企业的网络安全态度：平衡网络风险和业务加速

简译版

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	Enterprise attitudes to cybersecurity - Strategies to balance risk and business acceleration		
原文作者	Help Net Security	原文发布日期	2019 年 3 月 4 日
作者简介			
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/03/04/enterprise-attitudes-to-cybersecurity/		
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。		

企业的网络安全态度：平衡网络风险和业务加速

Help Net Security

2019 年 3 月 4 日

IT 决策者正面临着一系列重大挑战，包括：不断进化的攻击者、重要的立法和法规要求、业务数字化转型需求以及快速增加的技术解决方案等。

理想情况下，企业主要根据其业务需求确定网络安全策略。但是，根据安全公司 Optiv Security 的一份新研究报告，近三分之二的英国 IT 和安全决策者表示，由于不断变化的立法、威胁和其他外部因素，其安全计划一直是响应式的（reactive）。

不断变化的技术对企业的网络安全策略产生了重大的影响——79%的企业认为移动应用的激增对他们产生了重大影响；77%的企业认为迁移到云端会给他们带来重大影响。

“只关注外部威胁的安全团队正在被业务和数字化变革抛在后面，”Optiv 公司欧洲总经理兼执行副总裁西蒙.丘奇（Simon Church）表示。“我们看到，网络领军者正在转向‘业务优先’的观点，试图在抵御网络风险与维持企业业务之间取得平衡。然而，许多企业仍然采用老式的“外入模型”（outside-in model），即：基于最新的趋势和漏洞采购安全技术，以响应威胁并解决安全问题。这种方法根据威胁态势（而非企业目标）来确定安全基础设施和运营，且经常忽略成功的安全计划的其他重要元素——人员和流程。”

该研究还发现，企业的采购也面临着挑战。近五分之三的 IT 领导者认为，为他们的安全计划采购产品或技术是非常困难的，主要原因是董事会缺乏对这些问题的理解。

近三分之一的企业认为，“董事会缺乏理解”是实施其安全策略的主要障碍——只有 23%的 IT 部门认为，其他部门非常了解其安全策略。在 56%的企业中，IT 部门制定安全计划，但是需要董事会签署才能生效。此外，在近四分之一的案例中，是由董事会制定安全策略的。

“许多企业都在努力衡量和报告其网络安全投资回报率（ROI）。”丘奇说。“事实上，根据我们的研究，只有三分之一的 IT 部门通过实时仪表板或定期报告，向董事会呈现关键指标，向其告知安全计划是否成功。通过加强报告机制，IT 决策者可以更好地采购产品和技术，并证明其安全策略和解决方案的价值。”

该研究表明，超过四分之一的受访者认为他们的安全计划很有效。但越来越多的企业不

仅想要安全计划“有效”，还想要安全计划足够“简单”。当被问及“如果从零开始构建安全计划，企业对不同因素的重视程度”这一问题时，他们表示将把 32%的精力放在简单性上，这比当前的比例增长了 9%。

“企业面临的挑战在于，世界将继续以更快的速度变化和发展。”丘奇说，“所有人都已经意识到，随着全球化、互联网、云计算、数字化转型和移动技术的不断发展，全球经济和企业呈现指数级增长。上述技术的发展，加之现有的安全方法，构成了一个非常复杂和不景气的网络世界。我们的研究证实，安全行业需要新视角、新方法，以及新的网络安全交付和消费模型，从而实现更好的网络安全。该行业需要一种将业务策略和网络风险置于网络决策核心位置的方法。”

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*