管理网络安全成本：将相关因素纳入年度预算

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	Managing Cybersecurity Costs: Bake These Ingredients Into Your Annual Budget		
原文作者	乔治·普拉西斯（George Platsis）	**原文发布日期**	2021 年 1 月 15 日
作者简介	乔治·普拉西斯与私营、公共和非营利部门合作，以满足其战略、运营和培训需求。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/managing-cybersecurity-costs-bake-ingredients-into-your-annual-budget/		
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有方式，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。		

管理网络安全成本：将相关因素纳入年度预算

乔治·普拉西斯

2021 年 1 月 15 日

随着各行各业的发展，曾经的可支配费用逐渐演变成运营成本。例如，在许多行业中，保险几乎是一项“必须的”投资。最新的运营成本是网络安全成本，这是因为保护最重要的资产——信息——需要持续的资金投入。在规划网络安全预算时，企业应考虑到各个因素。那么，企业应将哪些因素纳入网络安全预算中，以减少整体风险呢？

如何与高管沟通网络安全成本

如果 IT 部门能够明智地分配信息安全预算，就可以将与网络相关的费用转化为竞争优势。这样一来，他们就可以获得高管的支持。因此，在规划 2021 年的预算时，IT 部门应使用决策者能够理解的语言。需要注意，这不只是比特和字节，防火墙和路由器的问题；而是一场商务演讲。他们应让高管知道，网络安全投资是值得的。

- 现金流（企业能否在经济上予以支持）
- 担保（需要抵押资产进行借款时）
- 资本（有多少资金可以使用）
- 品格（不仅包括借款人的品格，还包括担保人的品格）
- 经营环境（发展前景如何）

这就是信用和贷款的“五 C”分析。实际上，你希望管理层在网络安全培训和预算上进行投资，而他们希望获得投资回报。因此，如果你无法量化投资及其回报，就很难获得管理层的支持——在 2021 年尤其如此。

1. 漏洞评估和修复

如果企业无法自己进行漏洞评估，也无需太过焦虑。随着漏洞评估服务的日益商品化，此类网络安全成本不断降低。因此，作为买家的企业处于良好的谈判位置，可以经常（甚至以固定费率）使用此类服务。此外，即使企业可以自己进行漏洞评估，他们也可以选择使用

外部供应商，以便客观地看待自己的问题。在理想情况下，企业应每三或六个月进行一次漏洞评估；至少每年进行一次评估。

在这方面有一个难题：漏洞修复。如果企业只进行漏洞评估而没有相应的修复措施，就像成为健身房会员但不去健身一样。要想保护网络安全，企业就要修复漏洞。如果企业无法自行修复漏洞，可以与供应商合作。现在正是签订长期合同的好时机。

2. 渗透测试

商业思想家彼得·德鲁克（Peter Drucker）说："计划若未能切实执行，就只不过是纸上谈兵。"

企业应将漏洞评估视为"计划"，将渗透测试视为"执行"。渗透测试更加深入，而且其结果存在不确定性，因此企业应设置清晰的边界和规则。此外，企业应至少每年进行一次渗透测试。

许多漏洞评估供应商也提供渗透测试服务。因此，企业应从业务角度考虑网络安全成本。现在是时候与供应商协商此类服务了。

3. 将员工培训纳入网络安全成本

许多大型企业会确保，其员工每年都接受某种形式的内部信息安全培训。但是，要想防御如今的威胁，这还远远不够。随着防御技术的增强，攻击者也在不断改变攻击策略——他们再次走低技术路线，将重点放在社会工程攻击上。这意味着他们会利用企业的员工，而非代码。

如果企业想要避免企业电子邮件泄密（BEC）和勒索软件攻击，则应确保全体员工都接受定期、持续的安全培训，以帮助其识别可疑链接和诈骗电子邮件。这就像健身一样：你需要通过训练增强肌肉记忆力。这意味着，企业应确保预算能够持续支持 IT 培训。一年只进行一次培训是无济于事的。

4. IT 员工培训和认证

在网络安全领域，经常出现员工倦怠的问题。企业应通过培训和认证支持其 IT 员工。

这会带来两个优势。首先，员工可以将最新的知识应用于企业系统。其次，这有助于员

工的职业发展，能够提高员工士气。企业应记住，“投资回报”这一概念也适用于其员工。

5. 系统维护带来的网络安全成本

企业应注意，不要让其系统进一步降级或承受负担。如果系统的寿命即将终结，这一点就更加重要了。企业应接受这一事实。但是，在考虑年度维护成本时，企业需要注意成本是不断变化的。5G 网络的部署意味着，增强的端点保护、事件管理和编排都将越来越近。随着传统系统的寿命终结，数字化转型会不断加速。

因此，如果企业还未将“旧系统的寿命终结”纳入 2021 年的计划中，现在是时候开始考虑了。就像有些旧车不值得修理一样，有些旧系统也不值得企业支付昂贵的维护费用。在这种情况下，企业应考虑进行系统升级。

6. 网络保险

如果不将保险考虑在内，就无法计算长期的网络安全成本。尚未购买网络保险的企业，是时候开始考虑了。企业应找到适合自己的保险，并牢记：如果不考虑上述问题，网络保险的成本可能会超出想象。

网络保险可能很快就会跟“防洪保险”一样重要了。目前，很多企业通过一般保险条款提出网络索赔，因此保险业将在这一商业模式上大放异彩。这可能意味着，网络保险覆盖范围的确定需要参考定期漏洞评估、修复、渗透测试和培训等项目。此外，不要忘记将认证和审计作为证明。

逐步建立防御

总的来说，网络安全成本可能会很高，但这是一项不错的长期投资。企业可以根据上述建议制定网络安全预算，以增强其网络弹性。

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