小型组织的网络安全

CEO 检查清单:网络安全领导人

治理

- □ 如果无负责人员，任命一名首席信息安全官 (CISO)
- □ 制定并维护组织的网络安全政策，该政策以风险为基础，并知悉国际、国家和行业标准与指南。
- □ 确定网络安全涉及的所有工作人员的职位和职责。与您的 CISO 共同确认所有级别员工的适当网络安全职位和准入权限。
- □ 确立或明确处理网络安全不同方面的任何单独单位或工作人员之间的沟通渠道。
- □ 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。
- □ 定期邀请您的 CISO 或其他技术人员向高级管理层提供简报。
- □ 查看整个组织的网络安全政策、标准和机制是否统一。

风险评估和管理

- □ 与您的 CISO 或其他技术人员共同开展网络安全风险评估，包括:
  - 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
  - 考虑购买网络保险等保护措施。
- □ 分析并向关键利益相关人和董事会出示结果。
- □ 计划监督任何措施，以提高网络预备水平，并监督进展情况。

组织文化

- □ 在领导层层面定期讨论网络风险和安全。
- □ 确保网络安全培训成为所有员工入职的一部分，使所有员工签署同意遵守组织网络安全政策的文件。
- □ 为所有员工安排周期性网络安全培训。
- □ 确保组织在评估潜在供应商和与第三方分享数据时始终将网络安全考虑在内。
- □ 在考虑并购时，纳入组织的网络安全评估情况。
- □ 每年对组织的网络安全政策进行审核。
- □ 鼓励技术人员自愿分享有关网络安全威胁和事件的信息。

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org