水平的提升。在“数据驱动业务”的时代，数据安全应该早下手，安全建设和系统平台建设同步开展，不能再走先建设、后补课的路子了，这一点相信监管机构也是有认知的。