



**中国-2016年**

**Cybersecurity创业调查报告**

# 目录

序.....	4
前言.....	10
致谢.....	11
一、 报告简介.....	13
1. 报告目标.....	14
2. 报告范围.....	14
3. 报告方法.....	14
4. 结果简述.....	14
二、 产业概述.....	16
1. 全球网络安全产业规模.....	16
2. 全球网络安全创业投资.....	17
3. 中国网络安全产业基本布局.....	18
4. 中国网络安全产业发展规模.....	19
5. 中国网络安全产业政策环境.....	20
6. 中国网络安全产业发展预期.....	23
三、 数据分析.....	24
1. 创业项目.....	24
2. 创业人才.....	28
3. 创业挑战.....	34
4. 创业投资.....	38
四、 趋势观察.....	43

1. 网络安全行业最新特点.....	43
2. 网络安全创业投资热点.....	44
3. 创业者应关注的问题焦点.....	46
4. 各方观点.....	47
5. 总结.....	53
<b>附录：</b> .....	<b>58</b>
1. 近年来国际网络安全初创项目（部分）.....	58
2. 近年来中国网络安全初创项目（部分）.....	60

## 序

安在做中国网络安全创业调查报告，是因为一直在做创业新锐的系列报道。

原本做人物报道只是尽到专业新媒体之本分，但在此过程中，我们越来越觉得，互联网+和双创大潮，席卷的不仅仅是互联网相关领域，也实实在在地包含了网络安全这一“特殊”行业。说它特殊，实在是因为爱恨交织太久了，爱它才投入其中，恨它因它迟滞而不得发展。而现在，彼时的“特殊”正在变化，就像坚冰终于化开，它开始萌动和催生，甚至要开花结果了。

而置身其中，给这种变化“添油加醋”一番则成为兼具专业背景和媒体意识的安在的必然所想。到底该怎样“添油加醋”？作为咨询顾问，做一份高品质的调查报告首当其冲。于是，经过两个多月的紧张准备和实施，这份“菜品”终于端上桌了，热热乎乎，满满当当，诚意足够，品相尚可，至于是大菜还是小点，就要众多“食客”来品鉴了。

餐前总得有个引子，伙伴们说，那叫“序”。写点什么呢？第一时间跃上心头的，就是此前在安在微信公号里发过的一篇文章，是写给创业新锐的，感觉比较贴切，也算应景，好吧，那就它吧。

安在有些变化，看出来了吗？

最近连着发了三辑访谈，分别是瀚思的创始人高瀚昭、白帽汇创始人赵武、微步在线创始人薛锋。首先是标题变了，从“人物”跳跃到了“新锐”，其次，我没有再每次必写“采访手记”，而是等待一个恰当的时机。

什么时机？就是想想明白，安在正在做什么？以后还会做什么？

现在明白了吗？当然，很清楚了。

我们在寻找新锐，走访新锐，报道新锐，我们在做并且要更多地向大家呈现这个行业不同以往的新气象、新风尚和新趋势。

网络安全，求新待变。

网络安全，呼唤新锐。

其实这个念头不是一开始就有的。

仅仅两个多月之前，我都还不觉得中国网络安全有什么创业新锐。虽然这两年安全很火，

从上到下，整个产业界貌似群情激昂，但中间一度我很怀疑这是不是虚火？政策红利首先授益于既得利益，大牛人物和专业人才纷纷被 BAT3 收拢，云计算和大数据安全更多成为传统企业用于换汤不换药的“新概念”包装，有创业，但并不锐，很锐的人又多属于成功的大佬级企业，加上下半年互联网投资风变，创新创业环境趋冷，我更是强化了这样的印象，创新创业似乎与网络安全无关。

但当我走出去转一圈后，才知道，这真的是一种错觉。

当我走访中国网络安全 20 年发展历程中那些大 V 级影响力人物，从他们口中屡屡听到，某某某创业了，某某某又做了个有趣的东西，某某某拿到了 A 轮融资，当我微信通讯录加进来的认识和不认识的朋友越来越多，在微信群和朋友圈里眼见着不断发生与网络安全相关的各种新鲜事儿时，忽然觉得，也许我曾错过，但现在，我绝不能再次错过。

事实上，现在的网络安全界，正在经历一次前所未有的时代变革，傲立潮头的，是许许多多虽微小但却泛着亮光并且正在积蓄力量快速壮大的浪花。

如果说影响力人物代表着中国网络安全的昨天和今天，那我正在寻找并不断发现的，也许正代表着网络安全的明天。

我需要做的，就是带着一种好奇与欣喜，找到他们。

明天安在？新锐安在！

各行各业都有新锐，不同时期也都有不同时期的新锐。

对网络安全来说，什么是新锐？谁是新锐？

我不想用类似 80 后、90 后这样的年龄断代去定义新锐，首先想说的，新锐与年龄无关。再年老的“顽童”也会很新很锐，而再年轻的“世故者”呈现出的却是老迈。比如高瀚昭，和我同是 73 年人，在年轻人眼里堪称大叔甚至大爷了，可他在创业，他是新锐。甚至之前有好友提到的，像西安交大的马民虎老师，年龄虽长精神不老，虽不是创办企业，但在中国网络安全法律开拓上，却正创造着一番事业，他也是新锐。至于说年轻一代，只要是开拓创新有所独到，只要是不拘世俗勇于创业，都可能被归入新锐之列。

当然，我们还是要给新锐一个稍微清晰点的设定。

新锐一词的英文是 Aggressive，意为敢作敢当、锐意进取，多被用于各大排行榜上对具有 Aggressive 精神、作风和态度的人物的统称，特指各个领域的后起之秀和栋梁之才。

在我看来，“新锐”首先要新，对网络安全来说，最近两三年是个大致的界别。倒不是说两三年长短如何，而是恰好这个时间段属于“蜕变”的阶段，前有启明星辰、绿盟、天融

信等“功成名就者”，后有 BAT3 这样的互联网大佬们处处求“+”，什么都在变，网络安全亦如此，而在这变革时期的积极求变者，即可谓新锐。

其次，“新锐”还要锐，正是在变革时期，在各种“新旧势力”的夹缝中，若没有些勇气和棱角，没有些突破和创新，那是断难形成气候的。因为前无古人，所以才要做新的来者，因为有铜墙铁壁，所以宁愿头破血流也永不回头。

既新鲜且锐利，是为新锐。

瀚思的高瀚昭，算是网络安全老兵了，从外企出来做大数据安全，誓要颠覆传统 SOC。白帽汇的赵武，在华和 360 一番宝剑磨砺，曾经的挖漏高手要做新一代安全创业的排头兵。微步在线的薛锋，曾高就亚马逊中国 CSO，“冲动”之下一朝创业，坚信能够引领威胁情报发展之最新潮流。他们都是最近两年起步的，都无惧传统安全企业和互联网大佬们的重重“夹击”，都是新锐。

还有更多，比如第一个吃螃蟹要做网络安全电商的威客安全的创始人陈新龙，荣登福布斯 30 位 30 岁以下创业者排行榜的漏洞盒子创始人袁劲松，屡次突破 IOS 系统的“越狱”者——盘古团队创始人韩争光，等等。

新锐不少，新锐很多，在网络安全这个既老又新的行业，他们涉足大数据、云计算、移动互联、物联网、车联网、工业控制等相较以往更为广泛的领域，他们虽起步不久，但却“咄咄逼人”，有着舍我其谁、势不可挡的崭新气象。

大潘前阵子曾有过一个论断，说网络安全正从战国时期“重返”春秋时期，这里所谓的“重返”，并非倒退，恰恰相反，是在一个更新的时代和更高的层次上，网络安全行业所呈现出来的新一轮“百花齐放”。

所有的新鲜事物都是值得关注甚至讴歌的，而所有的新锐，也都是值得期待的。

那么，问题就来了，为什么会有创业新锐？似乎是一夜之间，他们就冒了出来？

除了说原本就在那里、只不过之前我太过封闭孤陋寡闻之外，在和几位创业者交流之后，至少以下几点可以道出其中玄妙。

首先是创业起点的变化。以前也有创业，但要么昙花一现，要么艰难度日，要么最终被“招安”，比如大成天下的吴鲁家、瀚海源的方兴、安全宝的吴翰清，都是技术大牛，都有不错的创意，但也许只是生不逢时，未能一如初愿地蓬勃发展。那现在呢？起点不同了。比如高瀚昭、赵武和薛锋，都有在外企、互联网企业长期从业的经历，懂技术，会运营，精管理，多资源，有人脉，都是既有“逼格”又接地气的，正是这样的积淀，使他们能够一开始就站在一个相对的高地，别人想学也学不来。

其次是资本市场的巨变。说巨变一点都不夸张，以前创业最痛苦的就是缺枪少粮，求爷爷告奶奶都没用，传统融资渠道如银行是不对草根创业者开放的，现在呢？随便一块砖扔到中关村创业大街，倒地的十有八九都是投资商。所以我们看到，像高瀚昭、赵武和薛锋他们，除了自身积累外，创业伊始已经有资本跟上了，天使轮、A 轮很正常。当创业者不再靠简单的“原始积累”缓慢求生，而能借资本的力量快步发展时，从 0 到 1 就相对容易多了。

再有就是市场环境的改善。个人觉得，自从国家高调支持网络安全，自从互联网+逐渐扩展深入，这上上下下方方面的市场环境就开始化冰、萌动甚至盘活了。很简单一个例子就看得出来，像乌云开启的安全众测模式，以前被怀疑、不屑甚至打压，现在呢？随着漏洞盒子、Sobug、360 补天、雷神等诸多平台的出现，一时间众测模式蔚然成风，为什么？有需求有市场呀！那其他呢？比如移动安全、大数据安全、云计算安全，技术在发展，时局在变化，网络安全早已经泛化为全民性的共识，由此带来了增量市场，催生的自然是创新创业了。

最后还有一点，就是合作的可能大大提高。以前我们诟病网络安全行业，多是说它的封闭和割裂，根本不是个完整的产业链。现在呢？你要做大数据，离不开与数据源的合作，离不开与应用场景的结合。你要做威胁情报，也少不了与产品厂商、数据属主以及权威机构的协作。随着像互联网安全联盟、网络防欺诈联盟、大数据联盟、云计算联盟、车联网安全联盟、威胁情报联盟等协作组织和机制的涌现，原先四分五裂诸侯割据的产业格局，大有被澄清、捋顺和接续的可能。

也许还有其他变化，但仅只上述几点，已经够创业新锐们群情振奋跃跃欲试了。

“再不创业，都对不起这个时代了。”是的，高瀚昭、赵武和薛锋，在这些创业新锐们的眼里，毫无疑问，这是一个最好的时代。

而在走访这些新锐的过程中，毫无疑问，我也强烈地感受到了他们的与众不同。

前面说了，新鲜加锐利，是为新锐，但支撑这种新鲜和锐利的，对创业者来说，该是怎样的品质和内涵呢？

首先是积淀。如果没有积淀，再大的热情也容易倏忽湮灭。像高瀚昭，在趋势科技十多年，先后做程序员、研发总监、高管，又有合资公司里 CEO 的历练。赵武，在华为和 360 这两家截然不同却各具代表性的公司里做过研究员、产品经理和主管。而薛锋，体制内体制外都有经历，微软和亚马逊又给他一个旁人甚难企及的高地。在他们身上，岁月给予的不只是年龄，更是在能力、经验、阅历和人脉上的丰厚积淀。

其次是自信。正因为有着足够的积淀，这些创业新锐才表现出无与伦比的自信。高瀚昭说要颠覆传统细分领域，赵武说舍弃 360 只为成就真正属于自己的事业，薛锋说根本无惧 BAT，在他们脸上和话里，根本感觉不到犹豫、怀疑和担心，有的只是舍我其谁的坚定信念。

他们知道自己要什么，知道该找哪些伙伴，也知道该往哪去，这一点非常难能可贵。

再有是乐观。尽管整个大环境处于变革与冲突交加的新旧之际，有希望，也有巨大的不确定性，但对高瀚昭、赵武和薛峰们来说，似乎没有什么理由不让他们笑脸相对，也没有什么值得惧怕与担心。更重要的是，这种乐观并非盲目，与他们畅谈，总能听到鞭辟入里、洞察如悉的观点，他们太懂这个行业了，太知道过去的不足和弊端了，也正因为此，他们才在这一伟大的转折期里看到了机会，并且乐观以待、义无反顾地去主动抓取这个机会。

最后是激情。如果要问，创业者最应该彰显的是什么？从我走访的新锐们身上，最深切的感触就是激情，或者再通俗点讲，是情怀。有积淀就有自信，有自信才乐观，而有了乐观，做事情就充满激情，就会给予所做事情更多的意义，这意义最直观的体现就是情怀。他们其实不缺钱，甚至可以说积蓄颇丰，他们创业不纯粹为钱，他们珍惜的是能够“开天辟地”的机遇，喜爱的是志同道合并肩作战的气氛，而追求的，则是创造价值的成就感。

积淀，自信，乐观，激情，是这一波网络安全创业者共同的特征。

从业与创业，看似简单，却有着与这时代所蕴涵同样的巨大变因。之前，他们是技术专家或企业高管，之后，他们成为自我实现的创造者。时代不同了，他们也“判若两人”，某种意义上，时代选择了他们，他们进一步推动着时代的变化。

也许因为我也是个创业者吧，虽然不再新锐，但在与他们的交流中，我觉得亲切而自然，时而感同身受，时而惺惺相惜。

套用这句话，“不创业都对不起这个时代呀。”我想说，“不去近距离感受创业，也对不起这个时代呀。”

所幸安在给了我这样的契机。

在接下来的一段时间里，我想，创业新锐们一定会在传统厂商和互联网大佬之外开拓出第三极的力量，这是真正可以媲美两端的第三极，是能够左右联络、上下腾挪且创新多变的第三极，他们从无到有，从星星点点到逐渐燎原，并且进一步激发一波又一波创新创业的连锁反应，甚至会重新定义网络安全产业的生态链。

那么，我能做些什么？安在能做些什么？

很简单，寻找他们，发现他们，报道他们，观察他们，服务他们。

在以影响力人物这条线索展现中国网络安全二十年风云全貌的同时，我们会沿着创业新锐这条线索洞察中国网络安全的未来十年。

也许安在还很微小，只不过是个自媒体，但我们也有了一颗新锐之心，我们也在创新突破，



不仅仅是媒体，更以平台的理念去探索和发展。创业者关注什么？需要什么？关注和需要创业者的其他群体以及整个产业界，又在关注和需要什么？而所有这些，都是我们关注和需要的，也正因为此，我们才使命油生，该去做些什么了。

至少我们要接触、了解和理解，要提供力所能及的支持，要对接更多价值。

这么一说就很简单了，现在，我殷切呼吁，如果你是新锐，如果你认识新锐，如果你知道有关新锐的林林总总，都请联络安在，联络我，我与你一样有着好奇之心和交友之意，让我们一起，与新锐共进网络安全的未来之旅。

网络安全不再陈旧不再落寞。

网络安全正风云突变新锐群起。

耀疆在关注，安在有行动。

无论你在哪里，我都会找到你。

**张耀疆**

安在新媒体创始人，安言咨询总经理

## 前言

2015 年 12 月 16 日，习近平主席在第二次世界互联网大会发表主旨演讲，对世界互联网的发展提出了五点主张，其中提到，没有网络安全，就没有国家安全，没有信息化，就没有现代化，并强调通过保障网络安全来促进有序发展。

以往我们对网络空间安全的关注，除了产业现状，还有就是专业人才，而随着互联网+以及政府主推的双创战略风起云涌，在网络空间安全这个细分领域，其创业热度和步调，也显现出与以往完全不同的面貌。安在作为一家立足信息安全、富有内涵和深度的新媒体平台，理所当然会把眼光聚焦于这波创新创业的大潮。通过两个多月的准备和努力，我们推出这份年度网络空间安全创业调查报告，试图从创业者群体、创业项目、创投环境等三个方面，勾勒出当前此领域的创业图景。我们尽量做到以严谨客观的数据和全面深入的分析，为政府部门、企业、投资等各界提供参考及决策依据。

未来，安在会以此次报告为起点，以更短的周期，高频度、持续性地跟踪相关创业项目。

鉴于时间仓促，安在首次呈现的这份报告难免存在各种不足和疏漏，还请各位多多批评和指正，您的任何一种反馈，都将是我們继续前进的动力。

**安在**

2016 年 2 月



**最有内涵的  
信息安全新媒体**

微信公号：AnZer\_sh

人物热点互动传播

## 致谢

本报告的数据采集工作得到了政府相关单位、企业以及社会各界的大力支持，各项调查工作得以顺利进行，在各相关单位、调查支持网站以及媒体等的密切配合下，基础资源数据采集才能及时完成。在此，谨对他们表示最衷心的感谢！

此外，本报告中部分文字和数据，有引述自互联网相关资讯的，这里对资讯源一并致谢，并恕未能一一列举。



上海安致信息技术有限公司



北京瀚思安信科技有限公司



上海斗象信息科技有限公司



瑞数信息技术(上海)有限公司



东巽科技（北京）有限公司



北京天际友盟信息技术有限公司



上海有云信息技术有限公司

西安四叶草信息技术有限公司



厦门服云信息科技有限公司



北京锦龙信安科技有限公司



北京微步在线科技有限公司



上海岂安信息科技有限公司



远江盛邦（北京）信息技术有限公司



北京白帽汇科技有限公司



乌云漏洞报告平台



盘古团队



北京娜迦信息科技发展有限公司



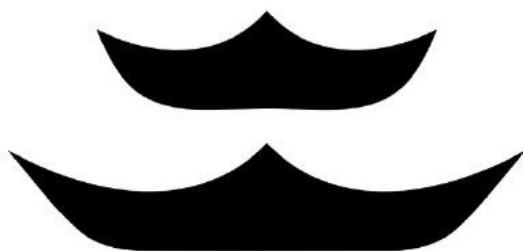
零日信息技术有限公司



北京洋浦伟业科技发展有限公司



杭州同盾科技有限公司



北京长亭科技有限公司



广州凌晨网络科技有限公司



奇虎 360 科技有限公司



苹果天使基金



上海优刻得信息科技有限公司



深圳百密信安科技有限公司

# 一、 报告简介

## 1. 报告目标

自“棱镜门”事件以来，网络安全日益受到社会各界的重视，而同时随着我国“互联网+”战略带来了产业链和生态链的互联互通，网络安全日益凸显其重要性。由此引发了网络安全创新创业的热潮。

目前，我国网络安全创业团队及项目已近百个，正形成一股新兴势力。基于此，我们针对网络安全创业团队及项目，采用了人员访谈和问卷相结合的模式，通过近两个多月的数据收集与分析，最终形成本报告，旨在客观的评判我国目前网络安全创业的基本情况，从而为行业创新发展提供决策参考。

## 2. 报告范围

本报告调查范围是网络安全初早期创业团队及项目。对项目情况及团队情况开展调查。

调查时间：从 2015 年 12 月 1 日至 2016 年 1 月 31 日；

样本分布：调查的样本目标是网络安全创业项目 CEO、创业团队核心成员及相关投资人，调查最终获得有效样本量 213 个。

## 3. 报告方法

本次调查采用人员访谈和在线问卷相结合的样本模式。通过对调查对象发布在线调研问卷，结合电话或现场访谈，获得报告样本。并通过数据分析，得出报告结论。

数据统计的方法统一采用加权平均算法，所有数据保留小数点后两位。

## 4. 结果简述

目前网络安全创业项目以北京最为聚集，有 42% 的项目选择落地在北京；92% 的项目处于 B 轮以前的初早期阶段；项目类型以云安全、威胁情报、安全众测、APT 防御等领域最为热门；其中，云安全类项目的融资能力最强，平均能达到 5000 万元左右；项目呈现较明显的技术特点，85% 的创业项目拥有自主知识产权。

风水：42% 落地北京

规模：30-50人

阶段：92% B轮以前



技术：85% 有知识产权

方向：25% 云安全

融资：均5000w

网络安全创业者以男性居多，占 97%；年龄主要分布在 31 至 35 岁之间；49%毕业于普通高等院校；网络安全创业者有浓郁的技术背景，67.86%的人曾经任职在传统网络安全公司；53.57%曾经从事过网络安全技术相关岗位。



性别：97% 男

年龄：31-35

学历：49%杂牌本科

履历：67.86% 安全厂商

背景：53.57% 安全技术

网络安全风险投资目前还处于启蒙阶段，71%的投资机构对行业情况上不熟悉，在 87% 的投资人看来，网络安全投资的风口尚未形成，但同时对于 2016 年网络安全领域持续看好，会追加相应的投资。

投资人  
画像



行业：TMT

了解：71% 不熟悉

观点：87% 风口未成

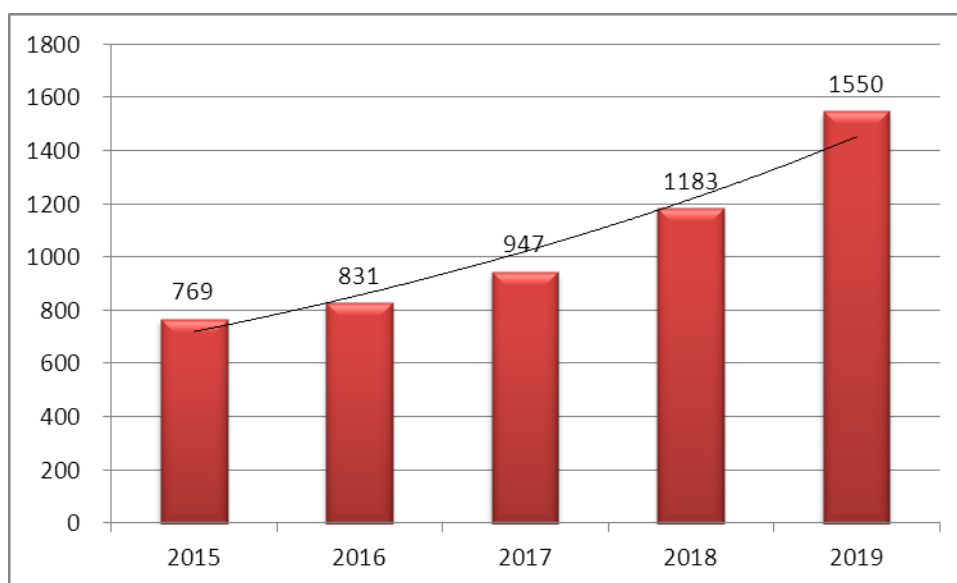
关注：42% 威胁情报、反欺诈领域

未来：100% 持续看好

## 二、 产业概述

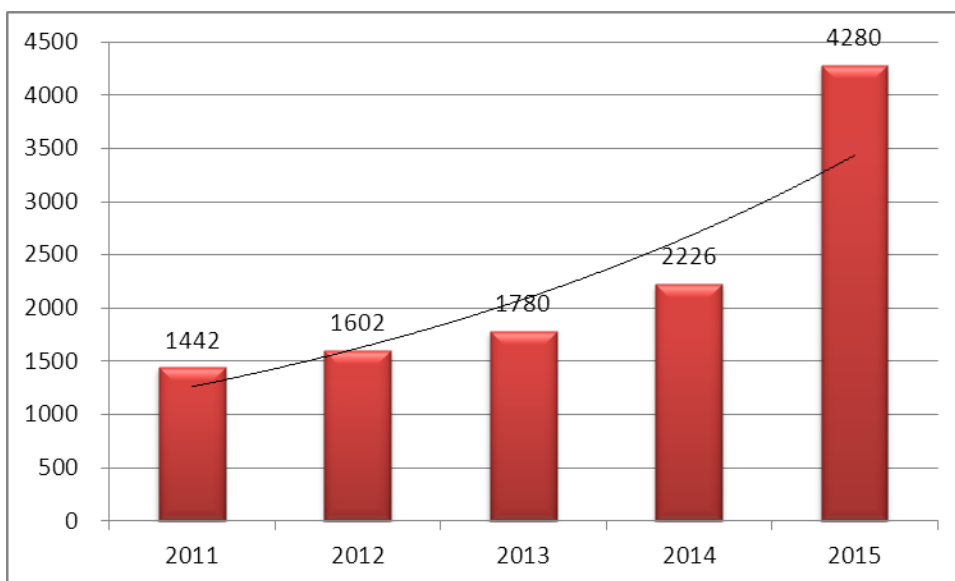
### 1. 全球网络安全产业规模

全球网络安全市场 2015 年的市场规模为 769 亿美元 ,预测到 2019 年将超过 1550 亿美元。复合年增长率(CAGR)从 2014 年至 2019 年将增长 10.3%。航空、国防及情报垂直行业将成为网络安全解决方案的最热门提供商。北美洲将成为最大市场，亚太地区及欧洲、中东和非洲地区在市场新引力方面有望增长。



全球网络犯罪不断上涨，每年为世界经济造成数千亿美元的损失。2015 年，全球所有行业检测到的网络攻击共有 4280 万次，比去年增长了 48%。每年计算机及网络犯罪活动为世界经济带来的损失超过 4450 亿美元。网络犯罪除了为世界经济造成数以亿计的损失，同时也为供应商及服务提供商创造了数以亿计的收益机会外，网络犯罪也为寻找投资资金的企业带来了负面影响。近 80% 的投资者因曾被入侵或效率低下的网络安全策略而遭拖延。



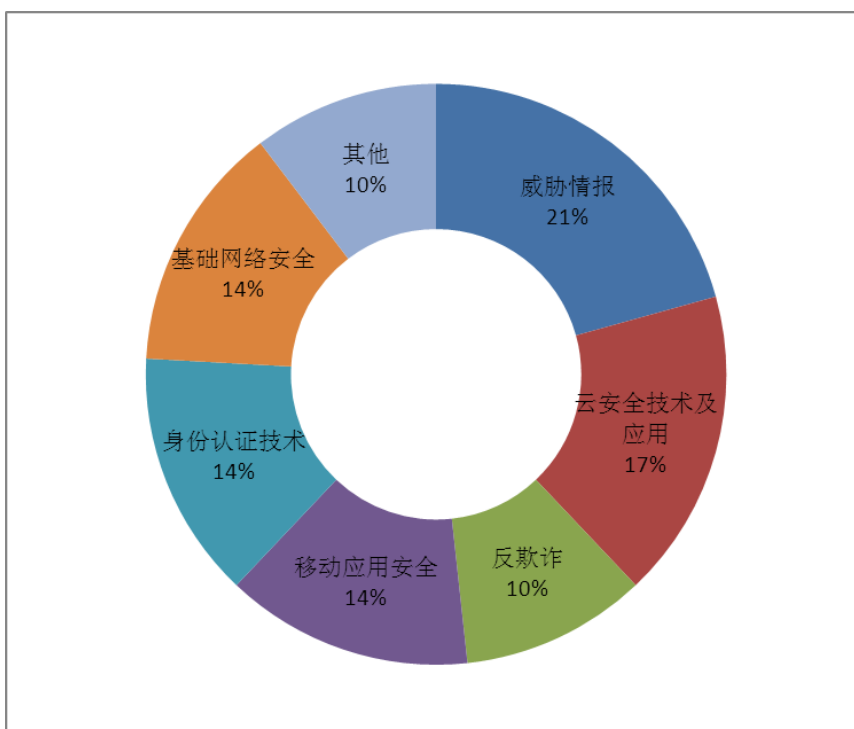


到 2020 年，亚太地区在关键基础设施上的安全支出将达到 220 亿美元。网络间谍及网络战争中的活跃活动影响了亚太地区的民族国家级私营企业机构。数字化的先进行业及新兴知识经济是网络威胁分子有利可图的目标，或与政治理想有关或为了经济利益。

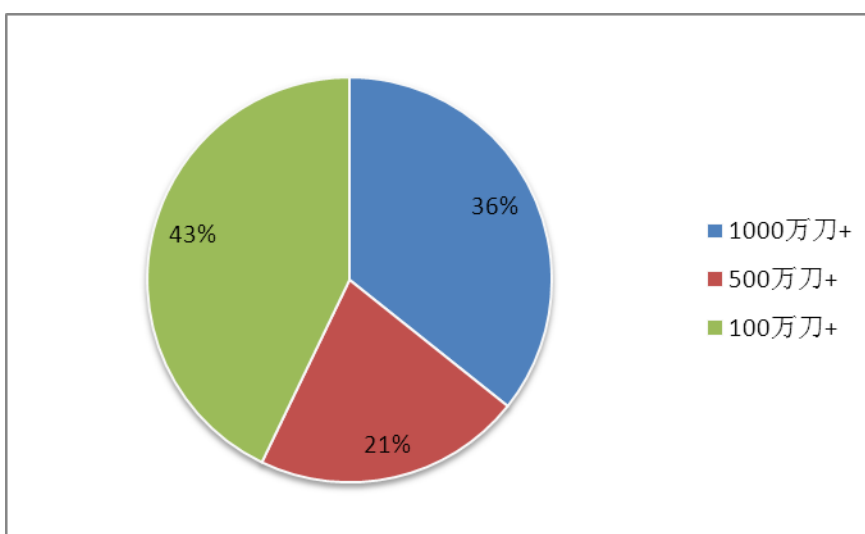
## 2. 全球网络安全创业投资

2015 年全球网络安全风险投资首次突破 20 亿美元大关。在未来两年内，从云端、IT 及客户安全市场到物联网安全的网络安全风投活动能够快速扩张。

综合全球数据看来，2015 年网络安全的初早期创业项目呈现多方向发展的态势，主要方向包括威胁情报、云安全技术及应用、基础网络安全、身份认证技术、移动应用安全、反欺诈等方面。其中，威胁情报是最热门的创业方向。



在融资成功的初早期项目中，有 36% 的项目融资额超过 1000 万美元。



全球网络安全创业与投资正进入高速发展期。

### 3. 中国网络安全产业基本布局

在中国，网络安全产业是为数不多的国内厂商主导占优的新兴产业，国内厂商目前的市场份额大约为 60% 左右，这将使国内网络安全厂商充分享受行业成长带来的机遇。同时，随着以“棱镜门事件”为代表的一系列安全事件的持续发酵，中国政府、企事业单位和网民对网络安全的重视度也在不断提升。

中国的网络安全产业发轫于 21 世纪之初，经过近 10 年的发展，目前行业已经初具规模，产品线日益丰富，已形成三大类、约二十小类、近百种产品的行业格局，细分程度非常高，并广泛的服务于政府、企事业单位和普通网民。

目前，国内的网络安全产业仍然以销售硬件和软件产品为主，服务所占的比例较小。其中，在硬件产品中，防火墙/VPN 硬件产品占据了最大的市场份额；而在软件产品中，安全内容和威胁管理软件是最主要的产品种类。

从下游客户来看，目前，政府、金融、电信、能源等行业是网络安全产品和服务的主要消费者。政府和大型企事业单位由于其信息系统的数据具有较高价值，其信息系统是黑客的重点攻击对象，一旦其信息系统被攻陷，将遭受较为重大的损失，因此政府和大型企事业单位更为重视网络安全建设。另外，资金实力和政策要求也是政府和大型企事业单位成为网络安全产业下游主要客户的重要原因。而相对而言，一些中小企业和普通网民由于遭受攻击后损失较小，因此对网络安全建设重视程度相对较低，同时资金相对有限也使得其采购相关的网络安全产品和服务的积极性有所降低。

但是，目前这一现状正在发生变化。随着智能设备的不断普及和信息设备国产化的不断推进，网络安全行业将向中小企业和普通网民下沉，同时更多适合小微客户的网络安全产品有待进一步挖掘，一个巨大的 B2C 蓝海市场若隐若现。

网络安全行业由于细分子行业很多，服务的客户也来自各行各业，行业内的厂商数量众多，不同的细分市场都有相应的专业厂商，很难实现一个企业掌握网络安全领域的所有技术。整个行业缺乏具有绝对领导实力的大型网络安全企业。

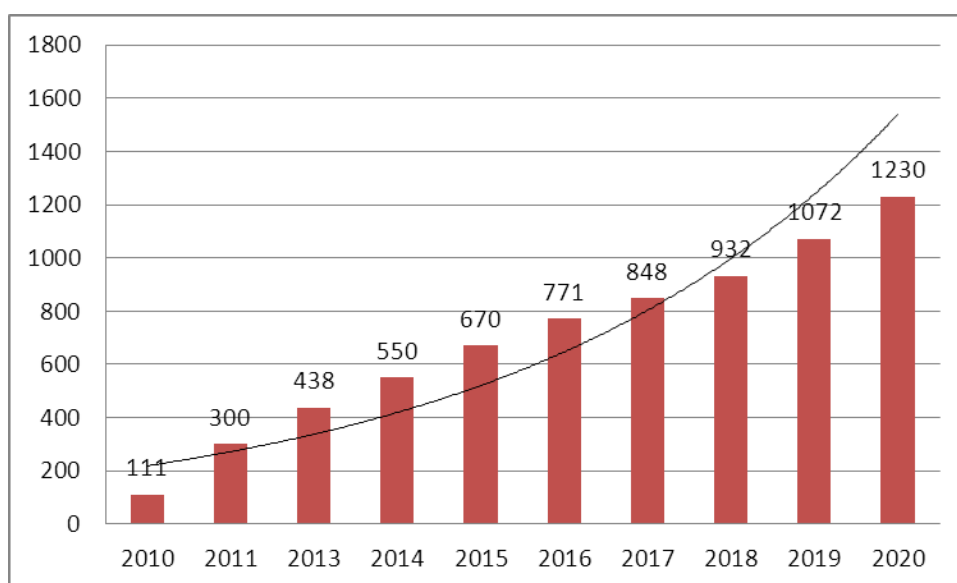
而从国内网络安全市场来看，和国外并无太大区别，山头林立的现象普遍存在，最大规模的安全企业销售收入也不足十亿元，每个细分行业市场份额居前的生产厂商均不尽相同。在细分行业内，各企业产品的同质性较强，竞争较为激烈，产品的品牌优势不是很明显。

未来，随着行业的不断整合，细分行业的破壁将成为大势所趋。领先企业有望凭借资金优势、平台优势和技术优势不断提升市场占有率，为下游客户提供一站式的网络安全解决方案和服务，分享更大的蛋糕，并具备走向国门的能力。这种趋势不仅对于我国网络安全行业的健康发展和技术进步具有重要意义，并且符合国家利益取向，有望得到更多的政策支持。

## 4. 中国网络安全产业发展规模

目前，我国经济正处于增长速度换挡期、结构调整阵痛期和前期刺激政策消化期的“三期叠加”特殊时期，在这一宏观经济大背景下代表经济发展新方向的新兴产业将成为经济增长的主要动力。网络安全产业不仅是新兴产业的重要组成部分，同时与国家安全关系密切，受到国家政策的大力扶持，是新经济中的一朵金花。中国网络安全产业产值与整个信息服务业产值的比例为 1%左右，而欧美发达国家这一比例普遍在 10%左右。未来，随着物联网、

大数据、云计算等技术的逐渐普及，我国的网络安全产业的产值比例逐渐接近欧美等发达国家的水平。即使考虑最悲观的情况，到 2020 年，网络安全市场空间也将达到约为 1230 亿元，是目前市场空间的 10 倍。



在国家安全方面，全球进入信息战的时代，网络战将成为重要作战形式之一，“网络安全”成为关键制胜手段。在未来的信息化战争中，战场主动权从制陆、海、空、天权转移到制信息权。不同于传统战争形式，信息化战争的表现形式包括心理战、情报战、潜力抗衡、电子战、用于摧毁信息设施的火力战、计算机病毒战、精确战、隐形战、黑客战、网络战、信息技术战等等，其中网络战将成为未来战争的主要作战样式之一。电脑网络空间与基础安全设施联系越来越紧密，在这个空间中，没有物理边界，军事信息基础设施完全暴露在威胁下，网上攻防已成为维护国家安全的重要屏障。未来，随着物联网、大数据、云计算等技术的逐渐普及，会有更多的下游行业和客户提高对网络安全建设投资的比重，使得我国的网络安全产业的产值比例逐渐接近欧美等发达国家的水平。

## 5. 中国网络安全产业政策环境

2013 年“棱镜门”事件后，中国政府将网络安全列为重中之重，成立中央网络安全与信息化领导小组，习近平担任组长，充分体现中国最高层在保障网络安全、维护国家利益、推动信息化发展方面的顶层设计和决心。

这给国内网络安全厂商的发展带来了历史性的发展机遇：一方面，网络安全行业将逐渐从以前政府和企事业单位 IT 消费中的可选品演变为必需品，市场空间被打开做实；另一方面，国外的网络安全产品将面临国内客户的信任危机，国内厂商的网络安全产品和服务将有机会不断的对国外的网络安全产品和服务进行替代，使得国内网络安全行业的市场份额将进一步提升。

# 国家网络安全相关政策一览：

时间	国家网络安全相关政策
2014 年 2 月	中央网络安全和信息化领导小组第一次会议召开，习主席参加并发表重要讲话。他强调，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。截至 11 月,北京等 17 个省成立了省级网络安全和信息化领导小组,2015 年省级网信办机构将建设完毕并开始落实国家网络安全政策。
2014 年 5 月	中央国家机关政府采购中心发布中央机关采购计算机禁止安装 win8 系统。
2014 年 8 月	工信部下发了《加强电信和互联网行业网络安全工作的指导意见》提出八大工作重点。对网络基础设施和业务系统安全防护、推进安全可控关键软硬件应用、网络数据和用户个人信息保护等做出强调。
2014 年 8 月	出于安全考虑 ,政府采购部门将赛门铁克与卡巴斯基从安全软件供应商名单中排除 ,将赛门铁克 “数据防泄漏” (Symantec DLP)软件列为禁用产品。
2014 年 9 月	银监会印发《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》 ,提出到 2019 年 ,安全可控信息技术在银行业总体达到 75%左右的使用率。
2014 年 10 月	中央军委印发《关于进一步加强军队网络安全工作的意见》。《意见》指出，要深刻认识加强网络安全工作是适应信息时代发展的必然要求，是实现能打仗打胜仗核心要求的紧迫任务，必须把网络安全工作作为军事斗争准备的保底工程，采取超常、

	务实举措解决突出矛盾和重难点问题，促进我军信息化建设科学发展、安全发展。
2015 年 6 月	十二届全国人大常委会第十五次会议 24 日审议了《网络安全法(草案)》，并于 7 月初向社会公开征求意见。《草案》的重要内容主要包括，确定了网络安全工作基本原则、将个人信息保护纳入正轨和网络产品和服务的安全保障，还规定了重大突发事件时政府可采取临时措施限制网络。可以预计，当《草案》成为正式法规发布后，其他相关的安全规定、条例也会相继出台。
2015 年 6 月	《中国互联网协会漏洞信息披露和处置自律公约》在京签署，公约提出漏洞信息披露的“客观、适时、适度”三原则;
2015 年 6 月	国务院办公厅发布《关于运用大数据加强对市场主体服务和监管的若干意见》。加大网络和网络安全技术研发和资金投入，建立健全网络安全保障体系。采取必要的管理和技术手段，切实保护国网络安全以及公民、法人和其他组织网络安全;
2015 年 6 月	新的国家安全法实施。新法要求建设网络与网络安全保障体系，提升网络与网络安全保护能力，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控;
2015 年 8 月	人大正式通过中华人民共和国刑法修正案(九)。明确了网络服务提供者履行信息网络安全管理的义务，加大了对信息网络犯罪的刑罚力度，进一步加强对公民个人信息的保护，对增加编造和传播虚假信息犯罪设立了明确条文;
2015 年 9 月	国务院印发《促进大数据发展行动纲要》，在网络和大数据安全方面要求，在涉及国家安全的领域采用安全可靠的产品和服务，到 2020 年，实现关键部门的关键设备安全可靠;

2015 年11 月	工商总局印发《关于加强网络市场监管的意见》，全面加强网络市场监管。推进“依法管网”、“以网管网”、“信用管网”和“协同管网”。
------------------	-----------------------------------------------------------------

通过政府的政策倾向不难看出网络安全已经成为事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，未来几年网络安全行业将继续维持较高的景气度快速发展。

## 6. 中国网络安全产业发展预期

参照欧美发达经济体网络安全产业产值在整个信息产业产值中占比 10%的行业现状，同时考虑到网络安全在万物互联时代更加重要的现实，保守估计到 2020 年，中国在万物互联领域的网络安全投资占比为 12%，则到 2020 年，网络安全行业在万物互联这一领域的增量市场将达 6000 亿元，是目前网络安全行业总产值的 50 倍。

如果再考虑到网络安全行业在传统领域占比的提升，则到 2020 年，网络安全行业的市场空间至少是目前的 60 倍，7 年年均复合增速为 80%。即使考虑最悲观的情况，到 2020 年，网络安全在整个行业的占比仅为 2%，则其市场空间约为 1230 亿元，是目前市场空间的 10 倍，7 年年均复合增速约为 40%。可见，中国的网络安全产业的增长速度将远远超过目前市场的预期，未来 7 年年均复合增速区间至少在 40%-80%。

### 三、 数据分析

本次调研涉及网络安全领域创业机构 41 家，较全面的展现了目前我国网络安全创业创新的整体面貌和状态。

#### 1. 创业项目

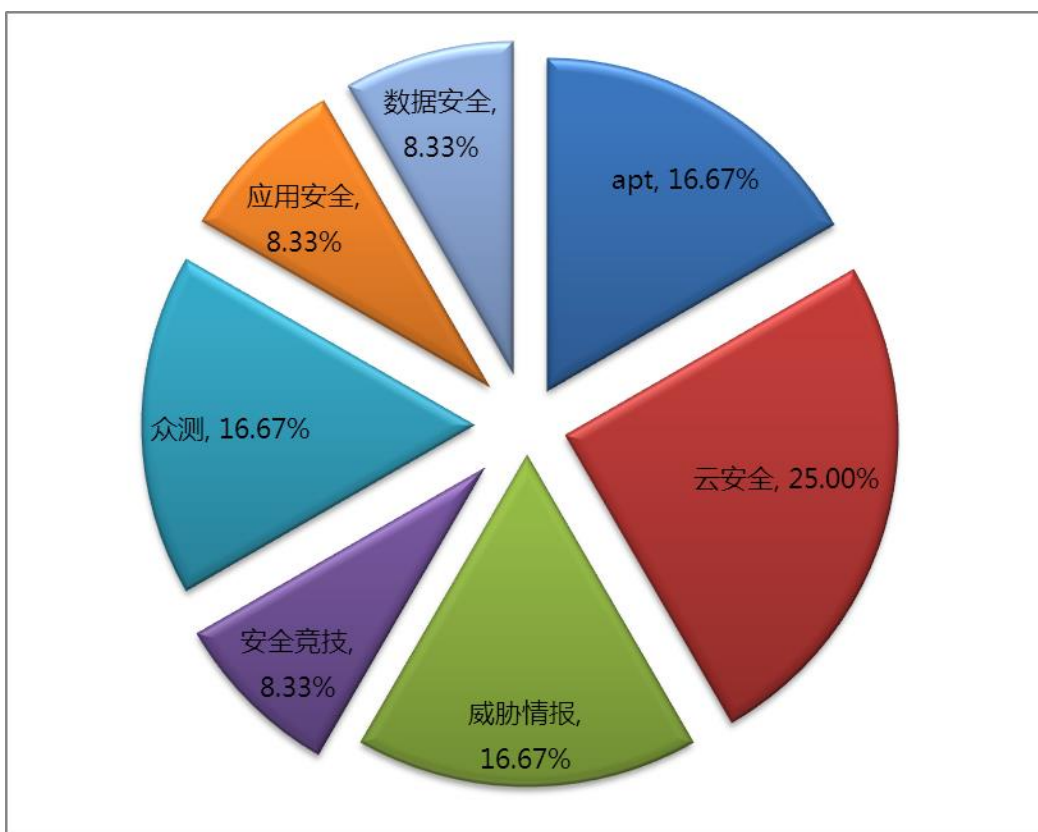
##### 1) 青睐的创业方向？

分析发现，目前国内创业项目青睐的领域主要涉及 APT 防护、云安全、威胁情报、安全学习和竞技、安全众测、应用安全、数据安全等方面。

- APT 防护是指为防护新型高可持续性攻击所研发的技术、产品、工具、服务等方面的项目；
- 云安全是指面向云计算及云服务的安全技术、产品、工具、服务等方面的项目；
- 威胁情报是指基于证据的知识，包括上下文、机制、指标、隐含和可操作的建议，针对一个现存的或新兴的威胁，进行识别和预警的相关技术、产品、服务等方面的项目；
- 安全学习和竞技是指支撑网络安全教学及竞技的技术、产品、服务等方面的项目；
- 安全众测是指通过互联网技术实现的在线众筹式渗透测试相关的技术、产品、服务等方面的项目；
- 应用安全是指针对网络及系统应用层保护的相关技术、产品及服务等方面的项目；
- 数据安全是指针对商业数据及个人隐私数据保护的相关技术、产品及服务等方面的项目。

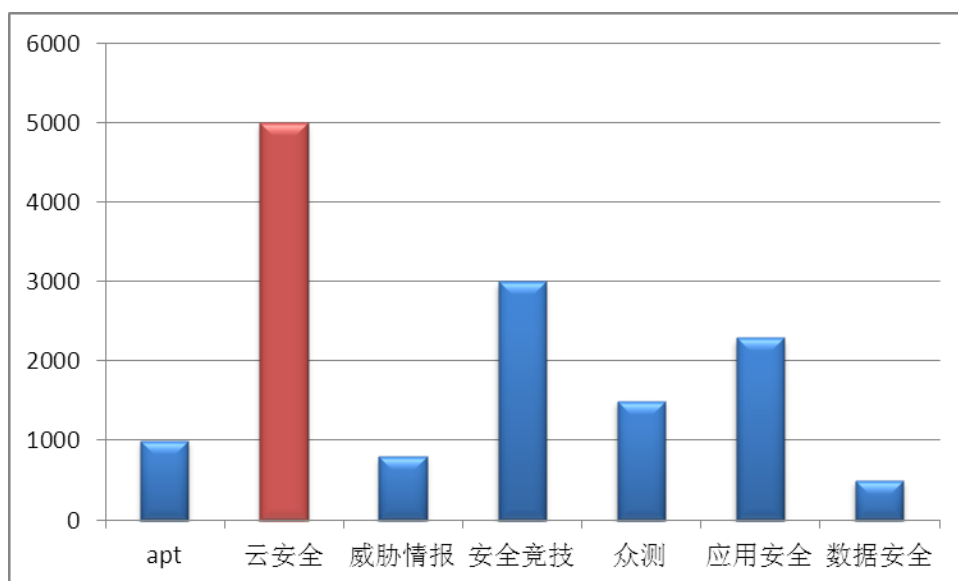
而其中云安全、威胁情报、安全众测、APT 防御领域是创业团队最为追捧的热点。





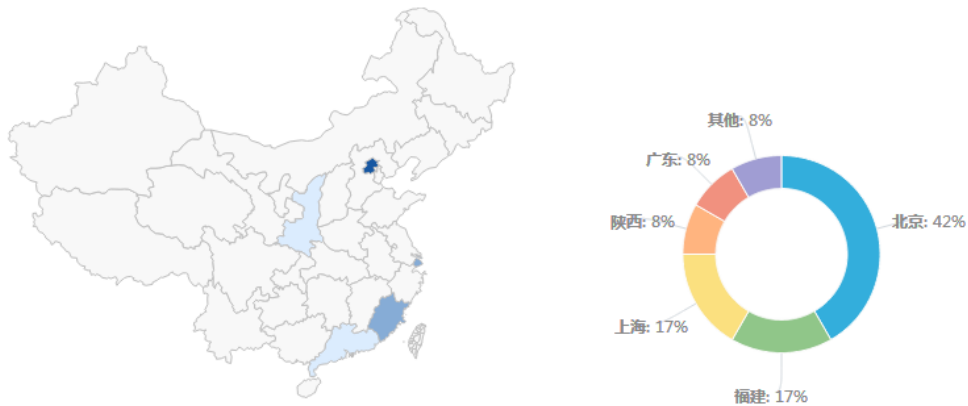
## 2) 这些类型的项目能拿到多少钱？

在所有调研的项目中，云安全相关项目获得融资的金额最高，平均达到 5000 万元。



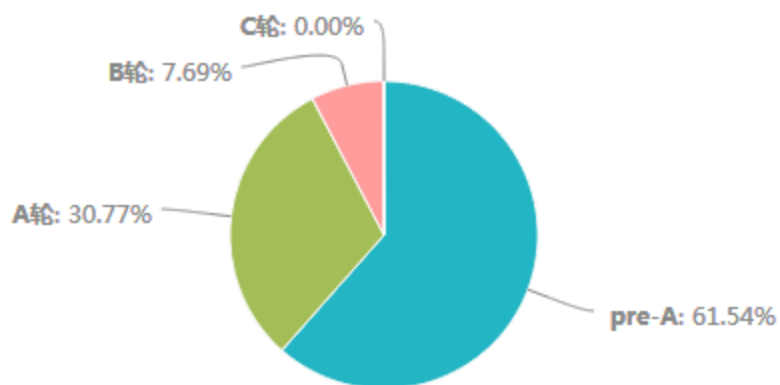
### 3) 网络安全创业的风水选择？

调查发现，北京是网络安全创业的风水宝地，有近 42%的企业选择在北京创业。



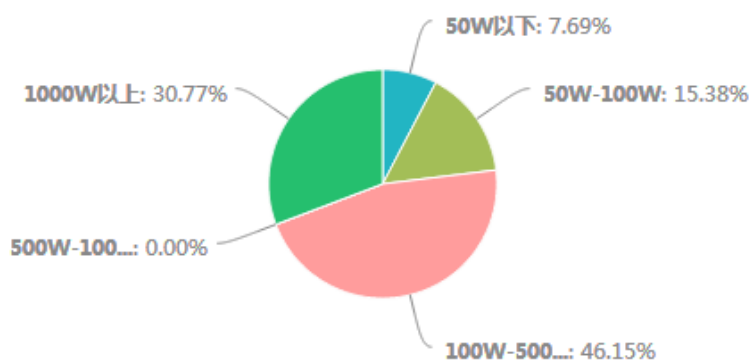
### 4) 目前项目所处阶段？

在所调研项目中，Pre A 轮的占比较大，说明网络安全创业项目目前整体尚处于早期阶段，发展潜力较强。



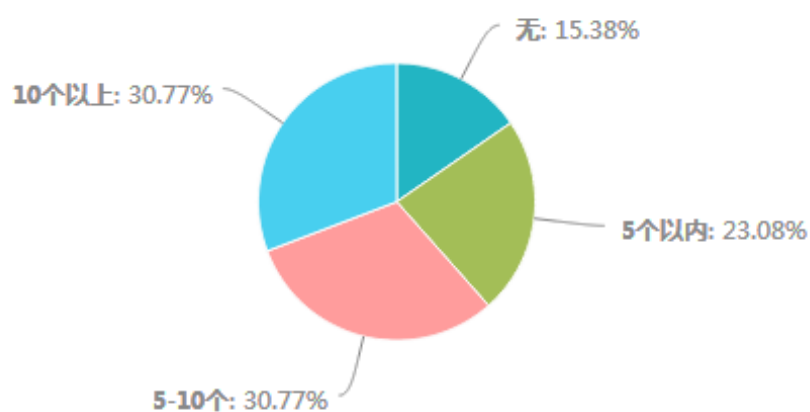
### 5) 销售收入

调研显示，有 46%的项目销售额超过 100 万元，就初创项目来说，网络安全类创业项目的早期盈利能力较强。



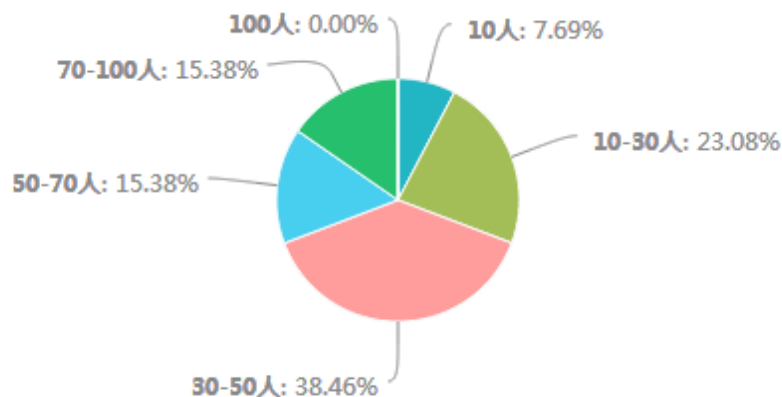
## 6) 知识产权数量

有近 85% 的网络安全创业项目拥有自主的知识产权，说明核心技术是网络安全类初创项目形成的基础。



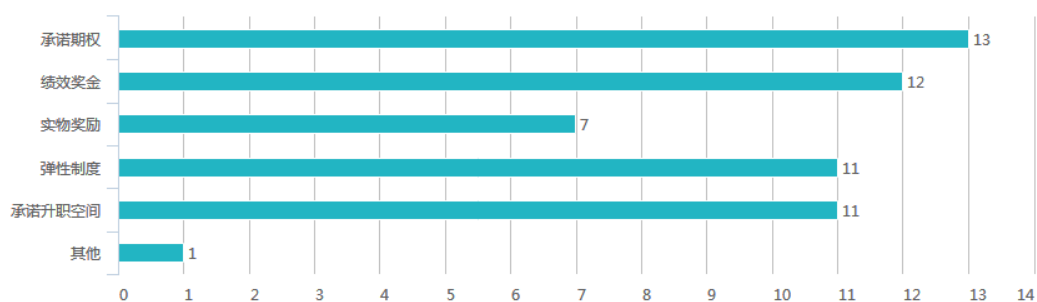
## 7) 人员规模

根据调研显示，网络安全创业初创团队的构建规模以 30-50 人为宜。



## 8) 如何设定激励机制

调研显示，承诺期权、绩效奖金、弹性制度、承诺升职空间，是网络安全初创团队主要采用的招揽人才的手段。

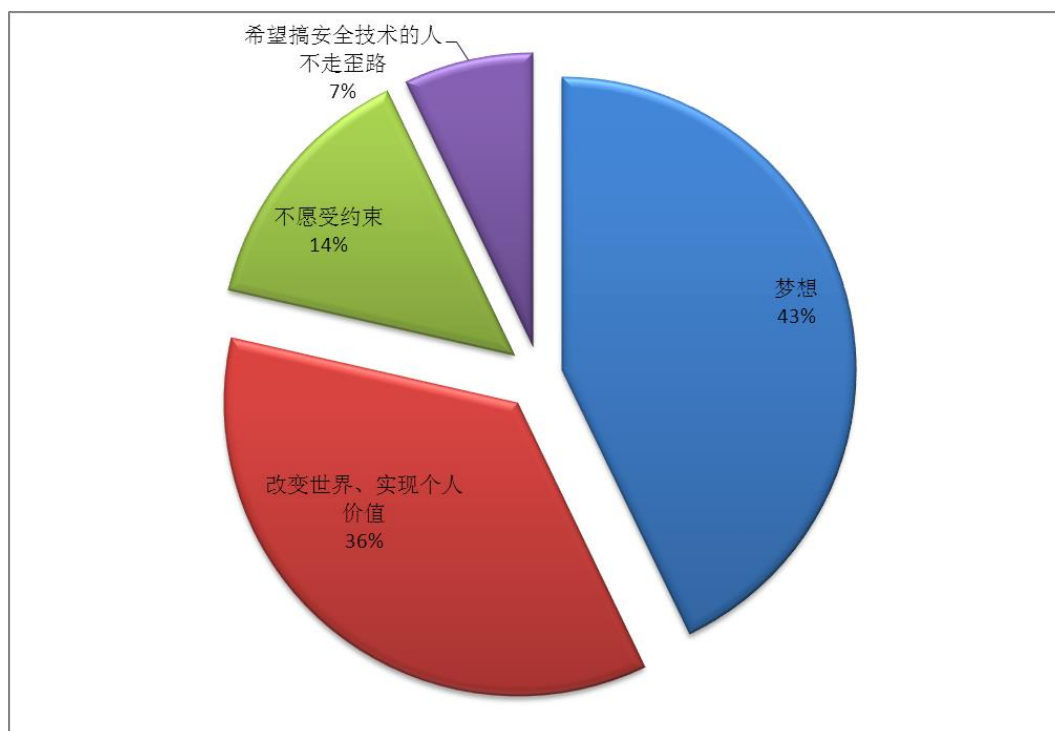


## 2. 创业人才

本次对创业人才的调研涉及创业机构创始人及核心团队成员 198 名，较全面的展现了目前我国网络安全创业者的整体状态。

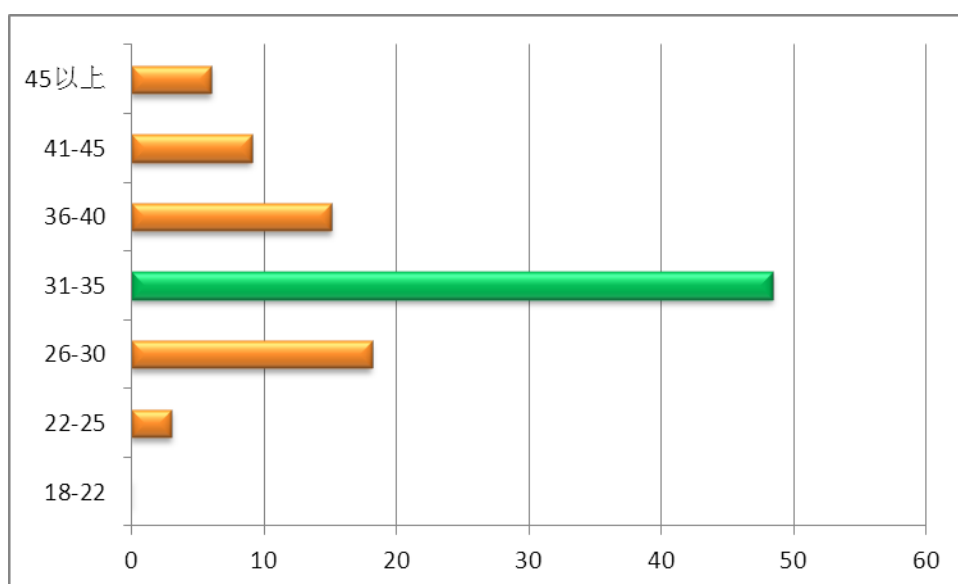
### 1) 为什么会选择创业？

创业是一种高层次的价值追求，近 80%的人创业的原因是梦想及改变世界、实现自我价值的愿望。他们把创业当成是实现自我价值的一个途径。



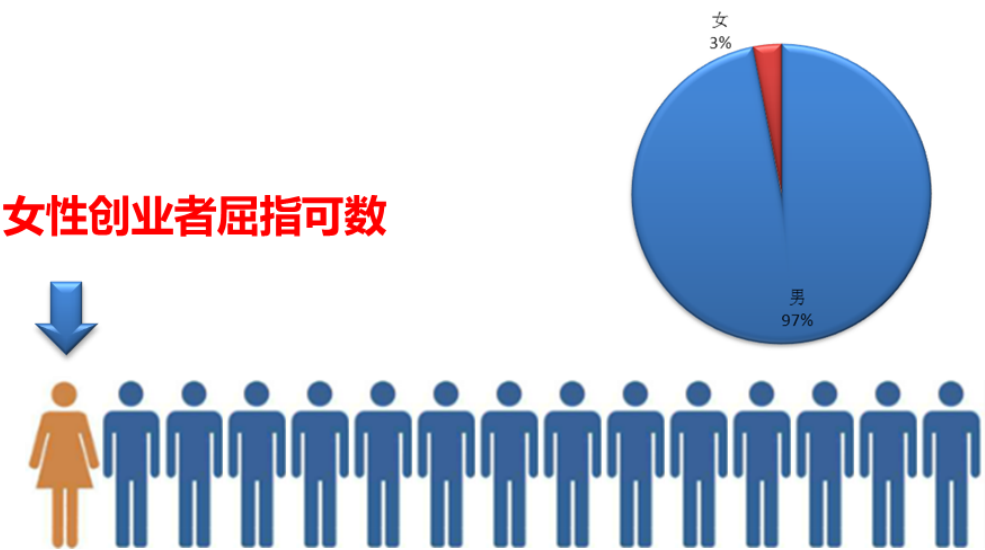
## 2) 创业者年龄分布

调查显示，31-35 岁是网络安全创业的黄金年龄。



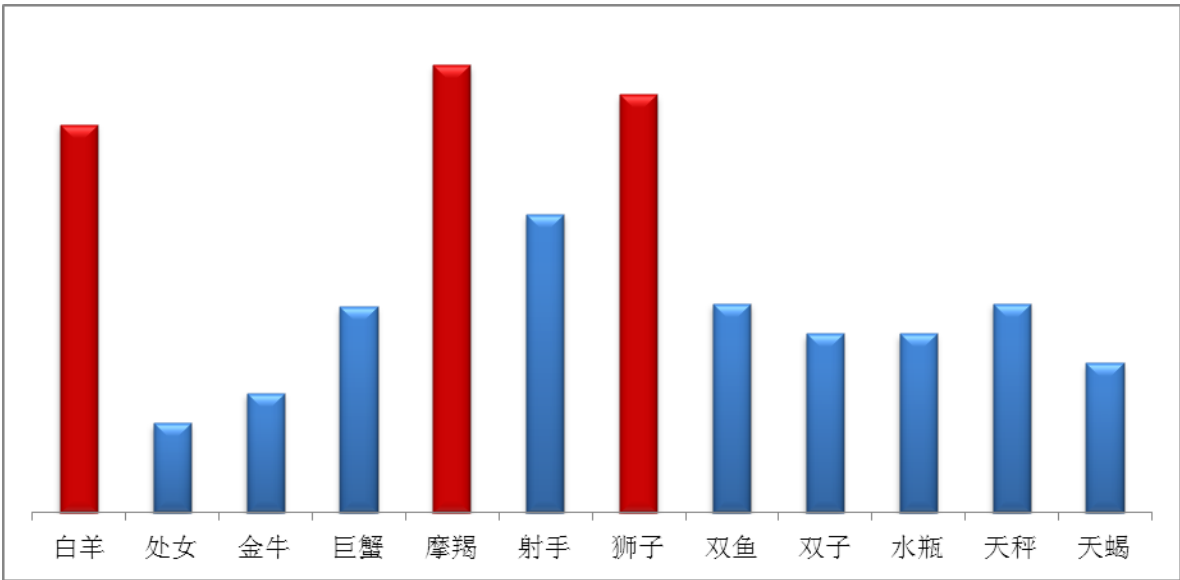
3) 创业者男女比例

调查显示，网络安全创业男女失衡情况严重。



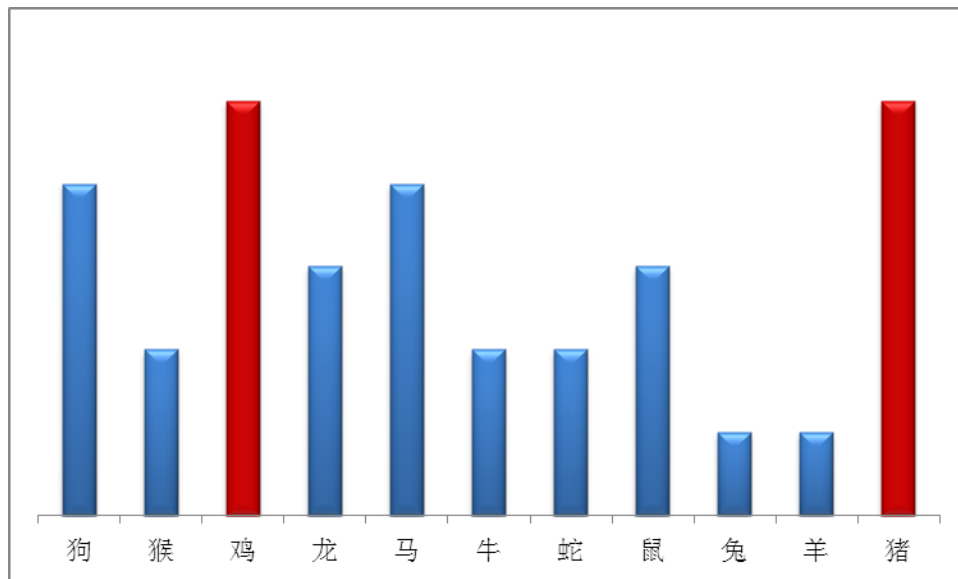
4) 什么星座最适合网络安全创业？

调查显示，白羊座、摩羯座、狮子座更适合网络安全创业。



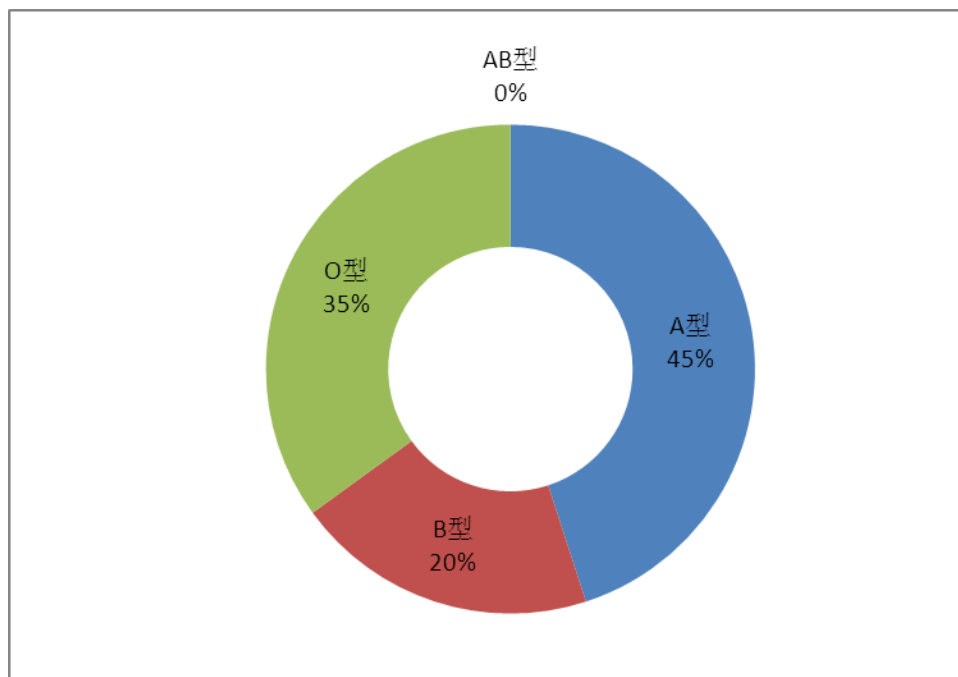
5) 什么生肖最适合网络安全创业？

调查显示，属鸡、猪的人在网络安全创业者中占比较高。



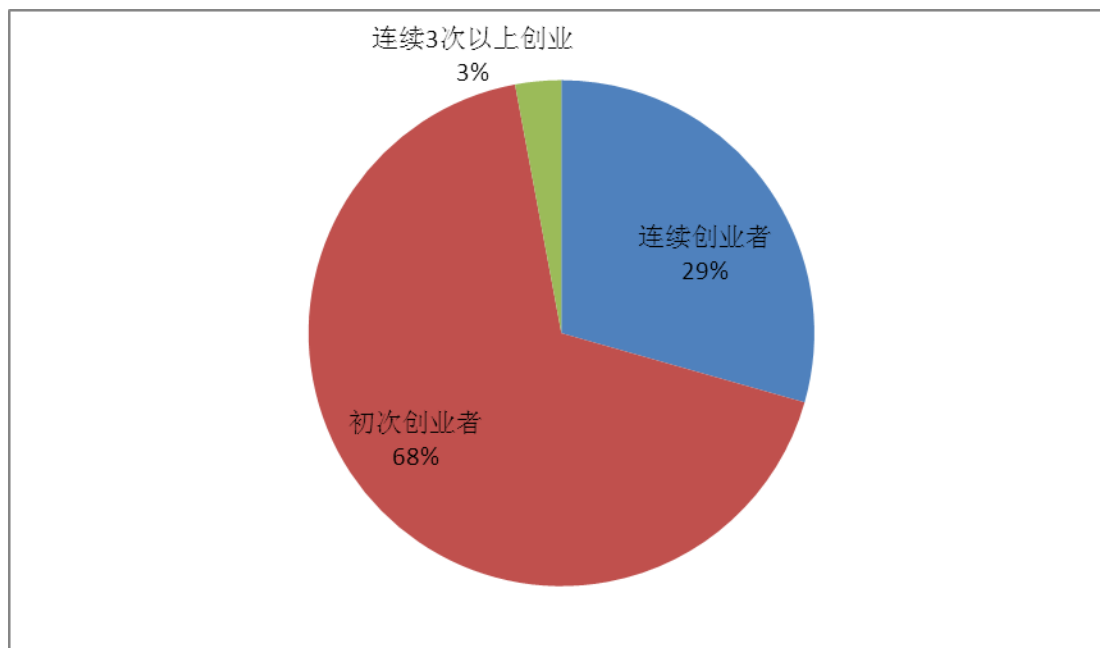
## 6) 什么血型最适合创业？

调查显示 AB 型血的不适合网络安全创业！



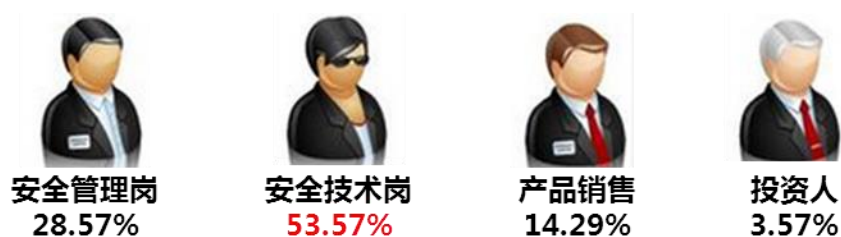
## 7) 连续创业更容易成功？

调查显示，有 30.3%的创业者有连续创业经历。但初次创业者有着更高的比重，说明网络安全创业潮还处于早期阶段。



## 8) 什么样的背景能创业？

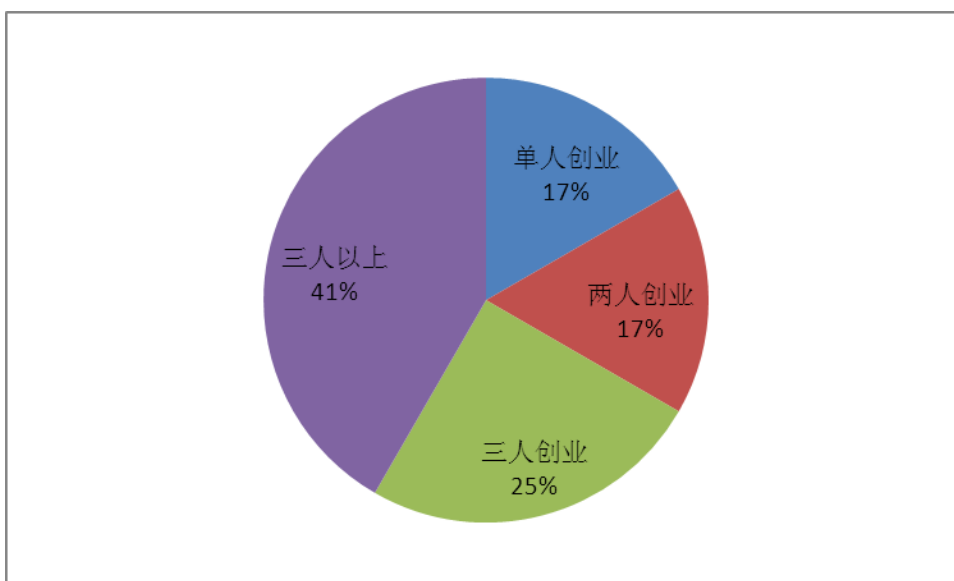
调查显示，从创业者创业前的履历来看，有安全技术背景的创业者占比较高。



## 9) 核心团队几人为宜？

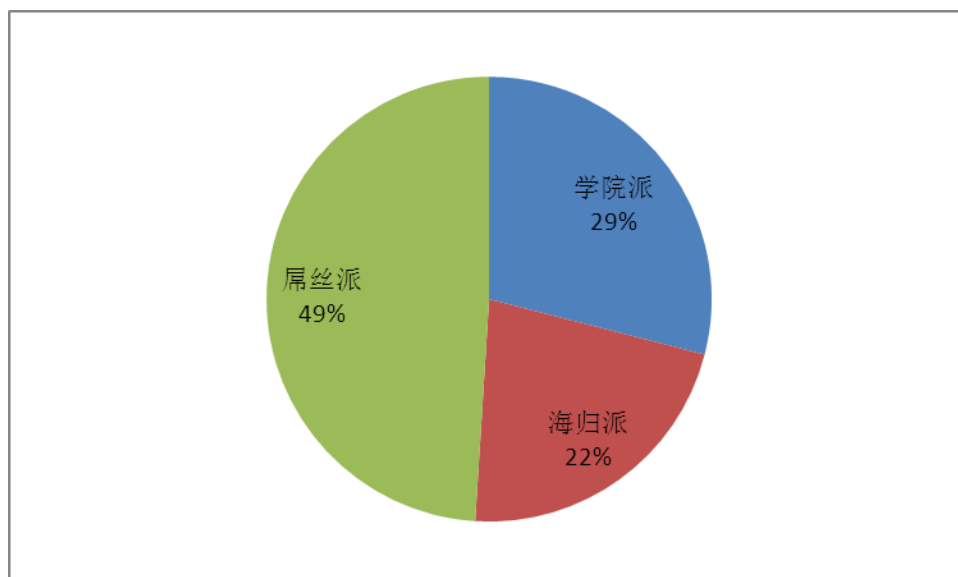
调查显示，网络安全已融资创业项目中 41.67%的项目核心团队人员在三人以上。这不是说明网络安全项目需要更多的小伙伴才能成功？





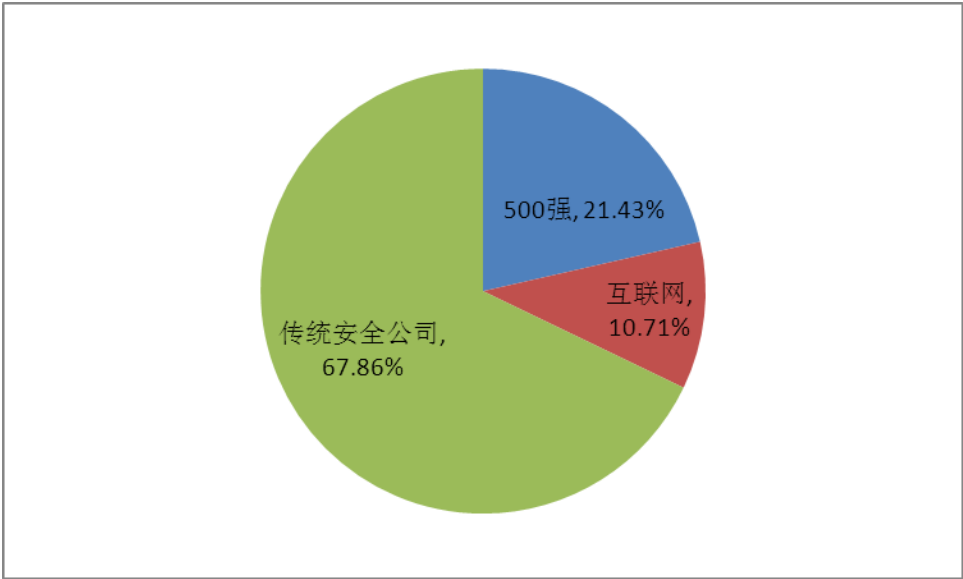
#### 10) 创业团队的流派分布？

调查显示，网络安全创业项目核心团队成员中，来自 985、211 等名校毕业的学院派占 29%，有海外从业经历的海归派占 22%，其他专科或普通高等院校毕业土生土长的屌丝派占 49%。



#### 11) 创业谱系

调查显示，来自传统安全公司的创业者在所有创业者中占比较大。其次为来自世界 500 强企业的安全团队，以及来自互联网公司的安全团队的创业者。



### 3. 创业挑战

#### 1) 什么是创业成功的核心要素？

在调查中，创始人反馈，团队是创业成功的最核心要素。其次是创始人个人魅力，产品市场定位，团队技术实力等方面。

排名	创业成功的核心要素
第一名	团队
第二名	创始人
第三名	市场定位
第四名	技术实力
第五名	资金保障
第六名	产品竞争力

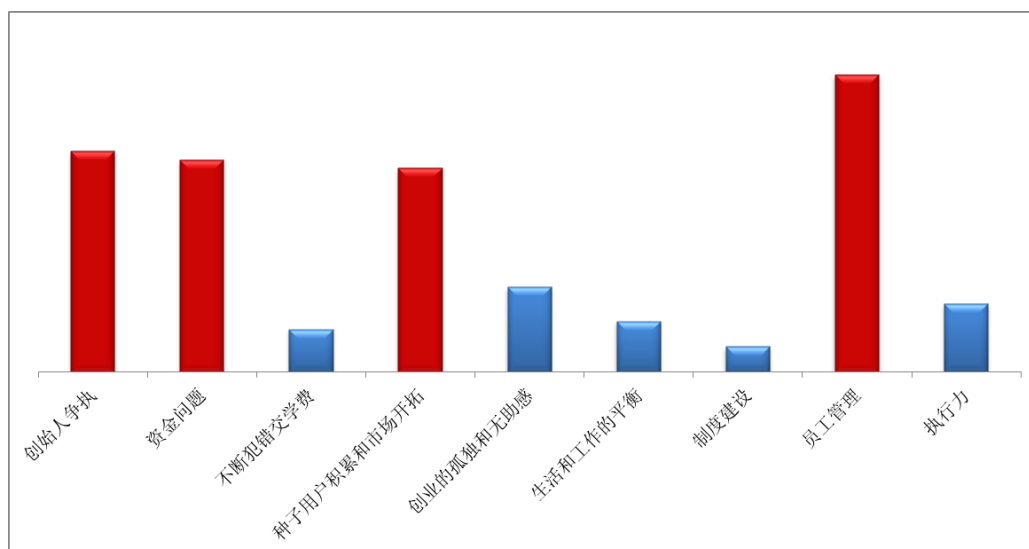
2) 困难排名

在创业过程中最大的困难时找不到合适的人才，其次是市场及客户的拓展，用人成本越来越高以及融资的困难等方面。

排名	创业中的困难
第一名	找合适的人才
第二名	市场客户拓展困难
第三名	人力成本高
第四名	融资困难
第五名	技术研发瓶颈
第六名	缺乏运营经验
第七名	政策环境阻碍

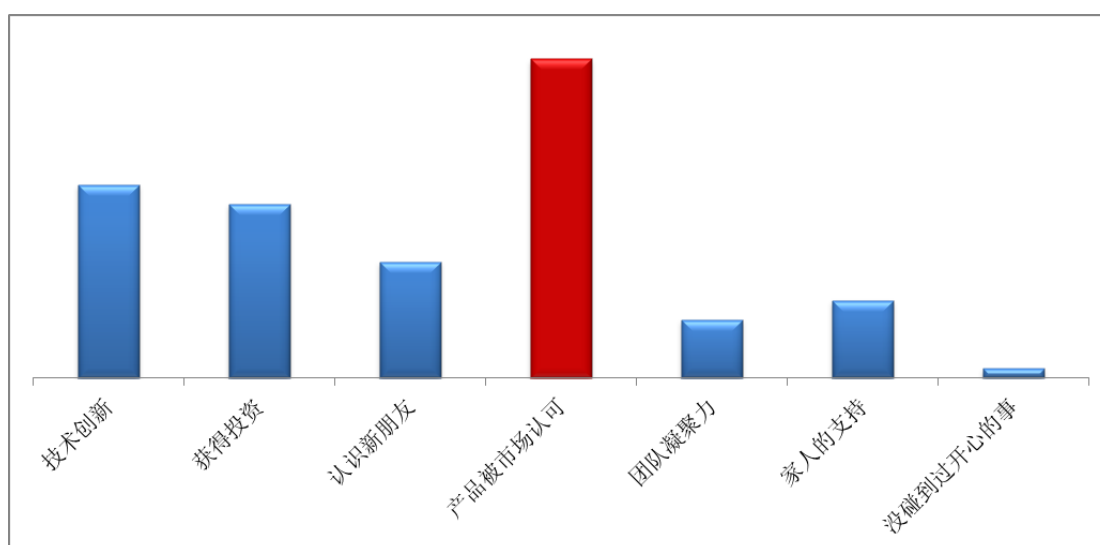
3) 创业中最痛苦的事

调查显示，创始人争执、资金问题、种子用户积累、员工管理是创业过程中令创业者最痛苦的事。



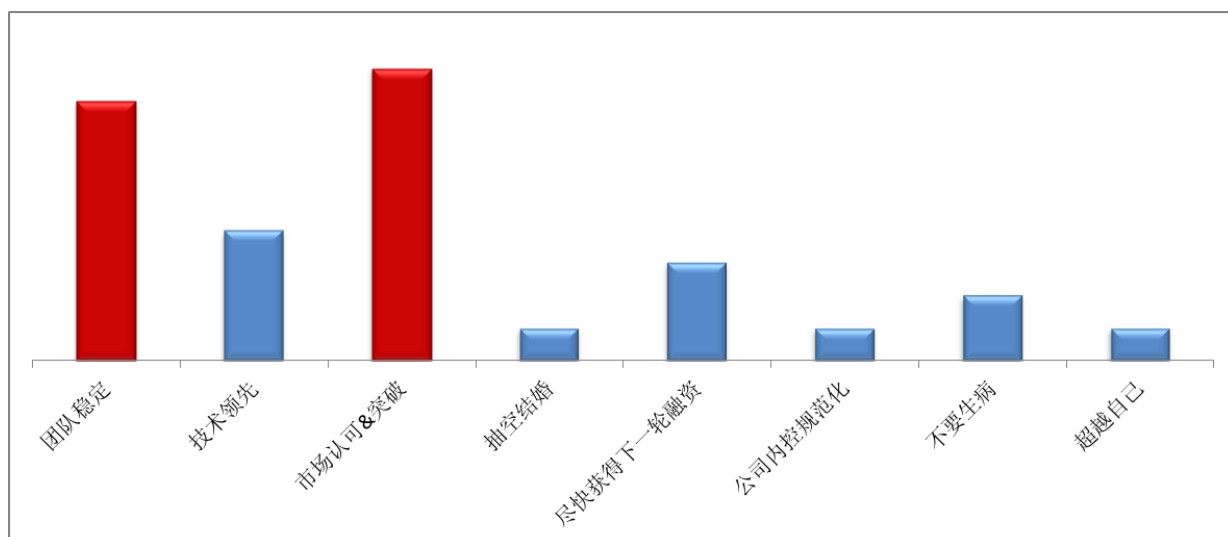
#### 4) 创业中最开心的事

调查显示，在创业过程中，最让创业者愉悦的事是在产品被市场所认可。



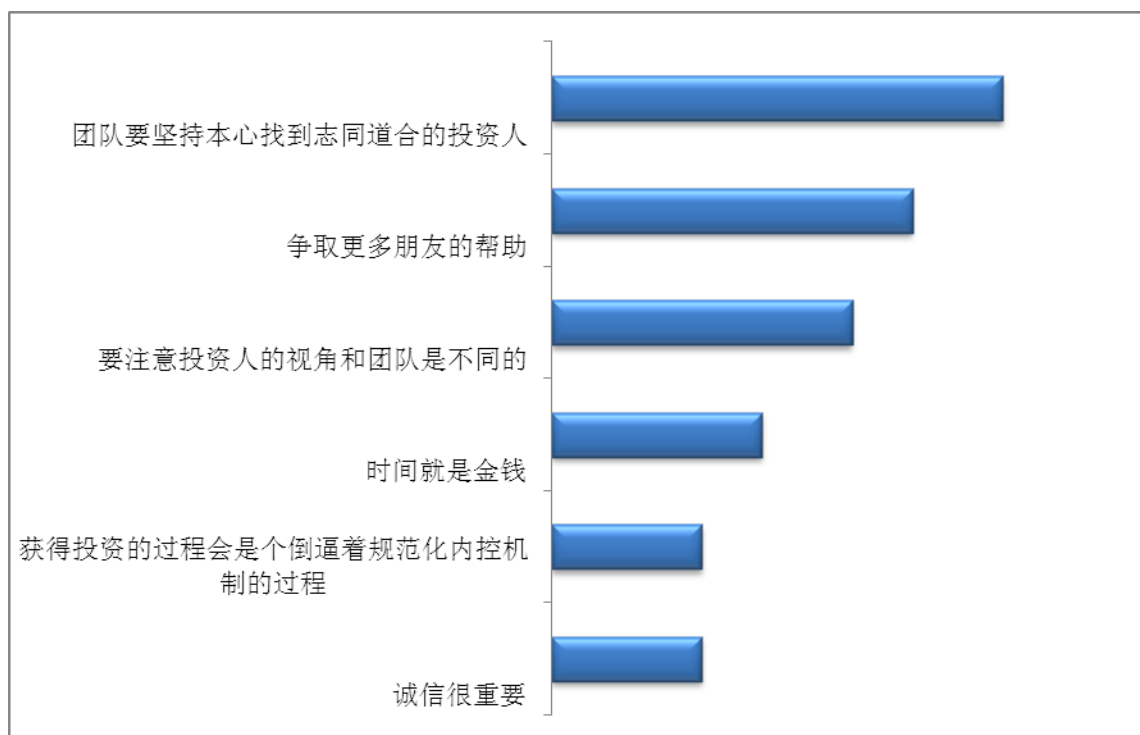
#### 5) 创业者的愿望

创始人最大的愿望是产品被市场认可以及团队稳定。



## 6) 争取投资时的建议

当问及在创业过程中争取投资的心得时，多数创业者表示，坚持本心，找到志同道合的投资人是争取投资过程中最重要的信念。

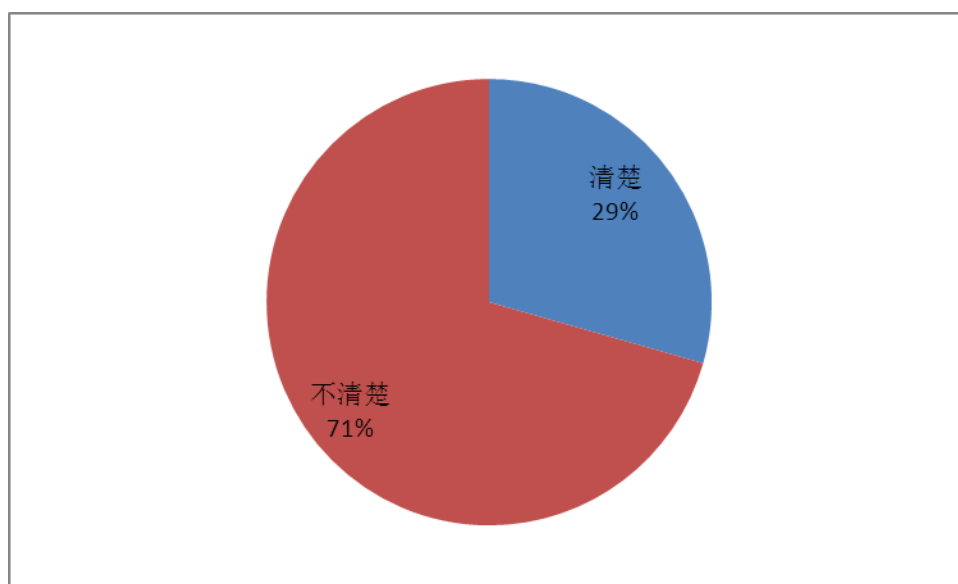


## 4. 创业投资

本次对投资机构的调研涉及已成功投资过网络安全领域项目的投资机构 15 家，从局部展示投资机构对网络安全创业项目的态度和观点。

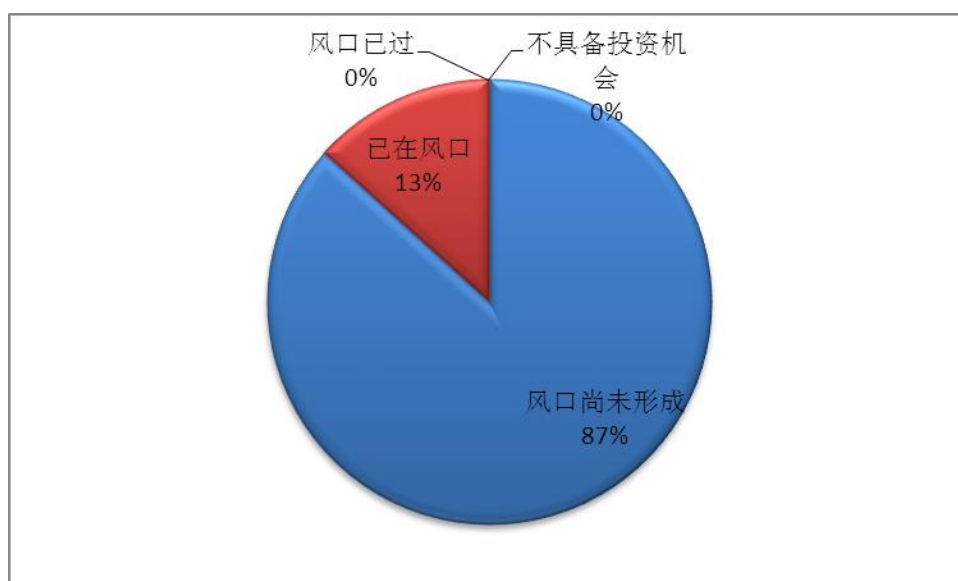
### 1) 对网络安全领域情况的了解

调查发现，目前的早期投资人对于网络安全领域尚不十分清楚，只有个别机构专注于网络安全领域的投资。



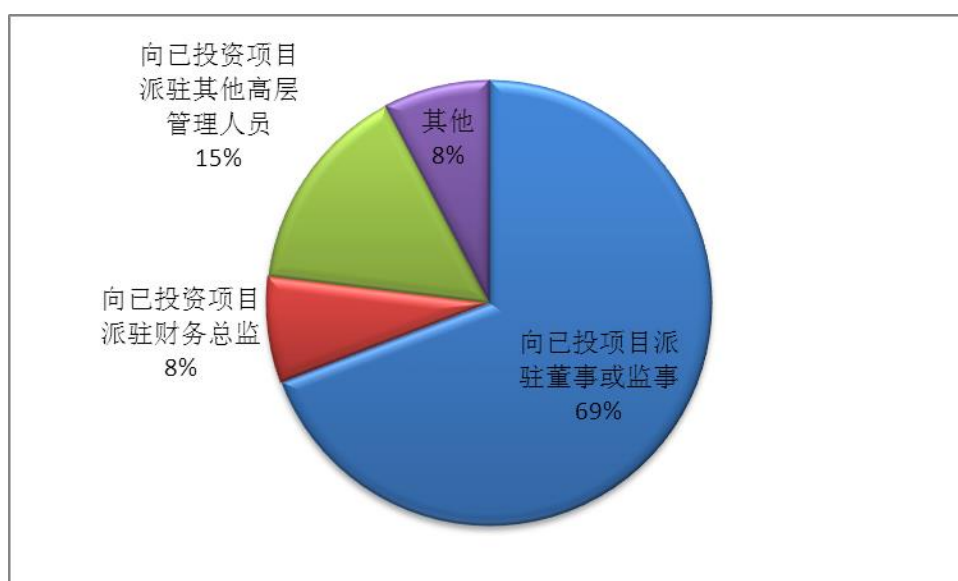
### 2) 对网络安全投资趋势的感觉

在 87% 的投资人看来，网络安全投资的风口尚未形成。



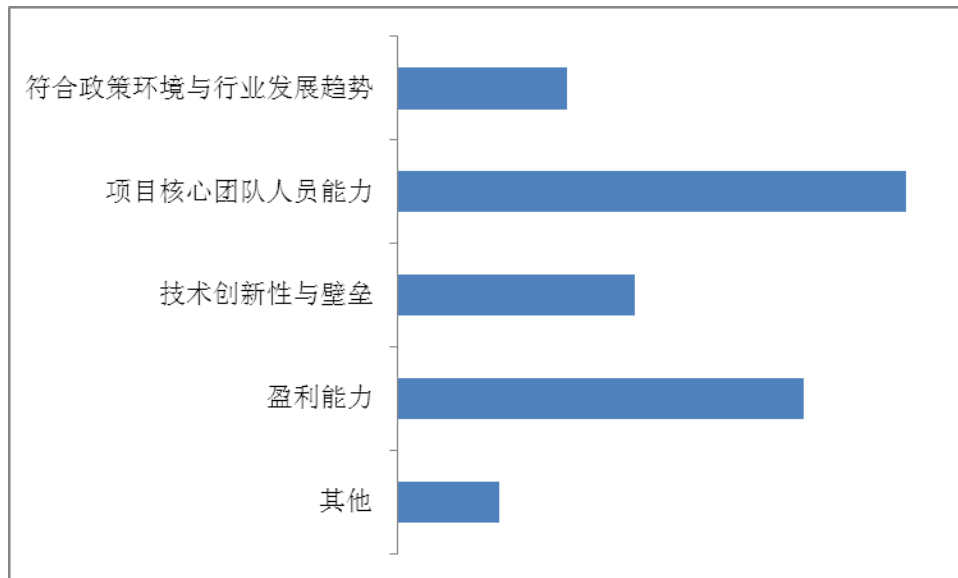
### 3) 对已投资项目通常的管理方式？

对于已投资的创业项目，投资机构最常用的是派驻董事或监事对项目进行管理。



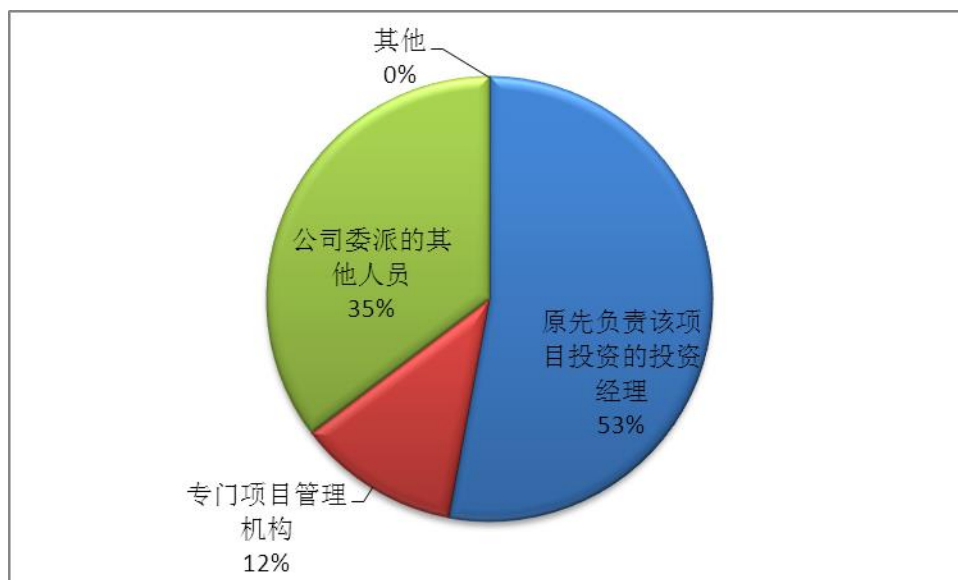
### 4) 最看重的是项目的什么方面？

投资人最看重创业项目的是项目核心团队的人员能力。其次是项目的盈利能力、技术创新性与壁垒等。



#### 5) 由谁负责对已投资项目的具体日常管理？

大部分的投资机构会选择在投资后由负责项目投资的投资经理参与项目的日常管理，另一部分投资机构选择委派其他人员对项目进行日常管理，有 12% 的投资机构选择由专门的项目管理公司对投资项目进行日常管理。





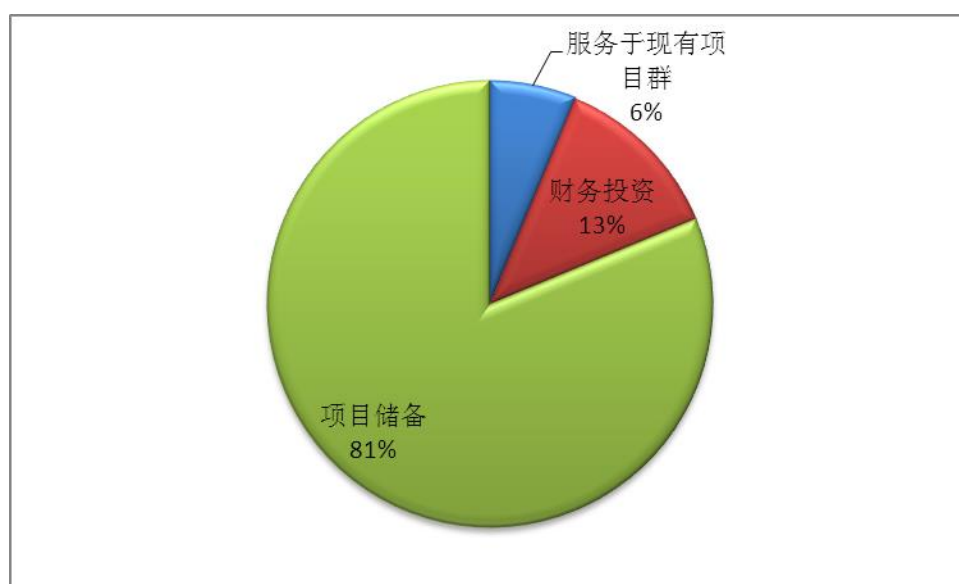
## 6) 是否在 2016 年继续追加在网络安全领域的投资

100%投资机构对 2016 年网络安全领域持续看好，会追加相应的投资。



## 7) 投资网络安全项目更看重

81%的投资机构目前投资网络安全领域的创业项目是为了项目储备，13%的投资机构是为了项目回报，6%的投资机构是为了服务于现有项目群。



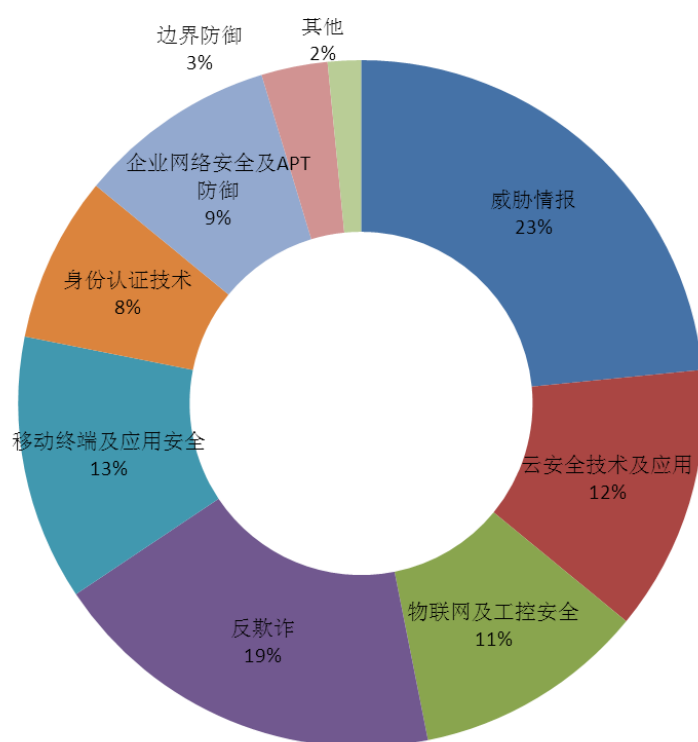
## 8) 投资人从哪些渠道获取项目信息？

调查发现，投资人发现创业项目的最有效渠道是通过朋友介绍，其次是参加各种会议论坛，创业比赛。

排名	项目信息来源
第一名	朋友介绍
第二名	会议论坛
第三名	创业比赛

## 9) 2016 年重点感兴趣的网络安全领域

调查发现，威胁情报、反欺诈领域是 2016 年投资机构最关注的网络安全领域。



## 四、 趋势观察

### 1. 网络安全行业最新特点

总体看来，网络安全创新创业呈现以下特点：

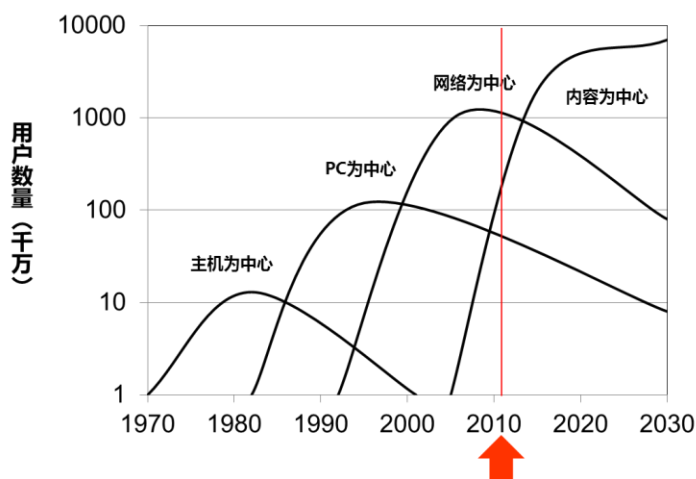
**国产化替代空间扩大。**伴随国家禁采 win8、禁用赛门铁克数据防泄漏产品等政策的提出，国产化替代机会凸显，网络安全将受到政府及重点行业的高度重视，国产网络安全产品有望在政策扶持下加快发展，国产化替代未来将有着巨大的发展空间。

**政企互动促进国家标准和行业规范发展。**2014 年，网络安全国家标准相继出台并实施，在政府标准和规范制定过程中，吸引了行业用户和企业的参与，企业作为网络安全的实践者更了解市场现状，对这些标准的顺利实施与推广起到了重要作用，通过政企互动推动国家标准和行业规范更符合中国网络安全国情，有利规范了网络安全市场健康发展。

**传统分散向资源整合发展。**一系列自主可控的政策明确指出要提高各重点行业网络安全国产化率，但现状是我国网络安全市场参与者数量超过 1000 家，主流网络安全厂商所占市场份额不到 50%，集中度较低，国内安全厂商企业规模普遍偏小，市场集中度分散，企业优势仅仅局限于某一个或几个细分领域，随着各领域优势企业资金和技术实力的增强，网络安全亟需形成整合式竞争优势以满足企业整体 IT 建设的需求。以自主技术为基础，以统一整合为主导，构建完整的信息化解决方案，才能适用目前快速发展的信息化需求，提升中国网络安全自主可控能力，未来传统分散的技术将趋于整合，行业集中度有望持续增大。

**数据安全成网络安全建设重点。**随着移动互联网、云计算的快速发展，数据成为用户信息的核心资产，“棱镜门”事件继续发酵，个人隐私意识和企业数据安全意识的双重提升。数据安全主要是解决数据级权限管理、数据防泄密的问题，也有利于解决云计算、移动互联网带来的系统边界模糊化导致的安全防护难题。国家相关监管政策的出台，预计金融、运营商和央企迈入数据安全建设的高峰期，而政府行业用户由于便民服务需求的紧迫性将紧随其后、快速启动。

**安全技术向以内容为中心转移。**在安全技术领域威胁情报、反欺诈、安全即服务等新型安全技术的发展，标志着安全技术正在以网络为中心的保护阶段向以内容为中心的保护阶段迈进。这一技术方向的持续发展将成为未来网络安全的主流形态。



## 2. 网络安全创业投资热点

通过对行业的观察，安在认为以下方面可能会成为未来网络安全发展的热点：

### （1）安全数据分析预警领域（威胁情报）

威胁情报一般包括信誉情报(“坏”的 IP 地址、URL、域名等，比如 C2 服务器相关信息)、攻击情报(攻击源、攻击工具、利用的漏洞、该采取的方式等)等。我们经常可以从 CERT、安全服务厂商、防病毒厂商、政府机构和安全组织那里看到安全预警通告、漏洞通告、威胁通告等等，这些都属于典型的安全威胁情报。而随着新型威胁的不断增长，也出现了新的安全威胁情报，例如僵尸网络地址情报(Zeus/SpyEye Tracker)、Oday 漏洞信息、恶意 URL 地址情报，等等。这些情报对于防守方进行防御十分有帮助，但是却不是单一的一个防守方自身能够获取和维护得了的。因此，现在出现了安全威胁情报市场，有专门的人士、公司和组织建立一套安全威胁情报分析系统，获得这些情报，并将这些情报卖给作为防守方的企业和组织。安全威胁情报市场现在是一个很大的新兴安全细分市场。

### （2）安全可视化领域

大数据可视化是个热门话题，在网络安全领域，也由于很多企业希望将大数据转化为信息可视化呈现的各种形式，以便获得更深的洞察力、更好的决策力以及更强的自动化处理能力，数据可视化已经成为网络安全技术的一个重要趋势。攻击从哪里开始？目的是哪里？哪些地方遭受的攻击最频繁.....通过大数据网络安全可视化图，我们可以在几秒钟内回答这些问题，这就是可视化带给我们的效率。

### （3）云端访问安全代理服务

云端访问安全代理服务是部署在企业内部或云端的安全策略执行点,位于云端服务消费者与云端服务供应商之间,负责在云端资源被访问时套用企业安全策略。在许多案例中,初期所采用的云端服务都处于 IT 掌控之外,而云端访问安全代理服务则能让企业在用户访问云端资源时加以掌握及管控。

#### **(4) 用户画像及适应性访问管控**

适应性访问管控是一种情境感知的访问管控,目的是为了在访问时达到信任与风险之间的平衡,结合了提升信任度与动态降低风险等技巧。情境感知是指访问的决策反映了当下的状况,而动态降低风险则是指原本可能被封锁的访问可以安全的开放。采用适应性访问管理架构可让企业提供不限设备、不限地点的访问,并允许社交账号访问一系列风险程度不一的企业资产。

#### **(5) 端点侦测及回应解决方案**

端点侦测及回应(EDR)市场是一个新兴市场,目的是为了满足不同端点(台式机、服务器、平板与笔记本)对高阶威胁的持续防护需求,最主要是大幅提升安全监控、威胁侦测及应急响应能力。这些工具记录了数量可观的端点与网络事件,并将这些信息储存在一个集中地数据库内。接着利用分析工具来不断搜寻数据库,寻找可提升安全状态并防范一般攻击的工作,即早发现持续攻击(包括内部威胁),并快速响应这些攻击。这些工具还有助于迅速调查攻击范围,并提供补救能力。

#### **(6) 新一代安全平台核心:大数据网络安全分析**

未来,所有有效的网络安全防护平台都将包含特定领域嵌入式分析核心能力。一个企业持续监控所有运算单元及运算层,将产生比传统 SIEM 系统所能有效分析的更多、更快、更多元的数据。预测至 2020 年,40%的企业都将建立一套“安全数据仓库”来存放这类监控数据以支持回溯分析。藉由长期的数据储存于分析,并且引入情境背景、结合外部威胁与社群情报,就能建立起“正常”的行为模式,进而利用数据分析来发觉真正偏离正常的情况。

#### **(7) 以遏制和隔离为基础的网络安全策略**

在特征码(Signatures)越来越无法阻挡攻击的情况下,另一种策略就是将所有未知的都当成不可信的,然后在隔离的环境下加以处理并运行,如此就不会对其所运行的系统造成永久损害,也不会将该系统作为矢量去攻击其他企业系统。虚拟化、隔离、提取以及远程显示技术,都能用来建立这样的遏制环境,理想的结果应与使用一个“空气隔离”的独立系统来处理不信任的内容和应用程序一样。虚拟化与遏制策略将成为企业系统深度防御防护策略普遍的一环。

#### **(8) 软件定义的网络安全**

所谓的“软件定义”是指当我们将数据中心内原本紧密耦合的基础架构元素(如服务器、存储、网络和网络安全等等)解离并提取之后所创造的能力。如同网络、计算与存储的情况,对网络安全所产生的影响也将发生变化。软件定义的网络安全并不代表不再需要一些专门的网络安全硬件,这些仍是必不可少的。只不过,就像软件定义的网络一样,只是价值和智能化将转移到软件当中而已。

### **(9) 针对物联网的安全网关、代理与防火墙**

企业都有一些设备制造商所提供的运营技术(OT),尤其是一些资产密集型产业,如制造业与公共事业,这些运营技术逐渐从专属通信与网络转移至标准化网际网络通信协议(IP)技术。越来越多的企业资产都是利用以商用软件产品为基础的 OT 系统进行自动化。这样的结果是,这些嵌入式软件资产必须受到妥善的管理、保护及配发才能用于企业级用途。OT 被视为产业界的“小物联网”,其中涵盖数十亿个彼此相连的感应器、设备与系统,许多无人介入就能彼此通信,因此必须受到保护与防护。

### **(10) 网络安全与国产化相关的人才教育**

目前我国网络安全方面人才缺口很大,相关专业每年本科、硕士、博士毕业生之和仅 8000 余人,而我国网民数量近 7 亿人,从业人员缺口达 50 万人。针对网络安全人才的培养将是一个可见的高速发展领域。另外,随着自主可控产品的研发和替换,随之而来的自主可控技术使用和操作相关的教育和培训市场也将逐渐升温。

## **3. 创业者应该关注的问题焦点**

网络安全领域已经面临了 5 年左右的黄金发展期,对于跃跃欲试的创业者来说,我们根据调研和访谈的情况,整理了创业者应关注的八个焦点问题,帮助大家厘清网络安全领域的创业思路,加大创业成功的砝码:

### **(1) 团队在哪里?**

创业项目的成败取决于核心团队的良优,对创业者来说,考虑初创团队的构建是第一重要的事情,构建具备一定专业度、内部沟通通畅、有进取心、执行力强的团队是成功项目的标配。这样的团队,即使首个项目失败,投资人也愿意继续帮扶,协步前进。

### **(2) 目标市场是否足够大?**

客户群体规模是又一重要元素,很多创业团队容易重技术、轻市场,把很多时间精力花在了技术研发上,忽略了产品的潜在市场需求,仅靠拍脑壳是无法验证实际市场需求的。假

如某项业务在思量下来市场规模不够大，那么及时技术实力再优秀也白搭。

### **（3） 是否具备壁垒？**

在面向一个大市场的情况下，创业项目是否具备足够的壁垒，也是非常重要的要素，壁垒可以是知识产权上的、也可以是技术迭代上的，也可以是推广速度上的，有基于自身优势形成壁垒的能力，是需要考虑重要一环。

### **（4） 是否据有可复制性？**

优秀的项目具有的特点需要既有很强的壁垒，又有很好的可复制性，一些安全服务类型的项目基于人员的经验和能力对外提供服务，可复制性就很弱，会比较劣势。

### **（5） 是否有军工潜力？**

网络安全是个细分的领域，就趋势来看，保障国家的网络安全是网络安全的重要组成部分，在创业项目初期也要考虑到在这方面的发展潜力。

### **（6） 是否在细分市场下具备了国际视野？**

网络安全领域创业往往产品面向的细分领域客户量较小，这个时候可以尝试拓展一下视野，看一下产品在国际范围内的前瞻性和竞争力，从海外市场切入可能会成为一击妖刀。

### **（7） 民用安全产品是否太超前？**

对一些 to C 的网络安全项目来说，由于普通民众对网络安全的感知尚在启蒙阶段，对实际的网络安全风险体会不深，因此切忌使用太过超前的理念，因为技术太超前容易死。

### **（8） 盈利模式在哪里？**

虽然早期项目的盈利模式并不是太重要，但是能盈利的项目和不能盈利的项目，估值会完全不同，能赚钱是创业项目可持续发展的立足之本。

## **4. 各方观点**

安在走访网络安全各界人士过程中，曾将网络安全创业作为专门一个话题，就此听取行业大咖、创业新锐以及企业人士的观点。总体上看，对这两年网络安全行业蓬勃向上的风潮，以及与“互联网+”相结合的网络安全创业的新气象，大家都给予了一致的积极看法，当然，也有不少经验人士，在保持乐观的同时，会指出其中略显浮躁或隐忧的地方。无论如何，从

近一年以来的种种迹象表明，中国网络安全产业正在迎来一波前所未有的发展机遇。

## 1) 方兴 (Flashsky, 闪空)

曾经的顶级黑客，原翰海源 CEO，现为阿里巴巴资深安全专家。其所创公司翰海源被视为中国版的 Fireeye，后被阿里巴巴收购。

“形势的确在变。我们创业的时候，市场对安全的重视很低，投资人出一点点钱，就能够占有 10%以上的股份，现在的创业公司比我们那时候好太多了，随便一个项目，10%可就是千万级以上的。除了投资环境，创业公司的归宿也好很多，BAT 对安全的重视，无形中多了很多并购途径，此外还有新三板上市，包括被其它大公司收购，等等。不过，再要像当初启明星辰和绿盟那样，走上独立上市的道路，就很难了。”

“从中国现实的情况来看，IT 领域有两块还没有形成普遍的消费认可，一是云，二是智能硬件。这两块，创业公司跟大公司有比较平均的竞争水平。好的创意、个性、快速迭代的方式，这些都是小公司相对大公司的优势。物联网、智能家居，健康医疗、汽车都还酝酿着大量的机会，其中智能汽车和医疗健康是很突出的两个方向，因为它与人的安全直接有关。我们以前说，网络安全的可见性不高，但是在这些新的领域，网络安全是可见的。比如汽车，要证明它有问题很容易，但问题是提出好的解决方案很不容易。将来谁能解决这些问题，很可能就会拥有一个巨大的市场。”

“在任何环境中都会出现泡沫，也会存在骗子，这是不可避免的，只要有热潮、有钱，就会这这些浮躁的东西存在。但是相对来说，安全比其他的环境要好些，因为安全本来就是个小市场，想忽悠也忽悠不了多少东西。其次是安全有专业门槛，稍微有几个懂的人，你就藏不住了。目前看来，安全领域不是没有泡沫，但是相比起其他领域要好很多。”

## 2) 季昕华 (Benjerry)

曾任华为、腾讯、盛大安全负责人，2012 年创业 Ucloud( 被誉为新一代的“独角兽” ) 并任 CEO，是网络安全圈公认的屈指可数的成功“转型”者之一。

“我一直认为，只有当创业公司眼睛盯着客户，屁股后面才会跟着投资商。你要了解投资者的利益，他们希望你赚钱，你做的好才会跟着你。你把产品做好了，他投你有钱赚，自然会投资你。”

“说到创业风气的变化，首先风口是在不断变化的，从手游到教育、金融、O2O、泛娱乐等，都在变化；其次热情从比较少到高峰甚至疯狂，那现在呢，互联网行业可能又遇到



冬天了；再有就是人群也在变化，原来是大公司出来的人创业比较多，现在似乎任何人都想创业，这可能导致泡沫，但是一个行业只有经历了泡沫后才会更成熟。”

“如果说个人反思，我觉得过去有 3 个错误以后不会再犯。首先是我们没有拿天使，这是非常大的失误。原来觉得用别人钱不好，现在觉得挺好。即便不缺钱，还是需要拿点小钱，可以用这个去做宣传。创业拿钱最关键的不是钱，而是背书，就像考证。其次是招人的方面，特别是招外企的人，因为民企的人还好，至少能沉得下去，但是外企的人不容易落地，不够接地气。还有就是人员结构，如果公司缺乏多样性，都是一类人，就会很危险。”

“对安全创业者来说，技术通常不缺，主要是方向和趋势的判断、团队的组建和管理，以及如何去抓用户吧。因为绝大部分安全圈的创业者都不是从销售做起的，很多人偏技术，缺乏综合性的能力。”

### 3) 谭晓生（谭校长，土人）

360 公司 VP，首席隐私官（CPO），网络安全多面手，最棒的“救火队员”。

“我个人认为，安全行业对创业者来说未必是个好领域。毕竟，安全这个行业能否挣钱？能挣多少钱？都还是个问题，如果有情怀也就罢了，但我看到更多的是有投机心的。说到底，安全行业有不明觉厉的特点，但更具声势的攻击和安全是两回事，我们最终要解决的是防御问题。在这把虚火之后，我们会看到，很多创业必然会以失败告终。问题在于，之后还有多少人心回去做技术，我非常怀疑。”

“需要警惕一种现象，现在基于竞争给出的估值都有点高，很多人看到了互联网公司的创富神话，所以对估值的期望会非常高。但是在期望和现实之间距离很大，如果干了两年到不了预期的估值，人就会很痛苦。”

“另外，互联网发展到现在，BAT 和 360，格局已定，要跳出来创业就会有成本收益的问题，代价会很大，又未必能在夹缝里发展起来，毕竟现有的安全市场还是太小了，未来的话，关键看政府和军队市场。说起来现在中国每年的网络安全民营市场也就两三百亿元，而涉及政府、军队的资金又差不多被机构和科研院所拿掉了，企业生存环境很差。所以我说，要看政府、军队市场未来两三年是否能开放，如果开放是好事，不开放就比较不乐观。”

“说实话，安全在 2 C 领域已经很难重复 3 6 0 的神话了，现在安全但凡有一点创新，大企业都会很快跟进，创新企业很难有机会。3 6 0 是基于大的用户基础，才有良好的转化效益，新的创业公司很难拿到这么多的用户。”

#### 4) 金湘宇 (Nuke, 金将军)

曾在启明星辰和埃森哲分别从事网络安全技术服务和咨询顾问工作,威胁情报在中国发展的重要启蒙者和推动者。现为“星源壹号”基金合伙人,也是网络安全界成功“转型”者之一。

“记得一份市场研究报告里提到,IT 市场增长最快的细分领域是移动相关的,第二就是网络安全领域。国内网络安全市场的平均增长率可能已经接近 20%,这个增长率其实已经很高了,可以对比的是 GDP 增长率为 7.4%,IT 市场的增长率为 8.4%。增长率高说明机会多,尤其是对于初创公司来说。如果一个行业的增长率很平稳或者很低,市场比较稳定,那新公司的机会就相对较少。增长率越高,新公司从增量中可能获取的份额就会大。所以说,至少从这一点看,网络安全还是很不错的投资领域。”

“中国目前的网络安全市场严格来说是个合规性市场,市场主体还是政府和各大央企。随着互联网的发展,政府政务要公开,甚至政务要上云,互联网威胁变得越来越现实。新刑法修正案以及其他一些网络安全相关的法律法规也已经开始陆续出台,可以预期,合规性需求会呈增多的趋势,因此网络安全行业未来会有一个爆发式增长的机会。”

“对初创公司来说,合规性市场往往难以进入。但是 IT 基础环境在快速变化,传统 IT 架构也正在向云计算迁移,大数据、物联网、移动办公、社交媒体等新的领域也正在逐渐进入主流市场,这中间初创公司都有很大的机会。”

“目前一波网络安全创业的可以分成几类,一类是之前有过成功的公司团队组建和公司运营经验的,现在做二次创业,这种成功率相对要高一些。还有一类是以前在传统安全企业里的,比如做售前、做销售的,懂一些解决方案,也有一些客户资源。再有一类就是互联网公司或者其他渠道的以技术人员为主的创业,这些人技术往往会很有前瞻性。”

“关于方向,一个是云安全服务相关的,因为基于云的架构对传统架构的更迭势头基本已经是不可阻挡的,新的基于云的架构下对应的安全防护体系自然也需要更新。再一个就是威胁情报相关的,威胁情报实际上是对安全整体解决方案的一次整个的提升,把以前孤立的产品给连接起来,甚至跨组织进行连接协同,以防火墙、IPS 等传统安全设备为例,这些设备未来都需要支持外部威胁情报,产品需要整个进行升级,这其中的机会就会很多。除此之外,值得关注的领域还包括移动安全、物联网安全、工控安全等。我认为移动安全市场已经逐渐开始成熟,但物联网安全、工控安全市场成熟还需要时间。至于大数据安全,的确很热,但如果只是停留在概念上,就比较泛泛。大数据是一种基础技术,其中包含和引申的东西太多了。我个人更倾向于做稍微具体一些的东西,比如说反欺诈、用户行为分析、网络行为分析、内部威胁发现等。同时大数据安全领域还有一个双刃剑,就是开源架构,很多的大数据安全概念都是大量基于开源构建,其自身真实价值难以体现。”

“对现在的创业者来说,能选择来做的东西其实很多,每一个领域都是有可能成功的,

但创业者要注意自己的执行能力。我看到的网络安全领域创业者最常见的问题就是看好了方向,也有技术,但就是没想好做好了怎么卖,怎么赚钱,这往往会成为未来发展最大的问题。”

“传统合规市场并不是滴水不进,这个市场的空间依然很大。为什么呢?因为出货量大呀。很多人可能觉得,现在还去做防火墙?还去做漏洞扫描?哪有人买?事实上,传统市场的容量相当大,就算你自己卖不了,还是可以通过渠道获得很大的销售量。”

“我认为比较好的模式,是既有技术先进性,也能赚钱的模式,创业公司需要将这两个灵活进行组合。比如我做一个盒子可以卖给传统市场,虚拟化放到云上卖就变 IaaS 了,自己租了云主机提供服务就又变成 SaaS 了。创业者不必追求凡创业必不能做合资非做云服务。DLP 也好,防病毒也好,都是有多种部署形态的,不用太过拘泥。”

“对创业公司来说,一定要有一个可以赚钱的业务模式,这其中建议可以关注一下传统企业市场。互联网安全市场跟传统企业安全市场比起来,互联网客户多是小公司,往往很在意成本。相比而言,传统企业市场才是真可以赚很多钱的地方,项目较大,利润往往也有保证。当然不能说互联网模式短期就不赚钱,有一些互联网模式的还真能短期赚钱,但总的来说,我认为短期内传统市场还是必须要关注的,它是可以赚很多钱的市场。”

## 5) 张矩 (光速资本)

安全是是我们看的三个方向之一,首先是移动和 saas,其次是基础架构,包括云计算和大数据,第三是网络安全。这三个都叫企业 IT 服务,在整体投资这三个占比有四分之一。

网络安全项目首先要对了趋势。有几个大的趋势,首先是安全态势发生了很大的变化,传统的以边界为导向的安全发生了很大的变化,在可控的边界上建立自己的地盘,边界越来越模糊,由于云计算和移动的原因;其二更大的趋势,线上的部分和线下的部分越来越紧密,界限也越来越模糊,比如在线下写信或者买东西的快递,你从来无所谓把家庭地址给谁,因为不给别人是不行的,但是这些信息在线上是比较敏感的。这个对下一代技术安全产品会产生很大的影响。今年政府会推出 EID (电子身份),这个还是很不错的,但是如果如果没有配套的安全和防范,可能会有很多想象不到的危害。真实身份暴露出来带来的安全问题,可能会比没有 EID 时更大。所以我们觉得网络安全是非常趋势型的东西,这些都会对。

其次要看团队,这个很重要。安全领域团队是尤为重要,安全的本质是对抗和攻防,到了金字塔尖就是高手对决,而且像现在的 APT, 0day 中,人的成分变得非常大,到了最高端已经不是系统化或者大家可以模仿的东西。所以这个领域里好的团队是非常重要的因素,包括经验的积累,这也是为什么 BAT 会花高薪去储备这样的人才。好的团队都被 360、腾讯或者阿里收购了。

我看好的细分领域里，安全情报是很重要的，但是什么形态是好的，这是有待探讨的，而且很重要的要求是情报的质量，这并不是简单的归纳就是情报，这是很大的领域。安全情报的很大部分是移动安全；还有非常基础性的东西，比如身份管理；和共享经济相关的分布式环境下的数据安全，数据的防泄漏、数据的一致性都是相关的重点。

安全涵盖了非常广的细分点，安全本身也是系统性工程，这里有很多内容都在发生，也需要非常全面的视角来看待，我们尽量把这些事情更加系统化的看待，这也是我们选项目。

安全有点像保镖，安全服务的价值，取决于保护的数据的价值。安全是为了保护机构的数据资产能够被正确的人在正确的时间访问。如果数据资产非常值钱，那么相关的安全方案一定也是很值钱的。所以安全为什么在中国是相对小的市场，这里面主要的原因是数据资产的泄露造成的损失非常小的，基本是公关的课题。比如携程的数据丢失，损失也就是公关的费用，既没有罚款，也没有用户的起诉，所以安全产品的价格高于公关的价格，就没有人用。所以安全在中国基本是合规的市场，合规的市场意味着达到等级保护就免责了。合规和等级保护是被动的市场，唯一的动力是用最低的价格拿到合格证，所以中国的安全现状是非常小的市场，这是非常不正常的。随着中国数据资产的增值和数字经济的发展，这件事从乐观方向来说，会朝着好的方向发展，那么这件事就会很有价值。现在还是在加速的。美国金融机构 IT 开支的 40%是在安全的，因为一旦发生问题是非常不可想象的，这个比例一定是按照数据价值来决定的。

2015 年随着双创，各个行业创业都有点过热，这是很明显的现象。2016 年会正常化一些，不是所有的人都急于创业，2016 年会更理性。但是安全肯定是越来越热的，因为现实状况是越来越严重，我觉得爆发点还没有到来，在这段时间还处于积累的状态。方向一定是往好的方向发展。

## 6) 胡洪涛（苹果天使投资）

以前的基金投过五个和网络安全项目，还有 4 个项目在运行；这一期的基金全部是安全，5000 万的规模。我们比较专注，不像别的投资机构什么都投，比如 TMT 行业；还有一部分基金是投 IT 技术架构，我们把资金全部投向网络安全。

网络安全和别的行业不同，是技术难度比较高的行业，需要掌握很底层的技术，不是大众随便能创业的行业，技术门槛更高。其次还需要懂行业，通常都是要在行业中了解业务后才能创业，所以还有业务门槛。所以这个行业和其他行业不太一样，比较偏技术创新型，没有技术创新肯定不投，这里没有商业模式可言。

全球来看，网络安全在持续升温，比如“威胁情报”，在美国类似公司都融到了数千万美元，这属于主动防御。现在有很多潜伏性的病毒，一般企业都感知不到，所以企业就需要

做体检，这就是风险监测，但是时间频率可以不一样，不能等头痛才去看医生。不要等到有攻击了才去防御，有类似的危险发生，就要主动防御。现在情报变得很重要。威胁情报在遥远的未来是个有前途的行业，但是目前还比较早，目前还是“头痛医头脚痛医脚”朝着“风险监测”在走，这个第二阶段都还没做出什么特别好的产品。现在威胁情报估计很难赚钱。现在很多企业连防火墙都没装或者没用好。还有“反欺诈”，欺诈在亚洲比较猖獗，所以做反欺诈也是离钱更近，这是有投入产出比的。这是刚需。“移动端”安全和“云端”安全是趋势，目前反欺诈也就是聚焦于这两端。

在项目的投资上，我们主要会考虑趋势，大趋势要在适合的时间窗口，比如现在做防火墙、杀毒，再好也可能没机会，基本是云安全、移动安全，比较符合发展潮流。同时，团队要比较强，是比较潜在的行业第一，有技术壁垒。行业里面很难碰到陌生人，只是看熟悉到什么程度。我们投过的人，安全圈还是一大票都知道。

安全这个蛋糕现在还没到快速增长的时间点，还要再等一等。现在舆论、政策都是比较热，但是确实落实还需要观察。比如安全法，什么企业做什么事还没有落地，都还没有正式的法规，等到颁布可能要在 2016 年，真正实行还要到 2017 年，安全法可能会有促进作用。还有工控安全，我国是制造业大国，这块基本就是空白，这块也应该纳入等级保护、国家安全范畴，不然被网军、黑客弄了，后果也比较严重。这些东西也都应该有合规要求。美国已经开始陆续颁布法规，包括军备企业的安全怎么保障。在中国，安全还是太新了，发展至今不过 20 年，法规是一片空白。未来还是有潜力，把安全意识变成安全法规，再到技术，可能还需要 5 到 10 年的时间。

网络安全的融资能力目前在不断提升，从 2011 年开始做投资网络安全，那时做安全没有人听得懂，而且没有人愿意听。现在基本上稍微大一点的基金，都很喜欢安全的案子，先不说听不听得懂，现在安全的案子比所有行业都要相对好融。13 年棱镜门是个“转折点”，然后就起来了。对于安全没有寒冬的感觉。

## 5. 总结

长期以来，在其他互联网创业者相比，网络安全创业者更像是金庸小说中的“逍遥派”，神秘、高冷、稀少。当然，这也和网络安全的行业特性有关，如果不是在行业中浸染多年的老手，决然不能做出什么成果，更不用说自立门户、融资发展了。

那么，是什么阻碍了网络安全创业者走向人生巅峰、赢取白富美呢？为此，“安在”潜心走访了数十位行业大佬、创业者和投资人，听取了多方意见，在进一步确信网络安全行业整体欣欣向荣的同时，也看到了一些具有浓郁行业特性的创业短板，妨碍了更多创业者在网络安全行业取得更高的成就。

## **（1） 缺少精准扶持网络安全的政策。**

很多创业者和投资人的共同感受是，如今网络安全行业的特征是“政府声音大，市场雨点小”。

一方面，在“棱镜门”的直接推动下，国家成立了网安小组、出台各种政策、做出各种表态，将网络安全提升到国家安全的高度。但是另一方面，大量互联网企业在信息泄露之后依旧免责、监管部门或法律对于企业网络安全没有刚性要求。

网络安全归根到底是“合规驱动”性市场，在缺少来自监管或法律的刚性要求之外，光靠网络安全行业的恐吓或者科普，虽然会让企业或者消费者开始意识到网络安全的重要性，但是距离为网络安全买单还有很长一段距离。

此外，政府虽然已经从国家战略高度开始重视网络安全，但是在政策末梢上对于网络安全的关注还是有待加强。

例如，在“安在”走访北京、上海、杭州、深圳等城市，遍访数十位创业精英之后，尚未发现哪座城市有任何一个定点扶持网络安全的创业园区或者孵化器，又或者针对网络安全企业有着特殊扶持政策的规定。反观被誉为“创业的国度”的以色列，则雄心勃勃地计划将贝尔舍瓦科技园打造成以色列乃至全球范围内范围上的网络安全中心。相比之下，中国的网络安全创业还如同星星之火一样，在各地伴随着网络安全传道者一起，像蒲公英一样随风起伏，而缺少一片优渥的土壤。

## **（2） 主要用户“玻璃门”依旧存在。**

目前网络安全的主要用户其实集中在政府、军队、银行等国有背景机构。但是，对于很多网络安全创业这来说，这部分市场只是可望而不可即的存在。所以，目前绝大部分网络安全创业企业都是以互联网企业为销售对象。但正如上文所述，由于目前法律法规及外在环境对互联网行业的合规要求比较低，所以，这也导致很多网络安全创业企业难以为继。

正是因为阳关大道走不通，才导致部分网络安全从业者开始走“独木桥”，即灰色产业乃至黑色产业。又或者，他们干脆“逃离”网络安全产业，进入其他相关的互联网行业。

十年树木百年树人，在网络安全行业尤为如此。对于网络安全行业，其实不需要更多的扶持政策，最重要的就是将市场开放，创造更为平等和开放的市场。让网络安全人才能够有机会为国效力，而不是报国无门。

而且，过多的“玻璃门”也不利于网络安全人才的培养。很多网络安全人才都是起于兴趣、成于专研但是逃于前途。如果没有相对平等的存量市场，坐等增量市场的扩展，就不会有一代代的年轻人愿意投身网络安全市场

### （3）技术长板与影响力短板并存。

在调研中也显示，很多网络安全创业团队均为资深的“技术宅”，“安在”走访的每个创业团队基本上都有一套成型的产品和过硬的实力。

但是，创业不仅仅是写完代码就了事，即使是以技术驱动型企业，比如谷歌、百度等，也都有很多市场、运营乃至营销人员，以不断提升团队的影响力。提升影响力不是为了“作秀”，而是为了让销售客户和投资人更好地了解自己。

目前组织网络安全创业团队“外向”的原因在于两点，首先是技术背景出身的人会更相信技术决定一切，其次网络安全行业本身就相对封闭，这也让他们缺乏感知到与外界沟通的必要性。

但是，网络安全创业真要做大做强，必须要关注“需求侧”，让那些可能听不懂技术、但是真正需要网络安全服务产品的人，能够了解、熟悉乃至信任网络安全创业团队的产品。可以这么说，传统的网络安全企业更加注重是自己所在“供给侧”，而未来的网络安全企业则必须关注客户所在的“需求侧”。从这个角度来看，目前网络安全创业也亟待一场“供给侧结构性改革”。

当然，和以往相比，如今网络安全行业已经更加重视品牌建设了。于是，各类比赛、论坛、活动已经此起彼伏，吸引了更多行业以外的大众媒体和公众的关注，有些比赛诸如“极棒”甚至还能造成不小的声势。不过，如果放眼更宽泛的视野，“安在”还是在调研中发现，很多人还是有中感觉，即很多活动是“圈内热热闹闹，圈外无声无息”。显然，在很多网络安全创业者在抱怨“对牛弹琴”的同时，也需要看清楚一个事实，即整个网络安全行业的品牌建设还是有待加强。

### （4）产业碎片化问题普遍存在。

进入互联网时代之后，网络安全创业也沾染了互联网时代的特色，在风投的加持下、快速迭代的风格下，新时代的网络安全企业开始从“大而全”走向“小而美”。

以前诸如启明星辰、安恒等安全企业，多数是追求业务覆盖面广、服务能力强等特色。但是随着越来越多的安全人才涌入市场，“小切口”、短平快的网络安全创业项目开始成批出现。这些创业者根据自己的一技之长和市场所需，通过一个个小步快走的产品在满足市场的需求。

但是问题也随之而来。正如安卓系统一样，通过提升开放性满足了大量手机厂商的独特性，提升了消费者选择的多样性，这也不可避免地带来了行业的碎片化特性严重。同样，在互联网时代的网络安全行业，随着大量的网络安全创业此起彼伏地成立。

那么，谁来成为这个日趋碎片化的产业链的整合者？目前还没有合适的角色。虽然目前BAT 都扮演着重要的“金主”角色，但是由于其浓郁的帮派色彩，因此不同帮派之间也会导致与邻为壑的弊病。同样，政府虽然最适合扮演整合者角色，但是由于专业能力和效率因素，目前整合效果仍有待观察。

一句被反复提及的话就是，“这是最好的时代，这也是最坏的时代”。对于网络安全行业来说，很多身处其中的人想必也深有同感。

如果站在十年乃至二十年的时间维度回望当下，网络安全一定会是重要但不那么耀眼的存在。过高的进入门槛、平平的想象空间、有限的应用场景，都让这个行业成为互联网行业“殿后”的角色，在急速飞驰的行业最后前进。但是，所有人也都明白，如果没有网络安全行业的护持，那么再光鲜亮丽的互联网行业也不过是空中楼阁。网络安全不是“皇帝的新衣”，而是“皇帝的卫队”，不可或缺的存在。

“安在”访问过的所有投资人和创业者均认为，网络安全行业还没有到真正爆发的时候，但是距离那一天也不远了。

那么，在上述种种的矛盾和未来之间，如何搭建起一座不绕弯路的桥梁？对此，“安在”提出以下两点思考，权当抛砖引玉吧。

## **（1） 信息安全将会成为整合行业的纽带。**

放眼任何一个新兴行业，凡是行业崛起前夕，必有相关信息平台崛起。比如最近新热的VR、区块链行业，就已经在一些投资人的支持下，一些垂直媒体和信息服务商应运而生。

同样，上海市市委相关领导也表示，上海市科技行业产业化之所以滞后，与科技中介的缺失有重要关系。所谓科技中介，就是在市场与技术之间搭建起桥梁，本质上就是信息服务业。

对于网络安全行业来说，也是如此。网络安全行业由于专业性，因此必须要有专业的团队来了解和梳理行业信息。同样，也要有针对同行业甚至跨行业的传播，以此提高行业内部的整合程度，以及对外的传播效果。

## **（2） 拓展应用场景成为“做大蛋糕”的不二法门。**

对于网络安全行业来说，做大蛋糕远比如何分蛋糕重要。因此，系统梳理当前市场上对于网络安全的需求情况，同时满足这些需求，将成为接下来网络安全行业重要的沟通工作，这样也才能有的放矢。

但是，这也算是一门比较系统的信息梳理工作，应该由更加专业化的团队来执行。原来的运作模式是创业团队完成一条龙的调研、开发、销售。但是随着行业生态的不断成熟，如



何用好用活行业内部资源，在行业内部形成精准、细分的专业分工，同时不同环节之间能形成无缝对接，最终展现在市场面前的是一个具备极强自组织能力的智慧行业。或许，这正是未来网络安全行业的最佳的发展形态。

## 附录：

### 1. 近年来国际网络安全初创项目（部分）

公司	主营	融资额	阶段
Illumio(加州森尼韦尔)	云及数据中心安全平台	1 亿美元	C 轮
Skycure(以色列特拉维夫)	移动安全	800 万美元	Pro A 轮
Lookingglass(弗吉尼亚州阿灵顿)	网络威胁情报监控及管理	2000 万美元	B 轮
Sqrrl(马塞诸塞州剑桥)	网络威胁识别及响应的大数据分析	700 万美元	B 轮
Team8(以色列)	安全智库	1800 万美元	A 轮
Pindrop Security (佐治亚州亚特兰大)	防电话诈骗及呼叫中心验证	3500 万美元	B 轮
Dtex Systems (加州 San Jose)	内部人员威胁防护方案提供商	1500 万美元	A 轮
Darktrace	网络安全	1800 万美元	A 轮
SecureKey Technologies(加拿大多伦多)	身份及验证	1900 万美元	C 轮
Zimperium(加州旧金山)	移动威胁防御	1200 万美元	B 轮
Emailage(亚利桑那州钱德勒)	反欺诈	380 万美元	A 轮
Evident.io(加州都柏林)	云安全	985 万美元	A 轮
V-Key Inc.(新加坡)	移动安全及密码技术	1200 万美元	B 轮
Endgame(弗吉尼亚州阿灵顿)	安全情报及分析工具开发	3000 万美元	C 轮
CipherCloud(加州圣何塞)	云可见性及数据保护	5000 万美元	B 轮
Clef (加州奥克兰)	利用 Apple 指纹阅读器双因素认证	160 万美元	天使
Cyber Squared (弗吉尼亚州阿灵顿)	网络威胁情报平台开发	400 万美元	天使
NowSecure (伊利诺伊州奥克帕克)	移动设备数据安全	1250 万美元	A 轮
ThreatStream (加州雷德伍德城)	SaaS 网络安全威胁情报平台	2200 万美元	B 轮
NexDefense (佐治亚州亚特兰大)	网络安全	240 万美元	天使
DB Networks (加州卡尔斯巴)	机器学习及行为分析安	1700 万美元	A 轮

德)	全		
Nok Nok Labs (加州帕洛阿尔托)	身份验证	825 万美元	C 轮
Area 1 Security (加州门洛帕克)	社会工程攻击	800 万美元	A 轮
EdgeWave 加州圣地亚哥)	军方网络安全	200 万美元	A 轮
Vkansee Technology (北京)	移动安全指纹传感器	700 万美元	A 轮
iSIGHT Partners (德克萨斯达拉斯)	网络威胁情报	3000 万美元	C 轮
Ionic Security (佐治亚州亚特兰大)	企业分布式数据保护	4010 万美元	C 轮
Phantom Cyber	汽车网络安全	270 万美元	天使
CloudLock (马塞诸塞州沃尔瑟姆)	云数据安全	670 万美元	D 轮
Veracode(马塞诸塞州伯灵顿)	云应用安全	4000 万美元。	F 轮

## 2. 近年来中国网络安全初创项目（部分）

项目	融资时间	阶段	融资方	公司成立时间	投资方	投资金额
乌云网	2015-7-23	A 轮	北京北冥鱼信息技术有限公司	2015.1	红杉资本中国	数千万人民币
通付盾	2011-11-1	种子天使	苏州通付盾信息技术有限公司	2011 年 10 月	未透露	数百万人民币
	2012-8-1	A 轮	苏州通付盾信息技术有限公司	2011 年 10 月	未透露	数千万人民币
长亭科技	2015-9-24	种子天使	北京长亭科技有限公司	2014 年 7 月	真格基金	600 万人民币
上海翼火蛇	2015-5-15	种子天使	上海翼火蛇信息技术有限公司	2013 年 12 月	新进创投	数百万人民币
山石网科	2007-3-	A 轮	山石网科通信技术(北京)有限公司	2007 年 2 月	启迪创投，北极光创投，奥迈资	600 万 USD

	22				本	
	2009-5-22	B 轮			伟高达创投 Vickers Capital , 北极光创投	1000 万 USD
	2011-8-22	C 轮			投资方未透露	数千万 USD
	2015-5-28	D 轮			北极光创投	数千万 USD
北京远为软件	2013-7-1	A 轮	北京远为软件有限公司	2012 年 2 月	中路集团	1500 万 人民币
威客安全	2015-7-26		北京锦龙信安科技有限公司	2014 年 1 月	如山创投，北京厚持投资，瞰澜天使基金	2000 万 人民币
道里云	2013-7-1	A 轮	道里云信息技术(北京)有限公司	2011 年 7 月	中路集团	500 万 人民币
点触验证码	2012-8-1	种子天使	杭州微触科技有限公司	2012 年 8 月	传媒梦工场	数百万 人民币

心安众旺	2014-9-21	种子天使	杭州心安众旺信息技术有限公司	2014 年 8 月	PreAngel 锺厉资本	数百万人民币
力控华康	2015-3-21	种子天使	北京力控华康科技有限公司	2009 年 11 月	绿盟科技	515 万人民币
极验验证	2014-5-12	A 轮	武汉极意网络科技有限公司	2012 年 10 月	IDG 资本	数百万美金
安司密信-安司源	2015-6-20	PreA 轮	杭州安司源科技有限公司	2014 年 6 月	未透露	1000 万人民币
青云 QingCloud	2014-1-1	B 轮	北京优帆科技有限公司	2012 年 4 月	光速安振，蓝驰创投，经纬中国	2000 万 USD
	2013-1-1	A 轮			蓝驰创投	200 万 USD
可信 CoverMe	2014-1-1	种子天使	南京卡米网络科技有限公司	2013 年 1 月	龚虹嘉	数百万人民币
安讯科技	201	B 轮	南京安讯科技有	2003 年	通鼎互联	6900 万

	5-2-15		限责任公司	10 月		人民币
青藤云	2014-8-20		北京升鑫网络科技 技有限公司	2014 年 8 月	真格基金，云天 使基金，丰厚资 本	650 万 人民币
	2015-12-28				宽带资本 CBC， 红点投资 Redpoint Ventures	6000 万 人民币
瀚思	2015.11	A 轮	北京瀚思安信科 技有限公司	2014.1	恒毓	3000 万 人民币
	2014.1	天使			光速	1200 万 人民币
有云	2015.5		上海有云信息技 术有限公司	2014.7	如山	2000 万 人民币
四叶草	2015.12	Pre-A	西安四叶草信 息技术有限公司	2012.8	如山	3000 万人民 币
安全狗	2015.3		厦门服云信息科 技有限公司	2013.6	IDG，北京华软	8000 万 人民币
东巽科技	2014.9		东巽科技（北京） 有限公司	2010.4	如山	千万级

Sobug	2015.8	Pre-A	深圳百密信安科技有 限公司	2014.5	经纬	千万级
岂安科技	2015.12	天使	上海岂安信息科 技有限公司	2015.4	经纬	千万级
	2015.6	种子				百万级
漏洞盒子		Pre-A	上海斗象信息科 技有限公司	2014	上海金融发展投 资基金，线性资 本	3000 万 人民币
微步在线		天使	北京微步在线科 技有限公司	2015.5	北极光	千万级
梆梆安全		C 轮	北京洋浦伟业科 技发展有限公司		海纳亚洲，IDG， 红点	数千万 美金
		B 轮			红点	1000 万 美金
		A 轮			IDG	
		天使			IDG	500 万 美金
娜迦科技		A 轮	北京娜迦科技信 息发展有限公司		达泰资本，伯黎 创投	数千万 人民币
		天使			触控科技	数百万 人民币



同盾科技		B 轮	杭州同盾科技有 限公司			3000 万 美金
		A 轮			宽带资本，IDG 资本，线性资本	1000 万 美金
		天使			IDG 资本，华创 资本	千万级
WebRAY	201 5.12		远江盛邦（北京） 网络安全科技股 份有限公司	2010.7	国君创投	2300 万 人民币