kaspersky BRING ON THE FUTURE

Kaspersky Security Awareness

エグゼクティブのためのサイバーセキュリティトレーニング

デジタル技術は生活のあらゆる部分に大きな影響を与え、より大きな機会を生み出し、コスト効率を高め、グローバルに拡大する能力などさまざまなメリットをもたらしています。しかし、その恩恵を十分に受けるためには、セキュリティ意識を身につけサイバーセキュリティスキルを適切に活用することがこれまで以上に重要になります。

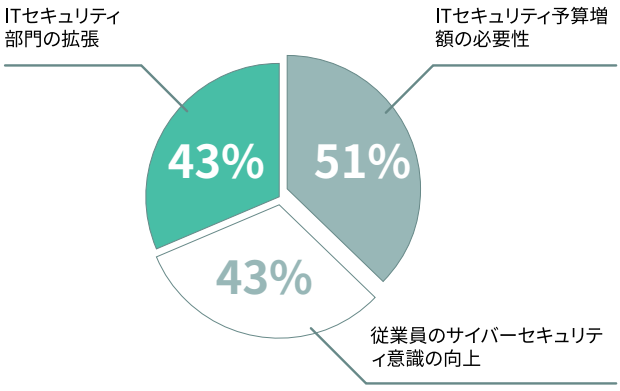
サイバー攻撃や侵害が成功した場合、影響が軽微であれば、社内システムに軽微な混乱が生じて企業のIT部門を悩ませる程度ですが、深刻であれば、組織が壊滅的な打撃を受けます。セキュリティの脅威に先手を打つためには、CISOやIT部門だけでなく、技術部門以外のリーダー達も積極的に関与し、組織全体でサイバーセーフティの文化の構築に取り組む必要があります。

最高レベルのセキュリティ情報や機密情報にアクセスできる経営陣は、サイバー犯罪者にとって格好の標的です。経営陣のサイバーセキュリティに関する知識が欠如している場合や、必要不可欠なサイバーセーフティスキルが不足している場合はもちろん、経営幹部が単純なミスをしただけでも、ビジネスに多大な損失をもたらす可能性があります。

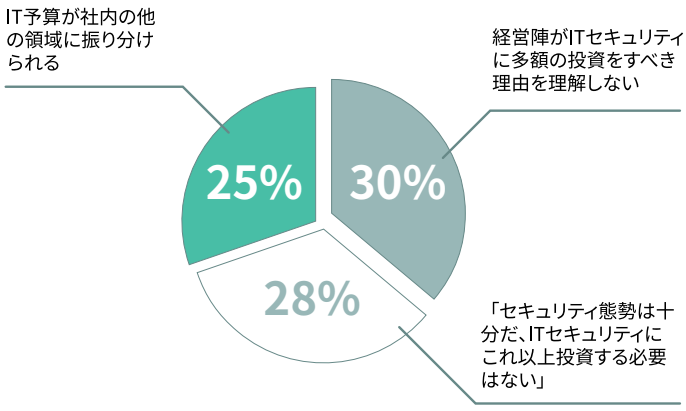
Cレベルの経営幹部とITセキュリティマネージャの認識は共通しているか

ITセキュリティチームと取締役会の連携はすべての企業で有益ですが、上級管理職がサイバーリスクについて十分に理解していると考えるITリーダーはわずか50%に過ぎません。実際のところ、90%ものIT意思決定者は、ビジネスリーダー達がデジタル変革や生産性、その他の目標を優先するためにサイバーセキュリティについて妥協することを予想しています*。このような考えから、IT担当者にとって、Cレベルの経営幹部とITセキュリティ予算の重要性について話し合うことは、最も難しい会話のトップ3に入ります。

最も難しい会話のトップ3:**



企業のITセキュリティ予算が削減される理由トップ3*:**



管理職の62%は、ITセキュリティ部門とCレベルの経営幹部との間にこのような断絶があることが、少なくとも1件のサイバーセキュリティインシデントにつながったと認めています**。

---

* グローバル調査「Business friction is exposing organizations to cyber threats」、トレンドマイクロ
** 「Fluent in Infosec」、カスペルスキー、2023年
*** 「Managing the trend of growing IT complexity」、カスペルスキー

サイバーセキュリティにおけるCレベルの経営幹部の関与 - 教育者の課題

サイバー脅威からビジネスを守るための議論や意思決定に管理職が積極的に貢献している企業は、サイバー攻撃への備えが万全であり、サイバー攻撃から迅速に回復する体制も整っています。組織全体に一貫した効果的なセキュリティ意識を行き渡らせるためには、重要な影響力を持つCEOの関与が不可欠です。しかし、経営幹部は他の重要事項で多忙を極め、スケジュールも過密です。トレーニングの時間を確保するにはどうすればよいのでしょうか？

その答えは、Cレベルのニーズに特化した専門のトレーニングにあります。必要なのは、経営幹部がサイバーセキュリティの状況について理解し、そうした状況とビジネスの効率との重要な関連性を認識しながら、組織全体に利益をもたらすサイバーセキュリティ戦略の構築・適用の運用に関して実際的な洞察を得られる、特別に設計されたプログラムです。

カスペルスキーのエグゼクティブトレーニングおよびエグゼクティブのためのサイバーセキュリティオンライントレーニング：経営陣と意思決定者のサイバーセキュリティ意識を強化

サイバーセキュリティは、プロジェクト管理、金融商品、および事業の効率性とともに、収益創出における重要な側面です。経営幹部を対象とするカスペルスキーコースは、このトピックを中心に展開されます。企業のリーダーや経営陣は、チューターによるコースを通じてサイバーセキュリティの基本を学び、サイバー脅威とそれらから保護する方法について理解を深めることができます。

トレーニングの内容

このコースでは、サイバーセキュリティの重要な側面とビジネスに関連する側面を、専門用語ではなくわかりやすい言葉で説明します。サイバーセキュリティのROIに焦点を当て、サイバーセキュリティに関する部門間の相互理解と協力を促進します。

エグゼクティブトレーニングには、カスペルスキーの専門家が講師を務めるオフラインのワークショップ（**エグゼクティブトレーニング**）とオンラインコース（**エグゼクティブのためのサイバーセキュリティオンライントレーニング**）の2つの形式があります。

エグゼクティブのためのサイバーセキュリティオンライントレーニングは、次のように6つのトピックで構成されています：

1. サイバーセキュリティ概要

a.サイバーセキュリティとは

b.サイバーセキュリティにマネージャが関与すべき理由

c.ユージン・カスペルスキーの挨拶：サイバー防御からサイバーイミュニティへ

2. ビジネスにとってのサイバーリスク

a.サイバー攻撃に起因するビジネス上の損失

b.サイバーリスク管理の手段とアプローチ

c.サイバーリスク管理の成功例・失敗例

3. サイバー攻撃と攻撃者のツール

a.攻撃者のツール：ソーシャルエンジニアリング、エクスプロイト、ダークマーケット

b.サイバー攻撃：タイプ、成功要因、標的型攻撃、大規模攻撃、データ漏えい、身を守る方法

4. 自分自身と会社をサイバー攻撃から守る

a.マネージャのサイバー防衛

b.スタッフのサイバーセキュリティトレーニングと啓発

c.会社のさまざまな発展段階に応じたサイバーセキュリティ

d.サイバーセキュリティ監査とサイバーセキュリティサービス

5. サイバー攻撃の影響への対処

a.サイバー攻撃への対応方法

b.サイバークライシス管理計画

c.インシデントコミュニケーション

6. サイバーセキュリティの将来

a.サイバー脅威：統計情報と攻撃ベクトル

b.インダストリー4.0とモノのインターネット

c.サイバーイミュニティ

各トピックの最後には、自己評価と新しい知識の補強のための実践的な課題と5〜10問の質問があります。すべての課題とレッスンの修了後、最終テストに合格する必要があります。

合格すると、修了証が発行されます。

本コースはカスペルスキーの経営陣および主要なサイバーセキュリティ専門家によって制作されました。合計50レッスンから成り、それぞれ3〜6分で終了します。クラウドプラットフォームにアクセスして受講する形式またはLMSに統合して受講するSCORM形式で提供されます。

これらのプログラムはカスペルスキーが提供するSecurity Awarenessポートフォリオの一部です。このポートフォリオでは、従業員のサイバーセキュリティ意識を高め、組織全体のサイバーセーフティの一翼を担うことができるようにする、魅力的なトレーニングオプションを提供しています。

詳しくはこちら
kaspersky.com/awareness

主なメリット：

- **習得しやすい：**マイクロラーニング + 実践的な課題 + テスト = 知識の定着と維持
- **便利なフォーマット：**オンラインコースはモバイル端末とデスクトップに対応
- **経営陣のニーズに関する深い理解に根ざした内容：**カスペルスキーの経営陣が制作したコース
- **実践的なガイドラインとチェックリスト：**すぐに使用できる資料付き

トレーニングの効果

本コースを修了したマネージャは、次のことができるようになります。

- IT担当者や情報セキュリティ担当者との相互理解を深める
- IT部門やITセキュリティ部門と協力してサイバークライシス管理計画を策定する
- 効果的なインシデントコミュニケーションを計画する
- サイバーリスク評価に基づいて戦略的な意思決定を行う
- サイバー防衛のルールを適用する
- サイバー脅威から自分の身を守る

www.kaspersky.co.jp