简译版

员工重返办公室时重建企业安全文化

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	Rebuilding your security culture as employees return to the office		
原文作者	克里萨·弗里曼（Chrysa Freeman）	**原文发布日期**	2021 年 7 月 14 日
作者简介	克里萨·弗里曼是 Code42 公司安全意识和策略高级项目经理。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/07/14/office-security-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	在员工返回办公室办公时，企业会面临各种安全风险。但是，通过创建积极正面的安全文化，鼓励员工将习得的知识付诸实践，企业可以增强其安全态势。对员工开展“内部人员风险管理最佳实践”的培训，并建立积极正面的安全文化，有助于员工在保护企业方面产生归属感。		
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。		

员工重返办公室时重建企业安全文化

克里萨·弗里曼

2021 年 7 月 14 日

在员工远程工作的情况下，企业内部人员风险管理计划中的一些举措无法实施。在员工重返办公室办公的情况下，安全团队可以重新关注这些问题了。这是企业重建更强大的安全文化的好机会。

为成功奠定基础

无论员工在公司工作了七年还是七个月，当他们重返办公室办公时，都应该被视为在公司的第一天。所有员工，无论有多资深，都应该温习企业的安全实践。

企业安全团队可以教导或提醒员工，如何在适当的环境中正确管理和移动数据，以最大限度地减少数据泄露风险。这能够促进健康的安全实践，并为所有员工提供定期和定制的培训。

如果企业正在转向混合办公方法，则应确保员工具备“双办公室办公”所需的正确知识和/或设备，以最大程度地减少数据丢失。例如，鼓励员工使用公司硬盘从两个办公室访问数据，而不是通过个人 U 盘移动数据。

营造积极正面的安全文化

员工需要移动数据来完成工作。一般来说，安全团队会对数据泄露告警做出负面的响应。然而，Code42 公司的研究表明，大多数数据泄漏事件都是在无意中发生的。举例来说，员工将个人硬盘连接到工作设备时，无意中将工作文件同步到了他们的个人云中，导致数据被泄露。如果发生这种情况，安全团队不应急于得出“员工是在窃取数据”的结论，而应进行调查以了解更多信息。

通常，员工只是想完成工作，或与同事/伙伴合作。安全团队可以利用这些机会，教育他们以更安全的方式共享数据。安全团队应始终以积极正面的心态与员工进行对话。例如，他们可以对员工说：“我们注意到这一点……你发现了吗”，而非用指责的语气与员工进行对话。这样一来，安全团队可以将员工定位为安全盟友而非安全敌人，更好地鼓励员工与其

合作。

寻找新的网络安全交流方式

安全团队应向全体员工强调安全的重要性。在员工返回企业办公时，企业就应该实施内部人员风险管理计划。所以，安全团队应将安全对话作为公司入职实践的一部分——即使只谈论几分钟也好。通过这些措施，企业可以设定适当的基调，让员工知道安全团队并不是在“发号施令”，让员工知道企业需要他们的帮助来保护公司资产。

为了使安全信息尽可能有效，安全团队应对其进行定制，以满足员工的需求和实际情况。即，安全团队要了解信息的受众，以及哪些信息和信息交付方式最能引起他们的共鸣。安全团队可以重复性地推送信息，以此来保持员工的参与度。如果安全团队不能在员工体验中的多个点进行安全对话，就不能指望员工知道如何应对现实生活中的安全风险。

员工和企业之间双向透明

安全团队应与员工之间建立信任，并鼓励他们轻松地与其谈论在线行为。安全团队应记住，员工只是想把工作做好而已。

员工和企业之间实现透明大有帮助。在 Code42，我们要求员工尽可能对自己的行为保持透明，而员工也希望我们的安全团队也能做到这一点。例如，在员工离开公司之前，如果他们将照片等个人文件从工作计算机转移到个人文件，他们通常会提醒我们。

最后，主动的行为对安全团队很有帮助，因为它能够缩短潜在的调查时间，使安全团队有机会推荐更安全的传输方法，例如加密硬盘等。

在员工返回办公室办公时，企业会面临各种安全风险。但是，通过创建积极正面的安全文化，鼓励员工将习得的知识付诸实践，企业可以增强其安全态势。

对员工开展“内部人员风险管理最佳实践”的培训，并建立积极正面的安全文化，有助于员工在保护企业方面产生归属感。

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