小規模組織向けサイバーセキュリティ

取締役会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

サイバーリスクガバナンスの基本

☐ グループ全体で、取締役会が以下の質問に「はい」と回答できるか定期的に評価する：

- 貴組織は、一般データ保護規則（GDPR）などの関連の法定および規制要件を満たしていますか?
- 貴組織は、サイバーエクスポージャーを定量化して、その財政的レジリエンスをテストしましたか?
- 貴組織は、サイバーエクスポージャーが合意済みのリスク選好度内に収まるよう、改善策を配備していますか?
- 取締役会は、経営陣が提供する組織のサイバーレジリエンスに関して簡潔、明晰、かつ実用的な情報の定期的な協議を行っていますか?
- 貴組織が配備しているインシデントレスポンス計画では、取締役会レベルを含めて最近予行演習を行いましたか?
- サイバーリスク管理を担当する主要人物の役割は明確であり、3つの防衛線と連携していますか?
- 貴組織のサイバーリスクポスチャに対する独立検証および保証を取得しましたか（例：テスト、認証、または保険）?

☐ 上記の1つ以上の質問に「はい」と回答できない場合は、CEO、CISO、関連組織の従業員、および／または社外リソースと協力して問題を是正する。

監督

☐ 取締役会が、貴組織のサイバーリスクおよびレジリエンスに関する究極の責任者である点を認識するよう万全を期する。

☐ 必要と見なされれば、監督機能を特定の取締役会委員会に委任する。

☐ 貴組織のサイバーレジリエンス管理能力およびサイバーレジリエンス目標の実装の進捗状況について報告する責任を1人の執行役員に任命する。通常、これには最高情報セキュリティ責任者（CISO）が指名される。

☐ この執行役員には、取締役会への定期的なアクセス、十分な権限、主題に関する運用能力、経験、そして当該任務の遂行に必要なリソースが備わっていることを確認する。

☐ 毎年、貴組織のリスク許容度を定義して、それが企業戦略とリスク選好度に合致していることを確認する。

☐ 貴組織のサイバーレジリエンスに関する正式な独立審査が毎年必ず実施されていることを確認する。

☐ 貴組織の総合的な事業戦略、リスク管理、予算編成、そしてリソース配分にサイバーレジリエンスとリスクアセスメントを統合するべく取り組む。

☐ 第三者リスクを定期的に審査する。

☐ サイバーレジリエンスプランの作成、実装、テスト、そして継続的な改善を監督することで、貴組織全体における調和、そして説明責任を負う CISO またはその他の執行役員による取締役会への定期的な報告を確認する。

☐ 上記に関するパフォーマンスを定期的に審査し、継続的な改善を実現できるよう独立した助言を得ることを検討する。

最新情報の入手

- ☐ 個人が取締役会に加入する際は、当該個人がサイバー脅威によるリスクの把握・管理に必要な適切かつ最新のスキルと知識を持ち合わせていることを確認する。
- ☐ 貴組織の現在および将来的なリスクの露出、関連の規制要件、そしてリスク選好度に関する業界および社会のベンチマークについて、組織の経営陣より定期的な助言を求める。以下の点に従事すること：
  - 新しい法規がもたらす義務に関する定期的なブリーフィング
  - 取締役会および執行委員会の共同計画、およびサイバーセキュリティ分野のベストプラクティスを実践している同僚およびリーダーを訪問
  - 脅威環境に関するセキュリティブリーフィング
  - ガバナンスと報告に関する取締役会レベルの情報交換
- ☐ 経営陣には、取締役会議中の常設の議案としてのサイバーリスク、脅威、およびイベントについて、定量化された分かりやすい報告を行う責任があることを明白に伝える。
- ☐ サプライチェーンの脆弱性、共通の依存関係、そして情報共有におけるギャップなど、進行中の体系的な課題に関連した進展について経営陣およびその他の関連職員と定期的に確認する。

基調の打ち出し

- ☐ 貴組織のサイバーレジリエンスを確保するため、あらゆる職位の従業員が各自重要な責任を負っていることを認識するよう万全を期する。
- ☐ 希組織のリスク文化の醸成および維持における経営陣の役割を監督する。安全性および健全性に対するリスク文化の影響を考慮した上で、貴組織のリスク文化の有効性を定期的に評価し、必要に応じて変更を行う。
- ☐ 全ての従業員が誠実に行動し、希組織内外で観察したコンプライアンス違反を速やかにエスカレーションすることを求めている点を明確に伝える。

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org