简译版

如何设立有效的 CISO

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	How to build a better CISO		
原文作者	Allan Alford	原文发布日期	2019 年 1 月 15 日
作者简介	Allan Alford 是 Mitel 公司的首席信息安全官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/01/15/better-ciso/		
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		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

如何设立有效的 CISO

Allan Alford

2019 年 1 月 15 日

长期以来，科技行业因其“日新月异”的发展为人津津乐道。遥想 20 年前，“互联网”还只是吸引消费者的噱头，而现在，几乎所有的家用设备都支持 Wi-Fi。当然，新兴技术的迅速普及也改变了其他 IT 市场 如安全市场。这种改变导致 IT 行业的现有角色发生了变化，而且还出现了新的角色，例如“首席信息安全官”（CISO）。

CISO 是一个人气不断飙升的职位，现在已成为所有企业的重要组成部分。尚未聘请 CISO 的公司需要接受这一职位——如果不想被罚款，某些州的公司需要迅速采取行动。随着威胁变得越来越精密、世界变得越来越互联，公司对 CISO 的需求不可否认。

即使公司所在的州不强制要求公司设立 CISO，但如果公司未设立 CISO，潜在客户会觉得公司不重视他们的安全性。随着安全威胁不断增加，对公司业务造成严重影响，公司需要弄清楚：成为一名有效的 CISO 需要哪些条件？

了解风险

CISO 全面负责安全可见性 ,他们必须全面了解信息安全风险对公司上线和底线的影响。CISO 需要在公司的多个方面具有实践经验，以构建完整的安全视图、了解安全风险，并用业务术语进行调整。这包括 IT 运营等技术部门的经验、安全运营和风险管理背景，以及直接参与业务的领导角色等。

有抱负的 CISO 必须接触或经历公司的所有内容，以充分了解其业务范围。然后，他们必须清楚地了解安全和风险如何影响公司的成功。

业务与 IT 的交叉

最终，CISO 必须能够将安全风险转化为整个管理团队可以理解的业务术语。管理团队是最容易被攻击的目标。如果能让他们理解安全风险，就能较快地采用安全标准，不至于让企业遭遇其他安全漏洞。

尽管 CISO 需要从技术方面理解安全性，但是该工作并非都是技术性的。CISO 也是管

理团队的成员，因此他们必须牢牢掌握如何领导和激励团队。此外，他们还必须向管理团队的其他成员提供安全和 IT 团队建议，以确保完全支持公司的安全策略。

我们以几年前臭名昭著的“心脏出血”（Heartbleed）零日漏洞为例。董事会不想听到“OpenSSL 库遭受缓冲区过度读取攻击”；他们关心的是，受 Heartbleed 的影响，即将进行的合并或收购的敏感文件是否会被泄露。

董事会关心的是攻击对公司底线的影响，而技术细节的意义在于更好地解释业务问题。换句话说，业务问题是最重要的，技术细节是对业务问题的补充。

当然，多年来，许多公司已经从战略上（或出于必要性）接受了网络安全。许多经验丰富的专家——不过他们很难请到——和大量能够胜任该职位的人士，需要机会来发展他们的业务和管理技能。

安全世界的发展并没有放缓，公司的业务也没有放缓。在 CISO 的短缺问题上，公司最好能够领先解决，确保以合适的价格聘请合适的 CISO。如果不这样做，公司就会把自己置于高攻击风险之中。

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，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、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有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

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厂商、IT 厂商选择安天作为检测能力合作伙伴 ,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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，为捍卫国家主权、安全和发展利益提供了有力支撑。

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的发言代表，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*