在网络安全防线上，人的漏洞是最难修补的。搞定操作计算机系统的人，和技术上搞定计算机系统是一样的效果。

西方国家的网络安全意识教育市场已经启动并且创造出KnowBe4这样的独角兽企业，中国的网络安全意识教育市场起步较晚，目前还处于发展的初级阶段，领军企业收入规模相差数十倍。

与防火教育一样，网络安全意识教育会是未来安全教育的标配之一，而全民网络安全意识的提升，方能筑起网络安全的“人防”工事，形成网络安全防线的闭环。

**1. 初识“社会工程学”**

2010年我刚接管360信息安全部的时候，有同事向我内推一个被信息安全部负责人雄哥面试毙掉的小黑客，雄哥的面试意见是：“渗透能力不行”。碍于同事面子我安排了一次面试，我感觉我捡到了一块宝，发了Offer。雄哥的专业判断并没错，他采用技术手段入侵网站的能力确实一般，但从他那里我第一次听说“社会工程学”这个名词，他会利用人性的弱点来拿下目标。当时已经40岁的我知道人是一种巨不靠谱的动物，人脑也是一种很不靠谱的思维工具。在网络安全的防线上，人的漏洞是最难修补的，搞定操作计算机系统的人，和技术上搞定计算机系统是一样的效果。



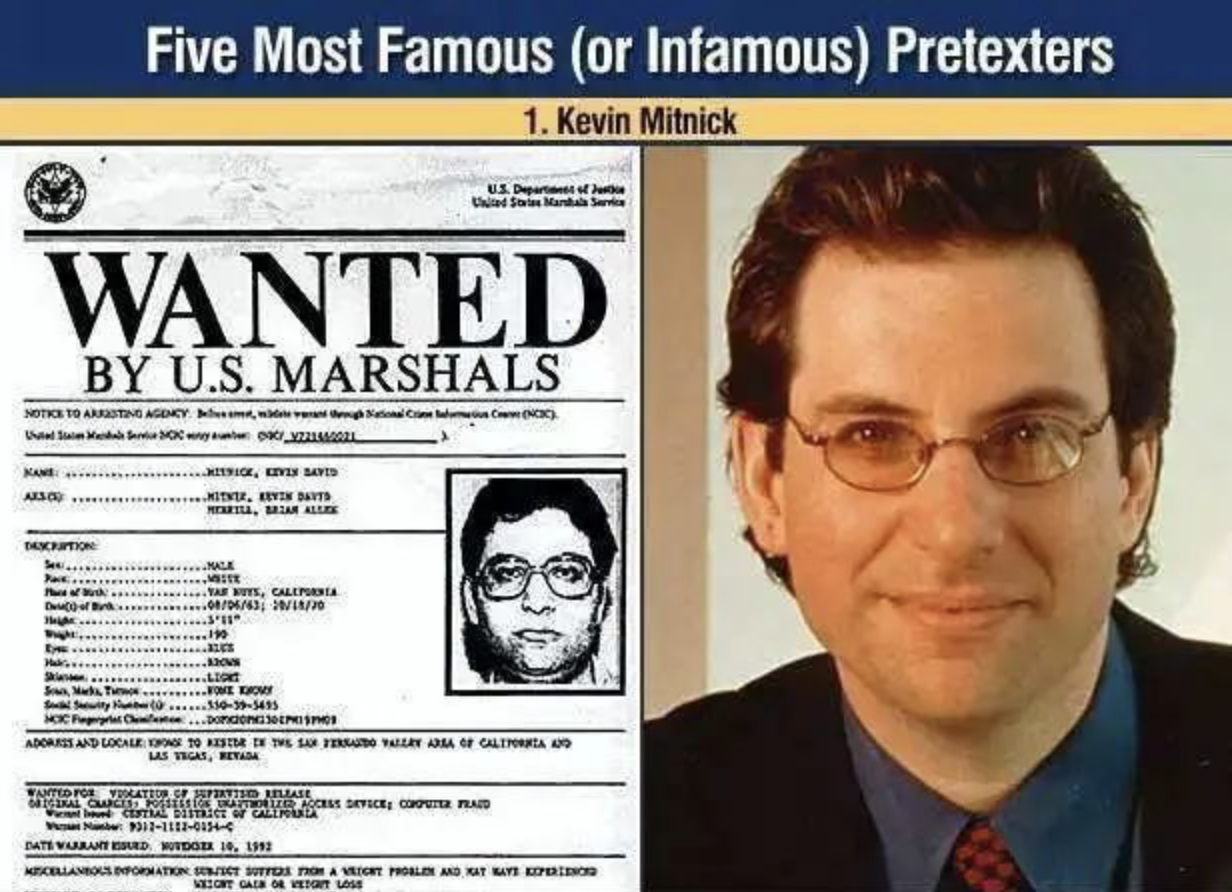
这个黑客的名字叫林伟，绰号“陆羽”，我和他一起共事了10年时间，一起完成了很多有趣的项目，比如对360的高管发动的一次社会工程学攻击，一周内攻破两位副总裁及以为高管秘书的账号，让高管们觉得“太可怕了”。高管网络安全意识的提升，使得后续8年多时间我在360所做的网络安全管理工作没有遇到来自管理层的重大阻碍。

林伟还研究过世界各国用户密码都是怎样构成的，生成一张多达10万亿条记录的密码组合表，并利用退役矿机计算出各种Hash值，形成一张巨大的彩虹表。2018年还根据窃贼的心理设计过豪宅的物理入侵的检测与防御系统。

而过去的10年间，社会工程学攻击逐渐引起网络安全界高度重视，今年RSAC2020的主题就是“Human Element”。

**2. 欺骗的艺术**

上世纪九十年代时读过一本书，讲的是包括凯文·米特尼克在内的几个美国大黑客的故事。当时就发现一个有趣的现象，这些大黑客们入侵计算机系统并不都是依靠计算机技术手段，采用欺骗手段获得用户账号往往是第一步，由于当时网络系统接入方式的限制，他们需要通过电话系统用MODEM拨号远程接入要入侵的目标计算机系统，冒充AT&T接线员骗取长途电话用户的账号就成了获得电话网络接入权限的手段，而冒充领导秘书给IT管理员打电话则是骗来高权限账号密码的主要手段。

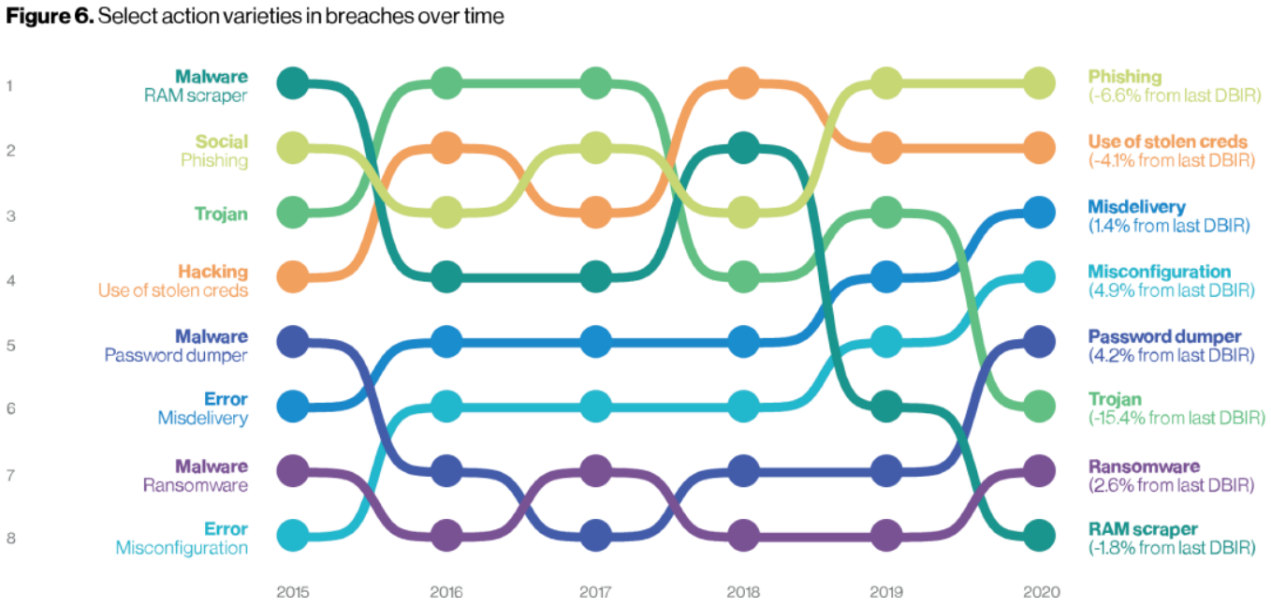


相对于暴力密码破解、软件漏洞利用这样的“硬核”网络攻击，利用人的恐惧、贪婪、懒惰等心理而发动的攻击，显然成本更低，更容易成功，也更难以防范。

凯文.米特尼克写过三本书，推荐阅读：《反欺骗的艺术》，《反入侵的艺术》，《线上幽灵》。

**3. 社会工程学攻击依然是网络安全的主要威胁**

在Verizon发布的DBIR2020中，依然把钓鱼攻击列为数据泄露的第一大威胁。



数据源：Data Breach Investigations Report 2020 by Verizon

发表于2015年的《海莲花APT报告》，是国内第一份公开发表的APT报告，360天眼实验室分析：“海莲花攻击的主要方式有“鱼叉攻击”和“水坑攻击”，前者最常见的做法是，将木马程序作为电子邮件的附件，并起上一个极具诱惑力的名称，发送给目标电脑，诱使受害者打开附件，从而感染木马。如，在2014年5月22日新疆发生了致死31人的暴力恐怖性事件之后，2014年5月28日，该黑客组织曾发送名为“新疆暴恐事件最新通报”的电子邮件及附件，引诱目标人群“中招”。该组织曾发送过的电邮名称还包括“公务员工资收入改革方案”等一系列社会高度关注的热点，令人防不胜防。



今年的新冠疫情席卷全世界，疫情也成为钓鱼攻击的题材之一，中央网信办2月7日发布《关于防范网络不法分子利用新型肺炎相关主题进行钓鱼邮件入侵的预警通报》：“近期，网络不法分子利用新型冠状病毒相关题材，冒充国家卫生健康委员会、疫情防疫等相关部门，向我国部分单位和用户投放与新型肺炎疫情相关的钓鱼邮件，钓鱼邮件附带恶意链接与包含恶意代码的office文档附件，利用仿冒页面实现对用户信息的收集，诱导用户执行恶意文档中的宏，向受害用户主机上植入木马程序，实现远程控制和信息窃取。”

这类鱼叉攻击的钓鱼邮件，从主题到内容都紧跟当今政治、经济形势或本部门工作，都是让人忍不住要点开看看，安全意识不足的工作人员很容易中招。据多家进行钓鱼攻击模拟的公司透露，在未经安全意识培训的组织中，钓鱼攻击的成功率在25%左右。

**4. 技术手段对抗社会工程学攻击效果有限**

网络安全具有攻防不对等的特性，攻击者发起100次攻击，哪怕99次失败了，只要有一次成功即大功告成，而防御者面对100次攻击，成功防住了99次攻击，有一次失误即宣告失败。而现有的技术防御手段，“漏报”是几乎无法解决的问题。

政府、企业大都部署了防垃圾邮件系统，有的甚至部署了邮件安全网关，采用利用杀软、沙箱、人工智能引擎等手段对邮件内容、邮件附件做检查。但对杀软、沙箱的绕过也有很多方法，用加壳、加花、沙箱环境检测等传统手段就有一定概率可以绕过检测，更别说还有采用0Day漏洞攻击的高成本方式，MITRE目前列出了超过60种反分析和逃逸技术。而防火墙、IPS、WSG等传统网络安全设备对于这种邮件投递、用户主动访问的内容的拦截能力更差。

并且钓鱼攻击的攻击者风险小，成本低，可以躲在安全的地方持续不断、花样翻新地对众多被攻击对象发起一波又一波鱼叉攻击，被攻击者只要百密一疏，攻击者就能得手。

**5. 提高网络安全意识，筑起网络安全“人防”工事是共识**

今年是美国“National Cybersecurity Awareness Month(NCSAM)国家网络安全意识月”的第17年，也是中国的“网络安全宣传周”的第7年，通过提升全民网络安全意识来提高网络安全能力，是国家网络安全管理机构的共识。

人类历史上在“防火”有成功的经验。曾几何时，“火”是人类历史痛苦记忆的一部分，罗马大火、东京大火、伦敦大火、哥本哈根大火、纽约大火。今天安全用火、消防培训是从学校到企业的必修课，消防检查是建筑物投用的前置审批条件，消防水龙、灭火器是必备消防物资，“防火”的意识深入每个公民的意识，是减少火灾发生、正确处置火灾的根本。

相对于“防火”，今年的新冠疫情反映出全球“防疫”上公民意识教育不足，尤其是西方国家政府和老百姓对“戴口罩”的误解甚至歧视，导致疫情在一些国家的快速爆发，虽然现在“戴口罩”已被广泛接受，但世界已付出超过60万人死亡的昂贵代价，全球经济也因为疫情备受打击。

**网络安全意识提升的意义，不仅仅是避免点击钓鱼邮件、钓鱼链接而中招，更重要的是可以依靠每个人的判断力，更早发现网络攻击，发出预警，提升全局安全防御能力，是“网聚人的力量”，形成“人人联防”的网络安全“人防工事”。**

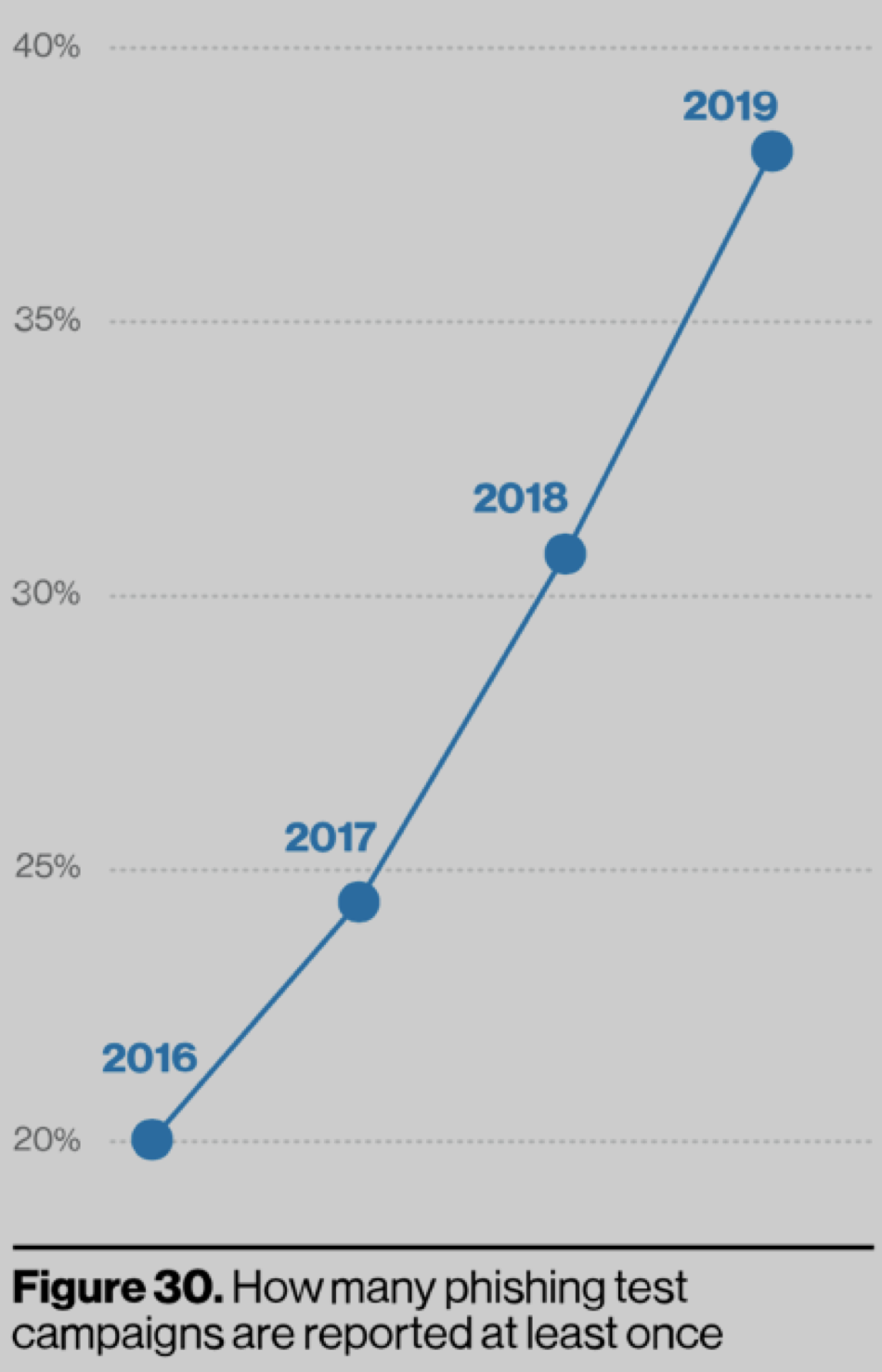
如何提升人的网络安全意识？这也是我当年遇到过的一个问题。哪怕是在一家安全公司，依然有大量的员工不是从事网络安全工作的，他们依然会犯一些低级的错误，比如连接免费的Wifi热点。于是信息安全部的同事在公司大堂与餐厅搞了钓鱼Wifi热点，并在餐厅的电视机上搞了一个“绵羊墙”，连接了钓鱼Wifi的同事的网络访问信息在经过脱密处理后会显示在绵羊墙上。

海报是进行网络安全意识宣传的好方法，360的信息安全部就曾经制作出“杜懵懵”系列网络安全意识教育漫画。设计出“杜懵懵”这个初入职场，不懂网络安全的小姑娘的卡通形象，通过她的一系列囧事儿，寓教于乐中让员工们掌握网络安全知识。

企业自己对员工发动钓鱼攻击也是非常有效的提升员工网络安全意识的方法，根据国内外网络安全意识教育厂商提供的数据，刚开始进行邮件钓鱼测试的时候，钓鱼邮件的点击率平均在25%以上，经过几轮的钓鱼测试后，一般可以降到5%以下。该领域明星厂商KnowBe4在《Phishing By Industry 2020 Benchmarking Report》中提供的数据显示，企业在实施钓鱼攻击模拟前的钓鱼邮件点击率高达37.9%，经过一轮培训之后降低到14.1%，经过一年持续教育后，降低到4.7%。

**6. 世界网络安全意识培训市场情况**

网络安全意识培训是网络安全细分市场中增长速度最快的细分领域之一，在2018年增长了约25％，Gartner预计到2019年增长将迅速加速至47％，并在2023年之前继续保持42％的复合年增长率。我没有找到2019年行业的统计数据，但在RSAC 2020上确实能看到更多的从事网络安全意识培训的公司参展。



数据源：Data Breach Investigations Report 2020 by Verizon

上图是DBIR2020中所统计的，从2016年开始，每年至少进行了一次钓鱼测试的公司的百分比，可以看到2016年进行钓鱼测试的组织只有20%，而在2019年，进行钓鱼测试的组织已经接近40%，这说明西方客户已经普遍认同网络安全意识教育的价值，并开始采取行动。

网络安全意识教育领域的玩家还有：ProofPoint，Infosec，MediaPro，Terranova，Inspired eLearning，SANS，Global Learning Systems，Security Innovation，JungleMap，Barracuda，Phishlabs，Meta Compliance，IronScales，Hutsix，SAC，RangeForce，Elevate Security，Secure Mentem，Habitu8。从业务渊源来看，有做培训/网络安全培训业务的公司开拓了网络安全意识培训业务；也有传统做邮件安全业务的开辟了钓鱼模拟的新业务，再进入这个领域；还有Elevate Security这样的初创公司。

据Momentum Cyber的资料显示，2018年网络安全意识培训领域的融资有10个，融资额3,940万美金，2019年有12个，融资额达4.36亿美金。2018年有6笔收购和兼并，其中最著名的是2007年成立的PhishMe被私募股权集团BlackRock以4亿美金估值收购并改名叫Cofense，2019年收入5,000万美金。

但最值得关注的还是KnowBe4，它是网络安全意识教育企业中的明星，由凯文·米特尼克出任Chief Hacking Officer。



2019年6月，2010年建立、打凯文·米特尼克安全意识培训品牌的KnowBe4获得KKR领投的3亿美元的投资，公司估值达到10亿美金，成为网络安全的独角兽公司。在此之前，Knowbe4已经完2017年由高盛（GoldmanSachs）成长型股票基金领投的3,000万美元B轮融资，2018年收购南非公司PopcornTraining，2019年收购巴西公司ElPescador和挪威公司CLTRe。从Business Observer今年年初的一篇报道看到，KnowBe4在2017年的收入是6200万美金，2018年达到1.2亿美金，2020年一季度销售收入比去年同期增长40%，员工达到884人。

KnowBe4的主要业务是网络安全意识培训服务，有凯文·米特尼克安全意识培训与KnowBe4安全意识培训两项主打产品，除此之外还有PhishER钓鱼邮件SOAR平台以及KMC治理、风险、合规平台。

安全意识培训的流程是先做基线测试，然后对员工进行安全意识培训，再实施钓鱼攻击测试，最后出分析报告。其中安全意识培训库有1,000多种安全意识培训内容，包括互动模块，视频，游戏，海报和新闻通讯，根据购买服务级别的不同，用户会看到不同级别的内容。

KnowBe4的服务采用SaaS模式，按人、按服务等级、按年收费，不同的服务等级所能访问的培训内容不同。在25-50名员工情况下，银牌服务17美元/人/年，金牌服务20.75美元/人 /年，白金服务24.50美元/人/年，钻石服务29.50美元/人/年，随着购买用户数的增多，价格随之降低，3,000用户以上的时候每个用户的单价基本降到了以上价格的一半，5,000用户以上的大客户可以直接商谈价格了，一次签署3年以上的合同可以获得特殊折扣。

**7. 中国网络安全意识教育市场**

西方国家的网络安全意识教育市场已经启动并且创造出KnowBe4这样的独角兽企业，中国的网络安全意识教育市场起步较晚，目前还处于发展的初级阶段。

习近平对2019年国家网络安全宣传周作出重要指示强调，“举办网络安全宣传周、提升全民网络安全意识和技能，是国家网络安全工作的重要内容。”《网络安全法》第六条中有提到：“采取措施提高全社会的网络安全意识和水平”，第十九条中说：“各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作”。但落地情况依然不好，只有极少数用户有网络安全意识培训的预算。

上海易念科技、北京红山瑞达是国内两家专门从事网络安全意识培训的公司，除此之外永信至诚、谷安天下也在这个方向有所尝试。

上海易念科技的创始人王怀宾是网络安全行业的老兵，做过网络安全咨询，是本土的安全咨询公司上海安言的联合创始人。2012年创办易念科技，2018年起，公司通过云SaaS模式来开展网络安全教育，自主研发的体验式网络安全意识在线教育平台已累计服务100+政企客户、30万+企业员工。该平台由移动网校、钓鱼仿真、学习系统、学习商城、竞赛平台与工具箱等模块构成，可单独或组合使用，满足不同场景的教育需求。

红山瑞达则是由几位自主择业的军人创办，从保密意识教育做到网络安全意识教育、钓鱼仿真。红山瑞达的产品线包括保密意识教育系列产品、网络安全意识教育系列产品、网络安全意识测评产品、网络安全钓鱼训练系统。

我分别看过两家公司的产品，感觉在培训类产品上，和KnowBe4、Terranova在培训内容的在制作质量、互动性上还有较大差距，员工培训方面内容为王，内容质量直接关系到用户的留存度和培训的效果；在钓鱼模拟上，钓鱼测试效果会较高程度依赖于钓鱼邮件模板的设计，没有试用过国外的产品，不好评价。

易念科技与红山瑞达2019年的营业收入都在千万左右，与KnowBe4相差数十倍。

**8. 中美网络安全教育市场规模差异巨大的原因**

首先是网络安全事故处罚力度不同。美国的企业出现数据泄露问题可能会遭到用户的集体诉讼，可能支付巨额赔款或缴纳巨额罚金：在2019年，英国航空公司遭受了创纪录的2.3亿美元罚款，紧随其后的是对万豪集团的1.24亿美元罚款，Equifax为2017年的数据泄露支付至少5.75亿美金罚款。重罚之下企业会平衡网络安全建设，包括网络安全意识培训的投入与不做这些事情所冒的风险，会有动力寻找更有效的防御手段，员工安全意识这块短板很容易被找到，用每个员工不到20美金的代价修补这块短板具备经济性。

国内已颁布的《网络安全法》以及正在征求意见的《数据安全法》虽然都有罚则，但都处于“棒子高高举起，但轻轻落下”的状态。虽然明确了网络安全事故的第一责任人，但在处罚不是很重的情况下，机构首先追求的是合规，当网络安全意识教育还没有纳入合规性检查范畴的时候，对员工普遍进行网络安全意识教育这件事，还没有提升大多数企业领导人的议程上来。没有领导人的重视就没有预算，没有预算信息安全部门就难以采购网络安全意识教育产品或服务。

其次是责任的错位，国内员工培训的预算在人力资源部或办公室，但网络安全的职责在信息安全部或IT部门，负责安全的人没有安全培训的预算，有培训预算的人不对网络安全负责。而国内的网络安全意识教育企业甚至没有意识到这种预算分配与责任的错位，或者缺乏与人力资源部门接洽的渠道，导致无法达成销售，或即使达成销售，但客单价上不去。

再次，还是产品质量需要提高，从国外公司提供的参考数据看，培训的形式、内容的差异，会造成受训对象留存率在25%和75%之间的波动，国内厂家的培训内容还是“上课”、“答题”的形式为主，提供更强互动性、游戏化的内容、组队答题等带更多社交属性的培训形式、设计短时间、高频度的培训，都是值得尝试的方向。

**9. 中国网络安全意识教育市场展望**

中国的网络安全意识教育市场，会是一个慢牛市场。

网络安全意识教育，属于重要但不紧急的事务。在网络安全方面法律法规不断出台、政府和企业忙于合规的时候，如果网络安全意识教育还没有纳入合规性要求，那么其优先级就会被放低。但习总书记发言中，网络安全法中对网络安全意识教育都有明确提及，在合规性检查中涉及网络安全意识教育只是时间问题，该来的终归会来。

网络安全的预算方式也是市场启动慢的原因之一。对一个组织来讲，网络安全意识教育的资金成本并不是很高，以5,000人的组织为例，按照100元人民币/人/年的成本，每年安全意识教育需要50万人民币。但如果没有安全事故等特殊事件的推动，这笔开支进入年度预算也需要时间。从安全负责人认识到安全意识教育的重要性、了解供应商解决方案情况，到做预算、说服主管领导、将网络安全意识教育经费纳入下一年度预算、次年预算的执行，也会要有一年甚至更长的时间。进入年度预算的好处是，今后每年都会有网络安全意识教育的预算，市场容易实现稳定增长。

近期，有网络安全的“国家队”开始关注网络安全意识教育市场，他们的介入，会加速网络安全教育在政府部门、国企的实施，客观上也会加速这个市场的成熟。

从长期来看，随着新基建、5G、工业互联网、物联网的建设，传统产业的数字化转型，网络安全是所有人都最终无法回避的一个问题，而网络安全“三分技术，七分管理”的现实会存在相当长时间，“人”这块网络安全防线中的短板，一定需要得到弥补，网络安全意识教育是必不可少的手段。即使每年只有1,000万人付费接受网络安全意识教育，那也是10亿级的市场。

网络安全产业应当主动去推动网络安全意识教育牛市的到来，包括：

* 向政府主管机构宣传网络安全意识教育的重要性，推动政府将网络安全意识教育纳入合规性范畴；
* 产品创新。目前国内的安全意识教育产品形态和内容还是处于跟随状态，存在教育内容呆板、互动性差、个性化差的问题，这会很大程度上影响安全意识教育效果。需要提高网络安全意识教育的互动性，使培训内容更喜闻乐见，提高培训的客户留存率，切实提高培训效果；
* 与传统教育培训机构合作，利用这些机构的销售通路与项目实施能力，扩大销售；
* 尝试与其它网络安全公司的产品和服务打包销售；
* 利用或创造事件营销机会。

与防火教育一样，网络安全意识教育会是未来安全教育的标配之一，而全民网络安全意识的提升，方能筑起网络安全的“人防”工事，形成网络安全防线的闭环。

作者：谭晓生

转载自：互联网安全内参

链接：http://toutiao.secjia.com/cyber-security-awareness-0724/