経営層向け

事例で学ぶサイバーリスクマネジメント
～経営トップがすべきこと　実践編～

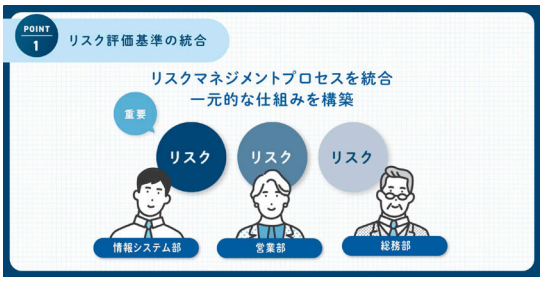
②適正なROI（投資対効果）を実現するサイバーリスクマネジメント

企業は、サイバーリスク以外にも、様々なリスクを抱えています。各リスクの影響度と対応の困難さを把握した上で、メリハリを付けた投資を実行する必要があります。

企業内に散在するリスクを一元的に評価する仕組みを構築した上で、コストをかけて対応するリスク、しないリスクを決定します。リスクの特性に応じて対応方針を決定したら、ステークホルダーへの説明も必要です。
それぞれのポイントについて、経営層が取るべきアクションのヒントをご紹介します。

ポイント1 リスク評価基準の統合

ある企業では、経営層直下の組織として全社統合のリスクマネジメント委員会を設立し、「リスクの発生可能性」と「影響度」を基準に共通のリスク評価の指標を定義しました。
まず各部門で自部門と関連するリスクの評価を行い、リスクマネジメント委員会が結果を集約しました。サイバーリスクについては複数部門が関連するため、情シス部門と関連部門が連携して評価を行いました。最終的に、リスクをマネジメントする一元的な仕組みを構築し、経営判断に資する情報を得ることが可能となりました。



ポイント2 リスクの対応範囲の検討

洗い出したリスクのすべてに対処するのではなく、優先順位をつけてマネジメントすることが重要です。そのためには、リスクの対応範囲を検討し、コストをかけて対応するリスク、しないリスクを比較して判断することが重要です。
特にサイバーの分野では、予測できない攻撃手口が発生しやすいため、いくつかのシナリオを用意して、それぞれに想定したリスク対応計画を策定することです。予測できない新たなリスクに繋りうる、メガトレンドを把握することも経営層の役割です。

ポイント3 リスクへの対応方針の決定

リスクの特性にあわせて対応方針を決定することが必要となりますが、その対応方針をステークホルダーへ説明し、理解を求めることも経営者の役割です。
一例として、ある企業では、リスクへの対応方針や、対策マニュアルの情報を、CEO名義で企業のIR情報やWebサイトへ掲載しました。各種媒体を通じて透明性を持った事前に行い、明確化することが、リスクが顕在化した際の反発を回避するためにも重要です。

より詳しい内容を動画で確認するには、QRコードまたは下記URLからアクセス
https://security-portal.nisc.go.jp/guidance/executives2/index.html

内閣サイバーセキュリティセンター(NISC)