

简译版

创建网络安全文化的八种方法

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	8 Tips for Creating a Cybersecurity Culture		
原文作者	帕姆·贝克 (Pam Baker)	原文发布日期	2021 年 11 月 19 日
作者简介	帕姆·贝克是一位专栏作家。		
原文发布单位	Information Week		
原文出处	https://www.informationweek.com/it-life/8-tips-for-creating-a-cybersecurity-culture		
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	IT 和业务领导者应如何帮助企业建立强健的网络安全文化，帮助全体员工形成网络安全意识呢？本文介绍了实现这一目标的八种方法：（1）向员工解释网络安全的重要性；（2）员工提供安全的工作方式；（3）消除 IT 和安全团队之间的矛盾；（4）对员工进行鼓励而非威胁；（5）量身定制网络安全意识培训课程；（6）使网络安全项目“竞技化”；（7）高管参与；（8）让员工知道他们的努力大有裨益。		
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。		

创建网络安全文化的八种方法

帕姆·贝 克

2021 年 11 月 19 日

网络安全是企业全体员工的责任。但是，员工往往专注于完成工作，而忽略了这一简单的事实。“在最后期限前完成工作”或“按时下班”是员工规避安全协议的常见诱因。即使是最勤奋和敬业的员工也常常会因为分心而发现不了电子邮件中的诈骗迹象。

上述问题是不会消失的，那么 IT 和业务领导者应如何帮助企业建立强健的网络安全文化，帮助全体员工形成网络安全意识呢？以下是实现这一目标的八种方法。

1. 向员工解释网络安全的重要性

领导者不应简单地发布命令，而应向员工解释“为什么要求他们这样做”。这样不仅有助于员工记住网络安全要求，还能帮助他们建立网络安全知识库，以便他们在今后的更多威胁场景中做出更好的判断。

Defendify 联合创始人罗布·西莫普洛斯 (Rob Simopoulos) 指出：“领导者应通过真实案例来解释网络安全控制措施的重要性。”

2. 为员工提供安全的工作方式

“企业应为员工提供安全的工作方式，包括安全文件交换、安全浏览、安全打开附件等。”安全咨询公司 NCC Group 的总监兼高级顾问蒂姆·罗林斯 (Tim Rawlins) 指出，“这样一来，员工更容易遵守企业的网络安全要求。”

大多数员工都有若干待办事项，这会造成他们的大脑容量过载。如果企业希望员工有足够的警惕性来识别狡猾的网络钓鱼邮件，就应该减少让员工分散注意力的事项，以释放他们的头脑空间。

3. 消除 IT 和安全团队之间的矛盾

不存在“健康矛盾”这样的东西，任何形式的矛盾都会侵蚀企业建立网络安全文化的努力。

Zscaler 客户体验与转型执行副总裁卡维莎·玛丽亚潘 (Kavitha Mariappan) 表示：“对于许多企业而言，这两个团队之间存在竞争性的推拉关系。这会导致基础设施和硬件老旧，很容易受到网络攻击。更糟糕的是，这种关系会加剧‘厌恶变革’的企业文化，为企业创建网络安全文化带来障碍。”

4. 对员工进行鼓励而非威胁

消极强化可能会弄巧成拙，因为员工更有可能规避或掩盖安全问题以避免受到惩罚。企业应注意，员工可能会将网络安全培训也视为惩罚性的。企业应通过积极强化来鼓励员工做正确的事情，包括上报问题和事件等。

“企业应使用与员工相关的术语和概念来解释网络安全”，AwareGO 联合创始人兼研发主管拉格纳·西古尔兹松 (Ragnar Sigurðsson) 指出，“让员工了解攻击事件会如何影响到他们自身，但不要用‘你不应该’这样的语言来责备员工。”

5. 量身定制网络安全意识培训课程

网络安全培训是很好的第一步。要想通过培训改变员工的行为，一定要实施行为科学技术，为员工量身定制培训计划以获得最佳效果。

“企业通常未使用与员工日常生活相关的术语来解释网络安全需求，这导致员工认为网络安全是超出其工作范围的技术。”西古尔兹松说。

Accenture 安全增长与战略负责人尼哈·乔希 (Neha Joshi) 表示：“企业不应开展‘一刀切’的安全意识培训，而是要针对存在的安全问题定制培训，以帮助员工改变自身行为。”

“建立网络安全文化必须从高层和基层同时着手，高层应做好榜样，努力建立安全信念以轻松实施变革。”

6. 使网络安全项目“竞技化”

网络安全工作不仅是全体员工的职责，也是一项竞技运动。“竞技化”是一种经过验证的技术，可以让人们保持参与意识。企业也可以使用该技术来建立和加强网络安全文化。

Balbix 创始人兼首席执行官高拉夫·班加 (Gaurav Banga) 表示：“安全领导者可以跟踪和验证任务的完成情况，并统计员工得分等荣誉。分数可以发布在排行榜上，以激励员工进

一步开展竞争。公司甚至可以考虑每月、每季度或每年对表现最好的员工进行奖励。”

“如果有机会赢得一次免费夏威夷之旅，哪个员工不想参与改善公司的网络安全状况呢？”

7. 高管参与

高管级别的支持至关重要，因此，管理层必须树立榜样。

Sungard Availability Services 安全监管高级总监米奇·卡瓦爾斯基(Mitch Kavalsky)指出：“管理人员参与 ISO 27001 等认证能够给员工树立榜样，鼓励他们都参与进来。”

IronNet 首席信息安全官乔治·拉蒙特 (George Lamont) 上校 (已退役) 表示，在领导参与、员工参与和同事参与的基础上，企业方能建立一支全公司范围的安全部队。

“要想使这种 ‘参与三重奏’ 有效”，他说，“员工需要看到全体高管的参与，还需要为全体员工提供一致的沟通渠道和透明度。”

8. 让员工知道他们的努力大有裨益

仅仅开展培训是无法保护企业的，最重要的是员工要真得关心。

CSI 首席信息安全官史蒂夫·桑德斯 (Steve Sanders) 表示：“如今，关于网络安全事件和公司未能保护数据的新闻层出不穷，以至于员工已经疲乏，他们要么觉得这无关紧要，要么觉得无能为力。企业内部安全意识计划需要简洁、有意义和可操作，让员工知道他们正在发挥作用。”

“企业应围绕各种网络安全主题进行定期沟通，但不要次数太多以免员工疲乏。每隔一两个月进行一次沟通就很好，能够提醒全体员工 ‘网络安全如何保护公司及其客户的利益’。”卡瓦爾斯基补充道。

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>