KnowBe4
Human error. Conquered.

セキュリティ意識向上トレーニングプログラムの実施に向けて、経営陣の全面的なサポートを獲得するには

はじめに

社内で新たな企画を立ち上げるためには、経営陣の全面的なサポートが不可欠になります。これは、全社展開を必要とするセキュリティ関連プロジェクトにおいては、経営陣の賛同は絶対要件となります。経営陣のサポートがなければ、実施するための予算から始まり、要員の確保を受けることはできません。言い換えれば、経営陣のサポートなしには、全社プロジェクトを立ち上げることはできないと言っても過言ではありません。

セキュリティ意識向上トレーニングプログラムを成功させるには、ここから生み出される従業員のセキュリティ意識変革とセキュリティカルチャーがサイバー攻撃の防御にとって極めて有効であることを経営陣に訴えることが必要である

セキュリティ意識向上トレーニングプログラムを立ち上げるにあたり、経営陣からの理解を得ることは簡単ではありません。経営陣の多くは、サイバーセキュリティを情報システム部門が対処すべき問題と捉えてきています。これまで、サイバー攻撃をテクノロジーソリューション中心に考えられてきました。しかしながら、ますます巧妙化するサイバー攻撃の大半は、「人」の心理的な隙や、「人」が生み出す人的なミスから始まっています。セキュリティ意識向上トレーニングは、サイバーセキュリティプログラムの人的防御の中核となるものですが、経営陣が人的防御の必要性を理解するか否かがセキュリティ意識向上トレーニングプログラムの採用の決め手となります。

経営陣の全面的なサポートは、社員全員が参加する有効なプログラムを展開するには、必要不可欠なものと言えます。経営陣が先頭に立って、トップダウン型で進めることは、このようなプロジェクトの成功の鍵となります。セキュリティ意識向上トレーニングプログラムを成功させるには、ここから生み出される従業員のセキュリティ意識変革とセキュリティカルチャーがサイバー攻撃の防御にとって極めて有効であることを経営陣がまずは理解し、有言実行で展開していくことです。

しかしながら、経営陣の全社的な理解を得るには、関連部門間の根回しと調整が必須ですが、ここには複雑な部門間の利害関係が発生してきます。そして、もう1つの障害は、セキュリティ意識向上トレーニングプログラムは企業に直接的な利益をもたらすものではないということです。

どうしたら、経営陣の全面的なサポートを得ることができるでしょうか。

このホワイトペーパーでは、セキュリティ意識向上トレーニングプログラムへの賛同を得るために、経営陣に問うべきポイントと、全面的サポートを獲得するためのベストプラクティスを紹介します。

採用のためのテーブルに付くためには、どうしたらよいか？

ほとんどの企業では、セキュリティ意識向上プログラムの採用が取締役会の議題に上がることは稀です。そのため、起案者はまず自分が所属する部門の役員にセキュリティ意識向上トレーニングが何故必要なのかを効果的に伝え、計画していることの真の価値と自社にとっての利点を強調することが必要となります。

ここでは、これを効果的に行うために考えるべきいくつかのポイントを紹介します。

- まず、起案者である「あなた」が訴求したいことを何ですか？さらに、決裁権のある経営陣に理解してもらいたい採用利点は何ですか？
- あなた自身が、セキュリティ意識向上プログラムを何故実施すべきなのかを十分に理解していますか？（少し厳しく聞こえるかもしれませんが、自分が何故提案するのか根拠とその背景を十分に理解していなければ、部門長や役員を納得させることはできません!）
- あなたの訴求ポイントと価値提案は、経営陣が納得できるものですか？(あなた自身で自分の価値提案を自問自答してください。あなたが伝えようとしていることと一致するでしょうか？そして、もしそうでないなら、改善してください。）

これらのポイントを押さえることが、セキュリティ意識向上プログラム提案の第一歩です。ここで注意しなければならないことは、多くの場合、他のソースから代替案を受けている可能性が高いです。セキュリティ意識向上プログラムが何故必要なのかをクリアに伝える必要がありますそのためには、あなたの訴求ポイントを整理して、明確で単刀直入なものでなければなりません。さらに、価値提案では、導入メリットを効果的に伝えなければなりません。どんなメリットがあるのかを訴求する導入効果を明確に示すことです。ここで最も注意すべきことは、時間をかけ過ぎて、提案のチャンスを逃してしまうことです。

コミュニケーション戦略がキーとなる

あなたの提案を効果的に伝えるためには、まずは何を目指しているのかを訴求することが必要です。重要なことは、単に数字やパーセンテージ、業界統計を示すことだけではありません。セキュリティ意識向上トレーニングが組織のセキュリティ戦略に欠けていること、そして人的防御が必須の要素であることを伝えることです。

統計データを示す場合、それが組織にとって何を意味するのか、何を達成しようとしているのかを明確に結び付けて、訴求してください。ここで必要なことは、あなたの訴求ポイントにブレが生じないことです。これは、経営陣ごとの独自の解釈が生まれる原因となります。

“What（それは何なのか）”を考える場合、“So What（だから何なのか）”と“Now What（今何をするのか）”の2つも同時に考えることが必要である。これらが欠如することは、最終的な目的を正しく理解してもらえない可能性を生み出すことになる。

あなたの訴求ポイントをまとめる際には、この3ステップのプロセス“What（それは何か）”、“So What（だから何なのか）”、“Now What（今何をするのか）”）を常に念頭に置き、自分の言いたいことを効果的に伝えることが大切です。

- “What（それは何か）” – 統計データなどを使って提案目的を伝える場合に、次の2つの要素を含めるべきです。
    - “So What（だから何なのか）”– それが実際に何を意味するのか？
    - “Now What（今何をするのか）”– この視点から何を実行するのか？

“What（それは何か）”を考える場合、“So What（だから何なのか）”と“Now What（今何をするのか）”の2つも同時に考えることが必要である。これらが欠落することは、最終的な目的を正しく理解してもらえない可能性を生み出す原因となります。

ここでのキーは、あなたのコミュニケーション戦略です。最近、欧米ではストーリーテリングというコミュニケーション手法が注目を集めていますが、起案者としてストーリーテラーになることは極めて有効です。ストーリーを語ることは、訴求ポイントとしての概念を埋め込み、記憶に残すための最良の方法の1つです。

セキュリティ意識向上トレーニングの提案において、まず目指すことは、セキュリティ意識の価値を概念的に理解してもらうことです。もちろん、必要であれば、図表や数字でそれをサポートしますが、このような統計データが経営陣ごとの独自の解釈を生み出さないようにすることです。すべてのコミュニケーションにおいて、あなたの訴求概念を明確に打ち出すことが不可欠です。そうしないと、経営陣は取締役会の前に図表や数字などの詳細な情報に目を通し、個々の独自の解釈のもとに、あなたが取締役会で詳細に説明する前に、不採用の判断を下してしまうかもしれません。

では、どうしたら経営陣の注目を惹きつけることができるか？

経営陣の注目を集めるための秘策があるとすれば、それは次の3つにあります。

1. 経営陣にとってのメリットが含まれているか

あなたの訴求ポイントに“So What（だから何なのか）”の要素を含めてください。ここで忘れてはならないことは、経営陣にとって何が有益なのかを明確することです。セキュリティ意識向上トレーニングの提案では、経営陣がその成果において何が最も重要かと考えているかを理解することです。

ここでは、ポジティブな側面とネガティブな側面の両方から訴求することができます。セキュリティ意識向上トレーニングが適切に行われなかった場合に受けるだろうネガティブな側面は、例えば、サイバー攻撃によって自社の機密情報や顧客情報が漏えいした場合や、サイバー攻撃の被害によって自社の評判に大きな影響が出た場合などから生じるペイン（痛み）について具体的に触れることです。人は常に恐怖に反応するものです。しかし、ポジティブな側面にも目を向けることを忘れてはなりません。例えば、継続的なセキュリティ意識向上トレーニングがもたらす効果として、従業員に自然に根付いてくる行動変容と自社内に生まれてくるセキュリティカルチャーの醸成があります。これらは、サイバー攻撃への耐性を高め、安全な環境作りにつながります。その結果、従業員の生産性を向上させることができるという副次的な効果も生まれます。そして、各部門やグループにとっての重要な組織目標や目的と結びつけることで、より大きな効果を得ることができます。部門やグループを統括する経営陣に対して、極めて有効な採用動機となります。

2. 実施内容と導入メリットの関連性を明確に示す

“So What（だから何なのか）”に答えるもう一つの方法は、セキュリティ意識向上トレーニングの実施内容と経営陣にとって重要な導入メリットとの間に直接的なつながりがあることを明確に示すことです。例えば、機密情報保護・顧客情報保護対策、セキュリティ規定要件、内部統制，コンプライアンス，法令遵守などの組織目標や目的に対する効果です。経営陣がすでに組織で関心を持っていることと明確な関連性を持たせることで、セキュリティ意識向上トレーニングプログラム全体がより親近感のあるものになります。

3. “見える化”と訴求ポイント

ここで、セキュリティ意識向上トレーニングプログラムの売り込みを企画することができます。プログラムの一部として何が数値化されるかを説明し、「これをしないとこうなる、これを正しくやるとこうなる」など、具体的にあなたの提案内容の正当性を実証してください。例えば、Phish-prone™ Percentage（PPP）によって同業他社との数字と比較することです。ここでは、他社に比較して遅れをとっているなど、感情に訴えることを恐れてはいけませんが、FUD（恐怖、不安、疑念）をあからさまに売り込むことは避ける必要があります。ただし、適切かつ透明性のある方法でそれらを使用することは、あなたのストーリーを売り込む上で極めて有効です。

経営陣を巻き込む

経営陣の注目を惹きつけることの次に必要なことは、経営陣をこのプログラムに巻き込むことです。このプロセスでフォーカスすべきことを次に、説明します。

- **コンプライアンス要件とプログラムを結びつける** - セキュリティ意識向上トレーニングは、ほとんどの業界で必要性が認識され、業界標準の法規制遵守のためのベストプラクティス要件となってきています。業界標準の法規制.を学ぶ上で経営陣にセキュリティ意識向上トレーニングの必要性を認識させることです。
- **同業他社で事例にスポットライトを当てる** - 恐怖を煽っていると思われないようにする一方で、自社の経営陣が関係するような出来事や組織に訴求ポイントを関連付けることで、提案を現実的なものにすることができます。ここで指摘された脅威が身近で現実的であればあるほど、より多くの経営陣が対応すべき注意義務があると感じるはずです。
- **確立されたベストプラクティスにあなたのプログラムをマッピングする** - NIST Cybersecurity Framework、National Association of Corporate Directors guidance on cybersecurity、またはあなたの組織に関連する業界固有のガイダンスなどに関連づけることは、この種のプログラムの実行に必要なデューディリジェンス（適正評価手続）を示すことになります。

目標設定フレームワークを上手に活用する

あなたはセキュリティ意識向上トレーニングの取り組みを成功させるためにプランニングを策定しているはずです。意思決定者である経営陣にこの内容を認知してもらうことなしに、あなたのプログラムが採用されることはありません。経営陣は、あなたが提案することの背後にある提案意図を探ろうとするはずです。経営陣のこの考察は、プログラムの採用を決める大きな要因となります。経営陣への提案の仕方が丁寧で几帳面であればあるほど、必要な賛同を得るための成功の可能性は高くなります。

しかし、賛同が得られ始めると、セキュリティ意識向上トレーニングプログラムの成功をどのように評価するかという疑問が噴き出てきます。そこで、あらかじめ目標を設定しておくと、経営陣に対して具体的かつ効果的な説明をすることができます。

目標設定フレームワークはいくつかありますが、お気に入りのものがない場合は、SMART方式で目標を設定してください。SMART方式での目標は次の通りです。

- Specific（具体的である）
- Measurable（計測できる）
- Achievable（達成できる）
- Relevant（上位目標と関連する）
- Time-bound（期限が定められている）

これは、具体的にどういうことを意味するのでしょうか？ここで、いくつかの例を挙げて考えてみます。例えば、「フィッシング攻撃被害をより多くの従業員が回避できるようにしたい」、「従業員がフィッシングのリスクをより認識できるようにしたい」という目標設定は、具体性に欠けると言えます。

しかし、「今後3～4ヶ月以内にPhish-prone™ Percentage（PPP）を30%から15%に減少させたい」という目標設定は、SMARTゴールの条件をすべて満たしているため、望ましい目標であると言えます。この目標は、進捗を測定できるという点で具体的であり、提案書全体のステップと関連付けることで実行可能であり、幹部の目標に関連付けることで適切であり、タイムラインを設定することで時間軸を設定することができます。SMART目標が到達すれば、経営陣の認知に大きなインパクトを与えることができます。このようにプログラムを提案することで、経営陣の賛同を得られる可能性はぐっと高まります。

OKR（Objectives & Key Results）フレームワークを検討する

経営陣を説得する上での効果のあるもう1つの手法が、OKR（Objectives & Key Results）フレームワークを使用することです。このフレームワークは、多くのビジネスリーダーが知っており、多くの経営陣も理解しています。そのため、このフレームワークを通して、経営陣に語りかけることは、極めて有効です。OKRフレームワークでは、具体的な目標を設定し、それを成果指標(Key Result)として測定することができます。

ここでは、この成果指標を提案プランに組み込むための例をいくつか紹介します。

目標（Objective）： 今後12ヶ月の間に、模擬フィッシング演習のPPP（フィッシング詐偽ヒット率）を22%から2%に減少させる。

- **成果指標(Key Result)** ベースラインフィッシングテストを実施し、KnowBe4のトレーニング開始前に現状把握を行う。
- **成果指標(Key Result)** 関連部門と協力して、毎月複数のフィッシングテストシナリオを設定し、継続的な模擬フィッシング演習を毎月実施する。
- **成果指標(Key Result)** 模擬フィッシング演習とセキュリティ意識向上トレーニングを組み合わせて実施して、是正学習を提供することで、学習成果を適時確認する。
- **成果指標(Key Result)** フィッシングを受けやすい従業員や部門を特定して、セキュリティ意識向上トレーニングのプログラムを強化する。
- **成果指標(Key Result)** ゲーム感覚で受講できるコースや報奨・表彰プログラムを開発し、参加意欲を喚起する。

全面的なサポートを得るためのブレーンストーミングスプレッドシート

あなたの提案が売り込む必要がある経営陣ごとに、どのように説得するかを考える必要があります。言い換えれば、それぞれの経営陣のモチベーションは何か、それぞれの担当部署にとって何が重要かを理解することです。そして、それぞれの具体的な価値提案を理解し、それを達成するためにあなたの提案がどのように貢献できるかを理解する必要があります。これは極めて重要で、事前にやっておく必要があります。また、この作業は、あなたの提案を承認してくれる人たちと信頼関係を築く機会でもあります。

また、予算や全面的なサポートを求める前に、相手の懸念事項を聞き出し、潜在的な質問に積極的に答える機会でもあります。これを実現するために、各経営陣について、以下の見出しをつけたスプレッドシートを作成することを考えましょう。（これはあなただけのもので、経営陣に見せるものではないことを忘れないでください）。

- 経営陣の名前
- 役職と部署
- 主な推進要因とニーズ
- 潜在的な懸念事項、質問など
- プログラムが成功した場合の各部門のメリット
- プログラムが成功した場合の各人のメリット
- その他の注意事項やコメント（共通の関心事、信頼関係を築くのに役立つもの）

まとめ

セキュリティ意識向上トレーニングは、短距離走ではなく、マラソンです。セキュリティ意識向上トレーニングを提案する場合、これが1回限りのイベントではないことに理解してもらう必要があります。セキュリティ意識の向上トレーニングは、「1回セットしたら終わり」というプロジェクトではありません。セキュリティ意識向上トレーニングを実施するにあたって理解すべきことは、セキュリティ意識向上トレーニングが「人」を狙う進化し続けるセキュリティ攻撃に対して継続的に対応することが求められるという終わりのない取り組みであることです。定期的に注意を喚起しなければ、いったん実現した行動の変化も、元の状態に戻ってしまいます。行動変化を常態化して、行動変容につなげる必要があります。

セキュリティ意識向上から生まれた行動変容を組織全体に根付かせるためには、時間と一貫したコミットメントが必要です。一朝一夕に効果が現れるものではありません。セキュリティ意識向上トレーニングを通して、セキュリティ意識向上から行動変容、そしてセキュリティカルチャーの醸成を達成しなければ、一過性の成果に終わってしまいます。そのため、経営陣には、この投資が継続と忍耐を必要とするものであることを強調することが重要です。

ここで訴求すべきことは、継続と一貫したコミットメントは必ず成果をもたらすことです。複利が貯蓄の増加につながるという概念は、継続と一貫した繰り返しが目標の達成につながるということを示すのに良い方法です。一度だけ宝くじを買って幸運を求めても、老後のための貯蓄にはなりません。

さらに重要なことは、成果を測定することで「見える化」することです。セキュリティ意識向上プログラムから生まれる成果（従業員のセキュリティ行動にどのような変化が起きたか）を測定して、数値化することです。

セキュリティ意識向上は、サイバー攻撃から組織を守り、より安全な組織を築くと同時に、セキュリティカルチャーの醸成へつなげることでもあります。

データドリブンのアプローチは、極めて有効です。例えば、フィッシングに遭いやすいかどうかは、Phish-prone™ Percentage（PPP）という評価指標を用いることで測定できます。トレーニング開始前のPPPを測定して、トレーニング後にこの数値がいかに改善されたかを測定することで、トレーニングの効果を数値化できます。

さらに、ベンチマーキングという手法を使うことにより、同業他社とのデータと深くすることもできます。また、KnowBe4では、セキュリティ意識習熟度評価（Security Awareness Proficiency Assessment）のためのセキュリティアセスメントを10分ほどで終わるQ&A評価シートで用意しています。このアセスメントは、最新の研究に基づき、サイバー攻撃をいかに受けやすいかをチェックすることができる。より具体的には、組織のサイバーセキュリティ要件に関して個々の脆弱性を評価することを可能にします。

すでに何らかの形で行動を追跡しているのであれば、データドリブンのアプローチによって、ほとんど何でも測定プロセスを構築することができます。

このホワイトペーパーのまとめとして、セキュリティ意識向上トレーニングプログラムが何故必要なのかを考えていただきたい。サイバー攻撃の大半は、「人」の心理的な隙や、「人」が生み出す人的なミス（従業員の行動）から始まっています。

サイバー攻撃者が狙っているのは、1回のヒューマンエラーです。1回の従業員のミスが自社の経営に影響するような惨事を引き起こします。進化し続けるサイバー攻撃に立ち向かうためには、全社一丸となって、継続的なセキュリティ意識向上トレーニングを実施することは不可欠です。セキュリティ意識向上トレーニングについて、各役員と個人レベルで話し合い、粘り強く取り組むことを約束し、継続的にセキュリティ意識向上トレーニングプログラムを行うことのメリットについて話し、説得することです。サイバー攻撃の被害は、もう対岸の火事ではありません。皆さんの会社で、明日起きてもおかしくはないのです

その他の関連情報

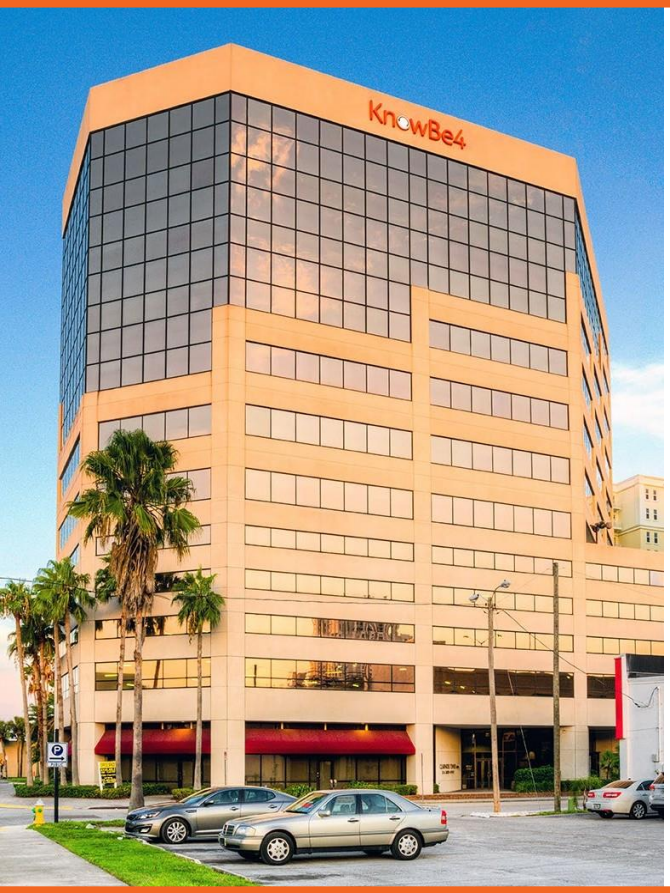
フィッシングセキュリティテスト
あなたの企業や組織の従業員の何パーセントがフィッシング攻撃に引っかかるかをスコア化することができます。

セキュリティプログラムビルダー
あなたの企業や組織のためにカスタマイズされたセキュリティ意識向上プログラムの作成を自動化します。

Phish Alertボタン
あなたの企業や組織の従業員がフィッシング攻撃の報告をワンクリックで行うことができます。

無償Email Exposure Checkツール
あなたの企業や組織の従業員のメールアドレスが、どれくらいインターネット上で公開されているかをチェックできます。

無償なりすましドメインテスト
ハッカーがあなたの企業や組織のドメインのメールアドレスを偽装できるかをチェックできます。



＜KnowBe4について＞

KnowBe4は、セキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。セキュリティの人的要素への抜本的な対策の欠如に気づき、KnowBe4は「人」を狙うセキュリティ脅威から個人、組織、団体を防御することを支援するため設立されました。

KnowBe4プログラムは、偽装攻撃によるベースラインテスティング、クラウドベースのインタラクティブなトレーニング、継続的なアセスメントを組み合わせた統合型のアプローチです。ここには、フィッシング、スミッシングといった多彩な偽装攻撃を通しての本番さながらのフィッシング体験とトレーニングがあります。セキュリティ第一のマインドセットを形成し、組織全体のセキュリティカルチャーを醸成します。

2022年7月現在、5万2千社を超える企業や団体がKnowBe4を採用して、防御 の最終ラインとして「人」による防御壁を構築して、日々求められるセキュリティ上の的確な意志決定を可能にしています。

詳しくは、www.KnowBe4.jpをアクセスしてください。

KnowBe4
Human error. Conquered.

KnowBe4 Japan 合同会社　〒100-6510 東京都千代田区丸の内1－5－1
新丸の内ビルディング10F　EGG 内
Tel: 03-4586-4540| www.KnowBe4.jp | Email: Info@knowbe4.jp

01C06K01