

首席执行官层面的指南：网络安全领导人

治理

贵组织的网络安全始终关涉最高的管理层。首席执行官与董事会必须保持对风险的理解，并对组织的网络安全活动和人员承担最终职责和责任。您应当：

- 如果没有 CISO, 请聘用一位 CISO, 或者如果资源有限, 任命贵组织内部的某个人执行 CISO 的职能。
- 与该 CISO 或者其他技术人员合作, 采用国际、国家和行业标准 and 指南制订并维持专门针对贵组织特定网络风险的安全策略。
- 针对执行和管理组织的网络安全明确相关人员的职责和责任。
 - 与 CISO 合作以明确各级员工适当的网络安全职责和访问权限。
 - 监管沟通与合作, 以确保网络安全管理是全面的, 特别是组织内的几名人员或几个部门共同承担网络安全责任时 (例如拥有单独的信息安全、风险和技术垂直部门时)。
- 确保 CISO 具有明确、直接的沟通渠道, 以便及时向您和董事会报告威胁。
- 邀请 CISO 或其他技术人员定期向高级管理层提供简报。
- 确保组织的安全政策、标准、执行机制和程序在所团队和业务范围内保持一致。

风险评估和管理

确保强大的网络安全意识和准备工作依赖持续、基于风险的分析。为了改进贵组织的网络安全：

- 将网络安全风险评估与管理置于贵组织广泛的风险管理和治理流程的重中之重。与您的 CISO 或其他技术人员合作制订计划, 以便开展涉及以下因素的风险评估：
 - 说明贵组织的资产及其各种技术依存性级别,
 - 评估贵组织的成熟度以及与贵组织资产的技术依存性相关的内在风险。
 - 确定贵组织期望的成熟状态,
 - 理解网络安全威胁在贵组织的风险优先顺序列表中所处的位置,
 - 明确您目前的网络安全状态和希望的目标状态之间的差距,
 - 实施计划, 获得和维持成熟度,
 - 评估和拨出资金投入网络安全, 并解决现有差距,
 - 持续再评估贵组织的网络安全成熟度、风险和目标, 以及
 - 考虑使用第三方渗透测试或者红队演练,
 - 考虑购买网络保险等保护措施。
- 在风险评估流程中领导员工工作, 以促进整个机构的及时响应。
- 分析并提交风险评估结果, 供管理层 (包括主要利益相关人和董事会) 监督。
- 监督任何变更, 以保持或提升贵组织理想的网络安全准备状态, 包括充分的预算, 确保为改善网络安全所采取的任何措施与风险相称且贵组织在经济上可以承担。
- 监督持续监测的实施, 以便在解决正在形成的网络风险方面保持灵活性。

组织文化

贵组织的网络安全不是一次性的程序或少数员工的工作；它是所有业务决策和运营活动中均需考虑的一个要素，是所有员工必须保持的一种实践。为了鼓励在贵组织实现持续、整体的网络安全：

- 与领导层开始讨论网络安全并与负责管理网络风险的人员定期沟通。
- 将网络安全培训作为所有员工入职的一部分, 确保所有员工了解最新——且已签署文件同意遵守——贵组织的网络安全政策, 且您的信息技术部门或其他技术人员已向它们提供最佳实践的简报。
- 机构应针对所有员工的短期和长期安全责任反复对其进行网络安全培训。
- 确保贵组织在评估潜在的供应商以及与第三方分享数据时始终考虑网络安全。
- 在考虑并购时, 纳入组织的网络安全评估情况。
- 每年审核贵组织的网络安全政策。
- 鼓励主动在贵组织内部以及与受信任的同行分享关于网络安全威胁和事故的信息。
- 培养一开始就纳入安全疑虑和计划的创新。