简译版

通过纵向学习减少危险的用户行为

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Use longitudinal learning to reduce risky user behavior		
原文作者	塞·文卡塔拉曼（Sai Venkataraman）	**原文发布日期**	2021 年 5 月 4 日
作者简介	塞·文卡塔拉曼是 SecurityAdvisor 公司的首席执行官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/05/04/longitudinal-learning/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	数十年来，尽管企业一直在开展长期、全方位的安全培训，但是几乎每天都会发生数据泄露事件。HR 和安全领导者应将网络威胁最关键的防御措施“人”置于首要位置，并据此创建网络安全文化。企业必须致力于改变用户的行为，以改善其安全状况。为实现这一点，企业可以使用情境化的纵向学习方法，不断地对用户进行安全培训。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

通过纵向学习减少危险的用户行为

塞·文卡塔拉曼

2021 年 5 月 4 日

人们通常会忽略与他们无关的信息，这就是 IT 和 HR 部门多年来一直无法正确地接受安全培训的原因。数十年来，尽管企业一直在开展长期、全方位的安全培训，但是几乎每天都会发生数据泄露事件。

HR 和安全领导者应将网络威胁最关键的防御措施——“人”——置于首要位置，并据此创建网络安全文化。企业必须致力于改变用户的行为，以改善其安全状况。

为实现这一点，企业可以使用情境化的纵向学习方法，不断地对用户进行安全培训。

安全到底是谁的责任？

从历史上看，“安全”一直被企业视为技术或 IT 团队的责任。而实际上，安全是整个企业的共同责任。

我们知道，在增强企业安全方面，最需要关注的是人为错误。这导致了旧观念的转变，企业领导者已经知道，保护企业的安全并不是某一个团队的责任。现在，企业通过开展有效且可衡量的安全培训，让员工承担更多的安全责任。

但是，如果员工不具备相关的知识和资源，就无法了解安全风险，让他们承担这种责任就是不现实的。如果员工能够接收到有关其行为的反馈意见，并直接应用这些意见，就能更好地理解和接受这种责任。

纵向学习可以防止认知偏见

纵向学习是一种在学术界尤其是公司培训中，越来越受欢迎的教学方法。在这种教学方法中，随着时间的推移，培训者会重复性地对特定内容进行简短评估（例如员工是否会点击由未知用户发送的电子邮件中嵌入的 URL）。

通过不断的评估，可以增强员工的安全概念和信息，帮助其逐步保留和积累安全知识。医疗行业的纵向学习研究表明，对医学生进行测试并给出解释，是驱动其长期记住信息的最有效方法。

一致、重复的课程，对于帮助员工克服认知偏见（网络犯罪分子正是利用这种偏见执行攻击的）至关重要。人的大脑容量是有限的的，也就是说，大脑每天要处理大量信息，因此会不断尝试采用捷径来节省能量并启用多任务处理。

网络罪犯分子知道这一点，并利用这一点执行有效的模拟攻击、网络钓鱼和恶意 URL 攻击。你发现最后一句中有错字了吗？如果没发现，请再次查看“rnalicious”（正确写法是 malicious）一词。如果读得太快，会将连在一起的小写“r”和小写“n”看成“m”。这种简单的伎俩每天都会在公司网络上发生数百次，这让安全领导者辗转反侧难以入眠。

人类对情境化学习的反应最佳，情境学习已在教育行业中实施多年，旨在帮助学生记住学习内容（尤其是注意力持续时间较短的学生）。纵向学习不再采用长时间的学习课程，转而采用授课时间更为规律的微课程。例如，上 10 节课，每节课听 5 分钟的播客，而非开展时长为 1 小时的 1 节课。

考虑到知识型员工经常要执行各种项目、应用程序以及其他任务，纵向学习能够提供一种将安全意识培训转变为个性化教学的方法，以配合员工的繁忙日程。

个性化和相关性

安全意识培训需要像 GPS 一样：指导用户走正确的路，并防止他们偏离航向。它需要实时适应用户的行为，进行纠正，并根据用户的需求逐步发展。

当人们收到针对其特定行为的直接反馈时，他们往往会很惊喜，这有助于他们吸收信息以备将来使用。随着时间的推移，这种情况会不断发生，并且会有轻微的变化，这有助于员工形成积极的行为模式。

纵向学习是分层网络安全策略的重要组成部分。企业应对这种学习方法持乐观态度，不要贬低，以免产生相反的效果。个性化的纵向方法能够配合员工的时间，允许他们以更有效、可扩展的方式吸收信息。这样一来，企业就可以创建一种强大的、可衡量的网络安全文化。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com