简译版

管理数字风险之四步走

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	Four Steps to Begin Better Managing Your Digital Risk		
原文作者	Alastair Paterson	**原文发布日期**	2019 年 3 月 7 日
作者简介	Alastair Paterson 是 Digital Shadows 公司首席执行官兼联合创始人。		
原文发布单位	Security Week		
原文出处	https://www.securityweek.com/four-steps-begin-better-managing-your-digital-risk		
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。		

管理数字风险之四步走

Alastair Paterson

2019 年 3 月 7 日

网络威胁情报（CTI）为企业提供了了解各种攻击者行为的宝贵信息。有了 CTI，公司就可以了解攻击者的策略和技术，并利用这些信息来制定防御策略，降低数字风险。但是，要使这些策略真正有效，企业必须考虑有效评估和管理企业风险的方法、需要保护的资产、联网系统的漏洞，以及攻击者可能利用的漏洞等问题。

通过监控暴露的资产并评估威胁，企业可以更好地了解需要保护的内容。接下来，我们将介绍管理数字风险的四个步骤。

第 1 步：确定要保护的关键资产

首先，企业需要评估拟保护的关键资产，以及这些资产对攻击者的吸引力。这些资产通常包括“人”（例如客户、员工、合作伙伴、服务提供商）、组织（例如服务部门、公共基础设施部门），以及支持上述“人”和组织的系统和关键应用（例如网站、门户、数据库、支付处理系统、企业资源规划[ERP]应用等）。

之后，考虑这些资产与企业重要业务和经济功能（可以产生利润，提供竞争优势或无形财产[如信任、声誉和商誉等]）的关系。知识产权（产品设计、专有代码和专利信息）的泄露往往会影响企业的竞争优势，客户数据的泄露会导致企业违反隐私法规。员工凭证、私人 RSA 密钥或安全评估报告等都有可能落入攻击者手中，使他们得以窥探企业。

确定了关键资产之后，企业还需要了解哪些攻击者最有可能攻击这些资产。

第 2 步：了解威胁

了解威胁是风险评估的关键部分，而 CTI 可以提供对这些威胁的实用见解。企业转向关注攻击者行为的策略，为防御现实世界的漏洞提供了支持。但是，了解攻击者行为只是一部分，企业还需要了解攻击者最常利用的漏洞并减少此类漏洞。

诸如 MITRE ATT&CK 之类的框架提供了一种通过战术、技术和规程（TTP）来描述攻击者行为的方法。通过将攻击者行为与威胁建模相结合，企业可以思考为何会沦为某类攻击

者的攻击目标、攻击者希望得到什么，以及攻击者的目的是什么。通过了解攻击者 TTP，防止可能使攻击者受益的数据泄露事件，企业可以大大降低风险。

第 3 步：监控暴露的资产

监控在开放网络、深网和暗网中暴露的资产是一项艰巨的任务。就网络安全公司 Digital Shadows 服务的中型企业而言，暴露的资产平均包括 290 个假冒域或社交媒体帐户、180 个证书问题、84 个可利用的漏洞、360 个开放端口和 100 个业务文件。很多工具可以对此提供帮助：DNS Twist 通过对公司域的排列组合，为企业提供钓鱼网站全览；Have I Been Pwned 可以检测已泄露的用户名和密码；Google Hacking Database 可以检测已泄露的敏感文档。企业还可以利用营销和品牌管理团队使用的服务来监控社交媒体，以便了解公众对某个组织的看法。

第 4 步：缓解策略

检测暴露的资产和了解威胁的确很重要，但是采取行动来解决和降低风险更加重要。企业的缓解策略包括：即时的战术响应；持续进行的业务响应；涉及投资或定向影响的战略响应。例如，如果企业发现大量凭证遭泄露，可以考虑实施多因子身份验证（MFA）。同样，如果发现员工在家用计算机上备份工作内容，则可以向公司提供更有效的存储解决方案。

虽然没有任何一种解决方案或方法可以完全消除数字风险，但是通过了解哪些资产已经暴露、这些资产对攻击者的价值，以及攻击者如何获取这些资产，企业可以制定更好的防御决策，并不断对其进行改进。

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*