小規模組織向けサイバーセキュリティ

CEO 向けチェックリスト：サイバーセキュリティにおけるリーダーシップ

ガバナンス

- ☐ 最高情報セキュリティ責任者（CISO）が存在しない場合は、当該責任者を任命する。
- ☐ リスクベースならびに国際的、全国的、および業界の基準かつガイドラインの情報に基づく、全社的なサイバーセキュリティポリシーを確立・維持する。
- ☐ サイバーセキュリティに関与する全ての従業員の役割と責任を定義する。自身の CISO との協力の下、あらゆる職位の職員に関する適切なサイバーセキュリティの役割とアクセス権限を特定する。
- ☐ サイバーセキュリティの異なる側面に対処する別個の部署または従業員間の明白なコミュニケーションチャンネルを確立または特定する。
- ☐ CISO には、適宜自身と取締役会に脅威について伝えることの可能な、明白な直通のコミュニケーションラインが設けられていることを確認する。
- ☐ 上級管理職へのブリーフィングを行えるよう、CISOまたはその他の技術職員を定期的に招待する。
- ☐ サイバーセキュリティのポリシー、基準、そして機構が組織全体で統一されていることを確認する。

リスクアセスメントおよび管理

- ☐ CISO またはその他の技術職員と共に、サイバーセキュリティに関するリスクアセスメントを実施する。これには、次の内容を含める必要がある:
  - 組織のアセットおよびそれぞれのテクノロジー依存の度合いの解説
  - 組織の成熟度、またアセットのテクノロジー依存度に関連した固有のリスクのアセスメント
  - 組織が希望する成熟度の判断
  - 組織のリスク優先度リストにおけるサイバーセキュリティ脅威の位置づけ
  - サイバーセキュリティの現状と目標とする状態のギャップの特定
  - 成熟度の達成および維持に向けた計画の実装
  - セキュリティへの投資資金の評価および割当て、ならびに既存のギャップへの対処
  - 組織のサイバーセキュリティの成熟度、リスク、目標の継続的な再評価
  - サイバー保険の購入といった安全対策の検討
- ☐ 結果を分析し、主要ステークホルダーおよび取締役会に提示する。
- ☐ サイバーレディネスを高める手順を監督して、進捗状況を監視する計画を立てる。

組織文化

- ☐ サイバーリスクおよびセキュリティについて、リーダーシップレベルで定期的に協議する。
- ☐ 全ての従業員のオンボーディングの一環としてサイバーセキュリティトレーニングを行い、組織のサイバーセキュリティポリシーの遵守に合意する書類への署名を要求する。
- ☐ 全ての従業員を対象としたサイバーセキュリティトレーニングを繰り返し実施する。
- ☐ 組織が潜在的なベンダーを評価し、第三者とデータを共有する際は、必ずサイバーセキュリティを考慮する。
- ☐ 合併および買収を検討する際は、組織のサイバーセキュリティアセスメントを組込む。
- ☐ 組織のサイバーセキュリティポリシーの年次審査を制定する。
- ☐ サイバーセキュリティ脅威およびインシデントについて、技術職員が自発的な情報共有を行うよう奨励する。

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org