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～

③強固なセキュリティを体現する企業風土の醸成

企業のサイバーセキュリティ対策を強化するため、基本となるのは人材です。従業員一人一人が基本的な知識を身につけ、事故発生時に正しい行動を取れるような企業風土を醸成していくことが、経営層の責任です。

情報セキュリティ事故の原因の約8割は、人の行動に起因しているというデータもあります。
企業のサイバーセキュリティへの考え方を、分かりやすい行動指針として経営層が策定し、従業員向けに発信することが必要です。
ただし、企業によってはサイバーセキュリティの知見のある役員がいないなどの課題があります。これらの課題を解消するためのポイントをご紹介します。

ポイント1 サイバーセキュリティ担当役員の任命

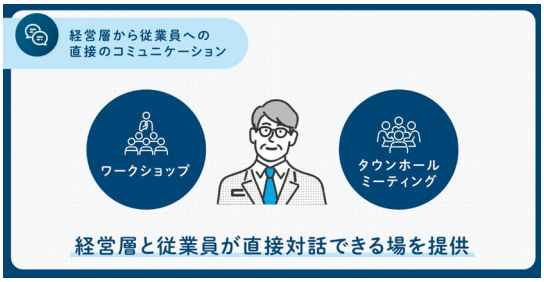
サイバーセキュリティの取組をスムーズに推進するには、「担当役員の任命」がお勧めです。ただし企業によっては「サイバーセキュリティの知見と経営者としての素養の両方を持った適任者がいない」という課題があります。
ある企業では、まず経営者としての判断力に長けた人材を担当役員に起用し、不足する知見を補うため、外部からセキュリティのエキスパートを招聘して役員の補佐をさせつつ、対策を推進しました。
この事例のように、時には社内人材と外部エキスパートの併用を検討することが有効です。

ポイント2 行動指針の策定

担当役員が任命されたら、全社的な情報セキュリティに関する行動指針を策定しましょう。指針の核となる点は、事業継続性の確保や顧客情報の漏えい防止といった内容が一般的ですが、業界やビジネスモデルによっても異なります。
経営層内で、自社の事業継続にとって最も重要な資産が何かを議論することが重要です。
また、指針が実用的でないものになることを避けるため、不明瞭な記述を避け、事故が発生した際の従業員の行動についてなど、明確に盛り込むよう指示することも、経営層の役割です。

ポイント3 経営層から従業員への直接のコミュニケーション

策定した行動指針を従業員へ定着させるためには、経営層から従業員へ強くメッセージを出し、直接コミュニケーションを取ることが重要です。
ある企業では、経営層と従業員とのワークショップを実施したり、経営層が現場に出向き、従業員を集めて意見を交わす場であるタウンホールミーティングを開催したりしました。これらの取組を通じて行動指針に対する疑問や懸念を解消し、従業員の理解を深めると同時に、モチベーションの向上を図りました。



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)