KnowBe4

業界別フィッシングベンチマーキングレポート

2023年度版

目次

VERIZONの2023年度のデータ侵害調査レポートによると**データ漏洩の74%は人的要因によるものです。**単なるミス、認証情報の盗難、ソーシャルエンジニアリングなど、データ漏洩には人的要因が大きくかかわっています。

人的要因によるデータ漏洩への関心の高まりが効果を見せ始めていますが、まだ十分ではありません。

はじめに

サイバー犯罪者は様々な方法でデジタル環境にアクセスすることができます。技術的なセキュリティ管理によって「ハッキングによる侵入」がますます難しくなる中、サイバー犯罪者たちは、レジリエンスが比較的低いターゲットである人的レイヤーに目を向けています。人的レイヤーは、恰好の攻撃ベクトルです。犯罪者はあらゆる弱点を探し、仕事とプライベートの両方の場面でこれを攻撃してきました。残念なことに、多くの企業はテクノロジーに基づくセキュリティレイヤーを重要視し、人的レイヤーの重要性をあまり考慮していません。また、ほとんどの人はプライベートでのリスク予防措置を取らないため、脆弱なまま日々を過ごすことになります。

サイバー脅威は増加の一途をたどっており、犯罪者は試行錯誤を重ねた攻撃手法を利用すると同時に、人的防御レイヤーの効果を最小限に抑えることより洗練された新たな方法を開発してデジタル環境への侵入を試みています。サイバー攻撃から組織を最善の方法で守るためには、従業員がセキュリティカルチャーを推進するために必要な知識、適応した習慣、行動を身につけることが必要です。そのためにはトレーニングをより発展的かつ一貫性のある、本能的なものに変える必要があるでしょう。

すべての地域、業種、企業/組織規模において、フィッシング攻撃は前年比で大幅に増加しています。サイバー犯罪者は被害者を選びません。様々な種類のソーシャルエンジニアリングを通じて、仕事場でも娯楽であっても、昼夜を問わず、ターゲットとなる人に対する攻撃を慎重に構築しているのです。サイバー犯罪者は次の侵入戦略を考える際も、こうした人間の脆弱性を狙い続けてくることでしょう。私たちは、世界的な社会経済問題や健康問題に対処し続けながら、サイバー犯罪者のスキルを強化する人工知能の進歩とも闘わなければなりません。

2022年度、FBIのインターネット犯罪苦情センター (通称IC3) が受ける**アメリカ一般市民からの苦情数は増加しています。80万944件 (毎日2,175件以上) の苦情が報告されており、これは2021年から5%増加、潜在的な損失は103億ドルを超えました。**
さらに、ビジネスメール詐欺は**21,832件にのぼり、調整後の損失額は約27億ドルとなっています。**これらはあくまでも報告された事案のみです。投資詐欺と重要インフラへのランサムウェア攻撃は、最も利益性のある詐欺だということが立証されています。各業界は、システムが危険にさらされ手遅れとなる前に不審な行動を検知・保護・報告するための人的防御レイヤーを備える取り組みに着手しています。

セキュリティリーダーが問題に目を向けず、必要最低限のことしかしない、またはテクノロジーだけを重視し、旧態依然としたトレーニング方法に頼っている場合、これは潜在的な攻撃に対して組織を脆弱なままに放置していることになります。さらに、必要なコンプライアンストレーニングをセキュリティ意識向上トレーニングと混同していると、従業員の知識や能力に大きなギャップが生じるでしょう。 この2つの重点分野を組み合わせて、組織に悪影響を及ぼす可能性のある分野をすべてカバーする、総合的かつ包括的な学習プログラムを作成すべきです。

さまざまなスタイルやバージョンのコンテンツ、継続的なテストやコミュニケーションを含む包括的かつ集中的なプログラムを推進することは、強靭なセキュリティカルチャーを構築する上で必要な取り組みです。

データ漏洩の根本的な原因の大半は人的要因にあるとされている中、セキュリティリーダーがテクノロジーベースのセキュリティレイヤーにのみ投資し続けていると、脆弱性を軽減できるベストプラクティスとして有効な「セキュリティ意識向上トレーニング」と、頻繁に実施すべき「模擬ソーシャルエンジニアリングテスト」が見落とされてしまうリスクがあります。
このアプローチは、サイバー犯罪に対抗する従業員の準備レベルを高めるだけでなく、組織全体に強力なセキュリティカルチャーを推進する上で必要となる重要な基盤を築くものです。

フィッシング攻撃が増加の一途をたどる中、サイバー犯罪者は、従業員に必要な知識・注意力・エネルギーが不足していることを逆手に取り、従業員を騙してフィッシングを仕掛けてきます。つまりストレスが多く、注意力散漫で、教育のなされていない従業員が一人いるだけで、悪質な行為者に狙われてしまうということです。

セキュリティリーダーは、従業員がフィッシングメールを受け取ったときにどう行動するかを知っておく必要があります。リンクをクリックするでしょうか？だまされて認証情報を漏らすでしょうか？マルウェアに感染した添付ファイルをダウンロードするでしょうか？セキュリティチームに知らせずにメールを放置したり削除したりするでしょうか？
あるいは、フィッシングの疑いを報告し、人的防御レイヤーとして積極的な役割を果たすでしょうか？**各企業や組織の従業員がこうしたフィッシング攻撃の被害をどれくらい受けやすいかを示したのが、Phish-prone™ Percentage (PPP: フィッシング詐欺ヒット率) と呼ばれるものです。**フィッシングリスクを測定可能な指標に変換することで、リーダーたちは侵害のリスクを数値化し、「人」を標的にしたサイバー被害のリスクを低減するトレーニングを導入することができるのです。

> セキュリティリーダーは、従業員がフィッシングメールにどう反応するかを知っておく必要があります。**メール内にリンクがあった場合、果たしてクリックするでしょうか？**

業界別リスクの現状把握

企業や組織に対して算出されるPPPは、従業員がソーシャルエンジニアリングやフィッシング詐欺に対してどれくらい脆弱であるかを示しています。標的となった従業員の中にはだまされてリンクをクリックしたり、マルウェアに感染したファイルを開封したり、または組織の資金をサイバー犯罪者の口座へ送金したりしてしまう人もいます。PPPの数値が高いほどリスクも大きく、攻撃被害を受けやすい従業員の数も多いということになります。PPPは低く抑えることが理想とされています。そのためには、従業員がサイバーセキュリティに精通し、こうしたリスクを認識して未然に防ぐことが必要です。

つまり、PPPの数値が「低い」からといって、企業や組織のヒューマンファイアウォールが脆弱であるわけではありません。むしろ、PPPが低い方がセキュリティは強化されています。PPPは実際の状況も踏まえて見るとさらに有効活用することができます。PPPを確認した後で多くのリーダーは、「自社の状況は他社と比べてどうなのか」、「PPPを低下させるのにできることは何か」、「自社でより良いチームを構築するにはどうすればよいのか」といったことを自問します。

本レポートは、自社のPPPレベルを同業他社と比較し、脆弱性ランキングが示唆するものを理解したいというニーズに応えて、KnowBe4が業界を横断して毎年実施している調査をまとめたものです。脆弱性を業種/組織規模別に分類し、組織のセキュリティをより強化してよりレジリエントなセキュリティカルチャーを築くために役立つパターンを探求します。

2023年度 各国業界別フィッシング ベンチマーキング調査

同業他社と比較してどのような評価を受けているかを知りたい組織は多いと思いますが、有効な結果を出すためには、科学的で実績のある方法と組み合わされた確かなデータが必要です。どの企業も、「自社と同じような他の企業とどのように比較するか」という点において大きな疑問を抱いていることでしょう。2023年度業界別フィッシングベンチマーキング調査は、この疑問への解答またはその対策を示唆するために、19業種を横断した3,210万回を超える模擬フィッシング攻撃テストにおいて、35,681社の中から1,250万人を超えるユーザーのデータ統計を分析したものです。

今年の調査の手法

まず、すべての調査対象を業界と規模によって分類しました。それぞれの調査対象のPPPを算出するために、KnowBe4プラットフォームを使用して模擬フィッシング攻撃テストキャンペーンを実施し、この間に誤ってフィッシングメールのリンクをクリックしたり、偽装添付ファイルを開封したりした従業員の数を測定しました。

2023年のレポートでも、これまでと同様に次の3つのベンチマークフェーズを検討しています。

- **フェーズ1:** ベースラインベンチマーキング (トレーニング開始前の事前テスト)
- **フェーズ2:** トレーニング開始後90日までのベンチマーキング
- **フェーズ3:** トレーニング開始1年後からそれ以降のベンチマーキング

トレーニングの効果分析

セキュリティ意識向上トレーニングの効果を判定するために、KnowBe4ではフェーズ1からフェーズ3の各フェーズにおいて次の質問への回答を集計し、トレーニングの成果を測定しました。

フェーズ1

トレーニングせずに模擬フィッシングメールを送信した場合の初期のPPP結果はどうでしたか？

このベースライン ベンチマーキングによって、トレーニング前に従業員がどれくらいフィッシング攻撃被害を受けやすかったかを確認できます。測定対象の個々のユーザーに対して、トレーニング前に模擬フィッシングメールを送信し、これに誤って反応したかを測定します。

フェーズ2

トレーニングを完了し、トレーニング後の90日以内に模擬フィッシング攻撃テストを受けた後のPPP結果はどうでしたか？

最初のトレーニング完了後の90日以内に行われた模擬フィッシングテストの成果をこの質問で判定します。

フェーズ3

その後の継続的なトレーニングと月一回の模擬フィッシング攻撃テストを行った後のPPP結果はどうでしたか？

この質問によって、12か月以上の継続的なトレーニングおよび模擬フィッシング攻撃テストを行った後のセキュリティ意識向上スキルを測定することができます。1年以上前にトレーニングを完了したユーザーを対象に、直近のフィッシング詐欺テストの成績を測定します。

調査方法および統計データ

3,210万
フィッシング攻撃テスト

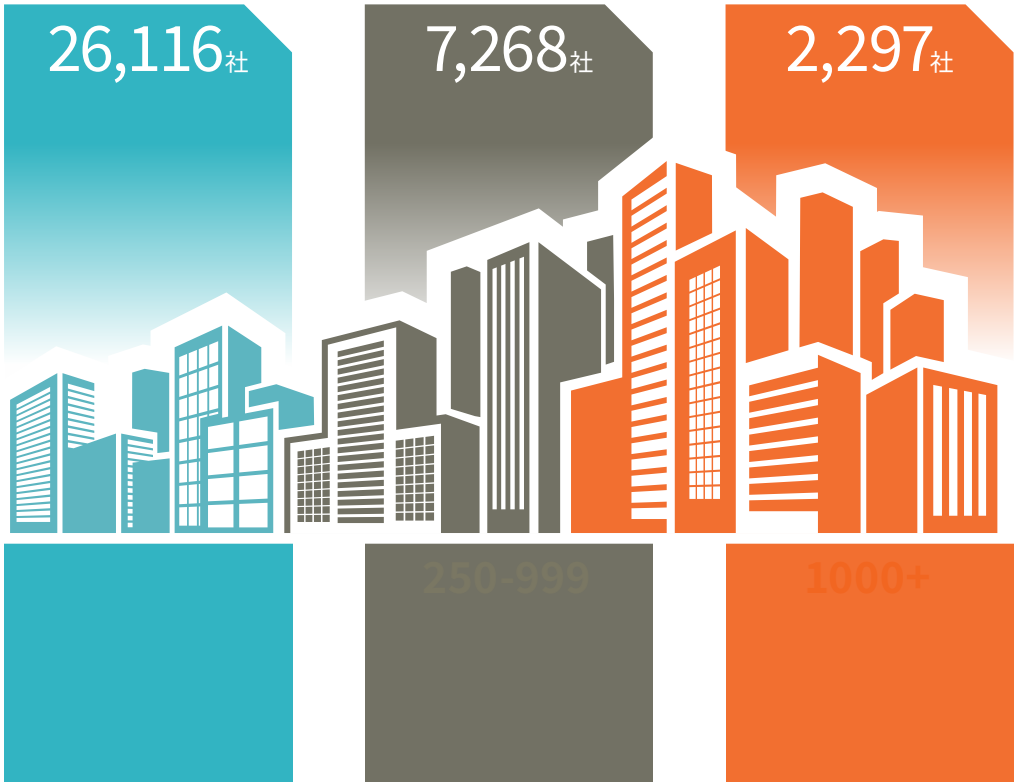
1,250万
調査対象ユーザー

35.6千
企業・組織規模(従業員数)

19業種

- 銀行
- ビジネスサービス
- 建設
- コンサルティング
- 消費者サービス
- 教育
- エネルギー・公益事業
- 金融サービス
- 官公庁
- 医療・介護＆製薬
- ホテル・観光
- 保険
- 法務
- 製造
- NPO
- その他
- 小売・卸売
- テクノロジー
- 運輸

企業・組織規模 (従業員数)



最も被害を受けやすいのは？業界別の脆弱性ランキング

1,250万人の調査サンプルを分析した結果、従業員に適切なフィッシング攻撃テストのトレーニングを実施していない企業や組織はソーシャルエンジニアリングに対して無防備で、被害を受けやすいことが示されました。本年度のPPPデータは2022年に比べて若干改善されたものの、サイバー犯罪者のフィッシングおよびソーシャルエンジニアリング手口を的確に認識している業種は、組織規模に関係なく、現在も一つとしてありません。トレーニング前のベースラインフィッシングセキュリティのテスト結果では、フィッシング攻撃のトレーニングや演習を受けていないユーザーがいかにフィッシング詐欺の被害を受けやすく、企業や組織にセキュリティ侵害リスクをもたらすかが明確に示されています。

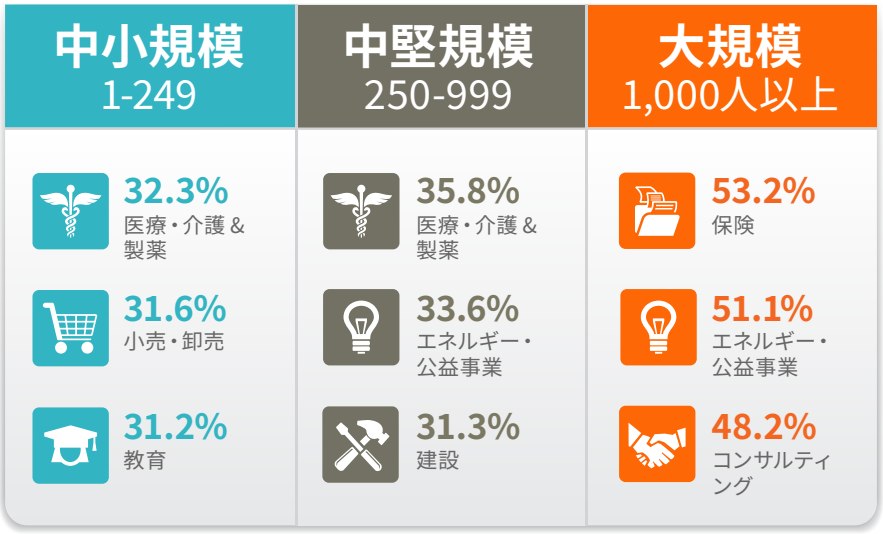
2023年、すべての企業規模とすべての業種の平均のPPPは2022年から1ポイント上がり、**33.2%**となりました。業界によってこの傾向は異なるものの、的確なトレーニングを受けていない従業員はフィッシング攻撃に対する組織の最終の防衛ラインとして失格であることは歴然とした事実です。
適切な知識、トレーニング、テストを受けていない人材は、企業や組織を破壊的なサイバー攻撃にさらすことになります。

- 中小企業 (従業員数1～249人) では、2年連続で上位3業種は変わりませんでしたが、順位が入れ替わりました。**医療・介護 & 製薬業**は2022年よりPPPが若干改善されましたが、2023年の**PPPは32.3%**で首位につきました。次に、**小売・卸売業**が2022年とほぼ変わらない**PPP 31.6%**で2位に続いています。 2022年に首位であった**教育業**は第3位となりましたが、**PPPは31.2%**と1ポイント上昇しています。

- 中堅規模 (従業員数250～999人) では、今年の上位2業種は2022年と変わらず、新しい業種が第3位に加わりました。**ホテル・観光業**は首位から脱出、代わりに**医療・介護 & 製薬業**が**PPP 35.8%**で2位から首位に浮上しました。
  中小企業・中堅規模のどちらにおいても**医療・介護 & 製薬業**が最もリスクの高い業種という結果になりました。
  エネルギー・公益事業は**PPP 33.6%**で第3位から第2位に上がりました。2023年に新たにランク入りしたのは**建設業**で、**PPP31.3%**で第3位となりました。注目すべき点は、**医療・介護 & 製薬業**と**エネルギー・公益事業**のいずれも、最もリスクの高い業種であることに変わりはないにもかかわらず、2022年の格付けに対して前年度比でPPPが高くなっていることです。

最も被害を受けやすいのは？

企業規模別のPPP上位3業種



- 大規模企業 (従業員数1,000人以上) では、**保険業**が2年連続で最もリスクの高い業種とされ、**PPP 53.2%**で2022年とほとんど変わりませんでした。**エネルギー・公益事業**は、2022年の第3位から2023年には第2位に浮上しました。**PPPは51.1%**と前年度をわずかに上回っています。最もリスクの高い業種第3位は、**コンサルティング業** (2022年2位)で、**PPPは48.2%**と以前より4ポイント改善しましたが、極めてリスクが高いことに変わりはありません。
- 中小企業 (従業員数1～249人) で最も低いPPPベンチマークを獲得したのは**法務**で**25.6%**、中堅規模では2年連続で**官公庁**で**26.3%**、大規模企業でも同じく**官公庁**で**25.7%**でした。調査結果の中では最も低い数値でしたが、これらのPPPの結果は、訓練を受けていないユーザー層でも依然としてフィッシング攻撃にかかりやすいということを強く示しています。

ベースラインフィッシングセキュリティテストの結果

ベースラインベンチマーキングは、KnowBe4プラットフォームによるセキュリティ意識向上トレーニングをこれまでに実施したことがない企業や組織を対象に実施しました。調査対象ユーザーに事前連絡を行わず、通常の業務時間内に模擬フィッシング攻撃メールを送信するというものです。ベースラインベンチマーキングでは毎年極めて高いPPPが示されます。

- すべての業種および企業規模のPPP平均は**33.2%**で、2022年から1ポイント増加しました。昨年と同様、3人に1人以上が模擬フィッシングメール内のリンクを誤ってクリックする、悪意ある添付ファイルを開封する、または犯罪者に言われるがままに操作を行ってしまう傾向があることが示されました。
- 2023年のデータで最も大きな進歩があったのは**中堅規模ホテル・観光業**で、PPPの数値が**39.4%から28.5%**へと大きく低下しました。逆に、最も残念な結果となったのは**大規模ホテル・観光業**で、PPPは2022年の**20.4%から2023年には29.5%**へと増加しました。ホテル・観光業は、膨大な量の個人識別情報(PII) を保持しており、その多くが世界各地に分散しているため攻撃対象が広く、サイバー対応能力が芳しくない従業員を雇用していることから、犯罪者の格好の標的となっていることが示されています。
- 最も懸念すべき点は、以下に挙げる大規模カテゴリーに属する業種のPPPがいずれも40%台であることです。**銀行：43%、医療・介護 & 製薬：46.7%、コンサルティング：48.2%、エネルギー・公益事業：51.1%、保険：53.2%** しかも、これらの業種は2022年と変わっていません。これらのカテゴリーの企業に属する従業員はソーシャルエンジニアリング攻撃にかかるリスクが高いということが、2年連続で示されました。

考察： 企業や組織は、従業員のための投資を最小限に抑えようと考えることはやめるべきです。人をターゲットにした攻撃から企業を守ろうとするとき、口先だけのセキュリティ意識向上トレーニングを提供しても効果は得られません。質の高いセキュリティ意識向上トレーニングとテストを高い頻度で提供し、最も効率的な方法で実施することが重要です。また、コンテンツを少しずつ頻繁に配信することで、セキュリティへの意識が高まり、スキルを磨くことができるでしょう。トレーニングや定期的なテストを実施しない場合、規模や業種に関係なく、すべての企業や組織がフィッシング攻撃やソーシャルエンジニアリング攻撃の影響を受けやすくなります。すべての業種で、従業員は攻撃者にとっての攻撃の入口となっています。これは、高価なセキュリティテクノロジーを導入しているかに全く関係なく、避け難い結論と推定されます。トレーニングとテクノロジーの両方に投資することで、適切な効果を得ることが可能になります。

フェーズ1

33.2% ベースライン フィッシング セキュリティテスト の結果

組織の規模	トレーニング前のPPP
1-249	28.1%
250-999	30%
1000+	36.8%

業界	1-249 従業員数	250-999 従業員数	1000+ 従業員数
銀行	25.7%	29.4%	43%
ビジネスサービス	27%	29.2%	31.6%
建設	28.8%	31.3%	36.3%
コンサルティング	27%	31%	48.2%
消費者サービス	29%	30.7%	25.7%
教育	31.2%	29.2%	30.3%
エネルギー・公益事業	27.9%	33.6%	51.1%
金融サービス	26.2%	28.9%	37.3%
官公庁	27.7%	26.3%	25.7%
医療・介護 & 製薬	32.3%	35.8%	46.7%
ホテル・観光	26.8%	28.5%	29.5%
保険	26.1%	31.2%	53.2%
法務	25.6%	29.5%	35.7%
製造	28.8%	30.5%	37.4%
NPO	27.1%	28.4%	28.9%
その他	31%	35.9%	23.1%
小売・卸売	31.6%	29.9%	42.2%
テクノロジー	25.8%	28.2%	32.9%
運輸	26.3%	28.5%	33%

トレーニング開始1年後からそれ以降のベンチマーキング

ベースラインベンチマーキングの後に、トレーニングと模擬フィッシングセキュリティテストを展開して数値を測定したところ、結果に大きな改善がみられました。 ユーザーが最初のトレーニング演習を完了してから、その後90日の間に実施した模擬フィッシングセキュリティテストでより良好な結果が出たのです。トレーニング完了から90日後の平均PPPはほぼ半減して**18.5%**となり、過去4年の数値と横並びになりました。PPPの大幅な低下は、特定の業種や企業・組織規模に限られたものではありませんが、興味深いデータ結果がいくつか得られました。

- 最も大きな変化がみられた組織規模とカテゴリー：小規模 (従業員数1～249人) の**銀行業**ではベースライン時の25.7%からトレーニング後90日以内には12.9%と**49.9%**低下しました。**教育業**も同様に、**85.6%**という大幅な低下を達成し、昨年に引き続き2年連続での結果となりました。中規模 (従業員数250～999人) の**医療・介護 & 製薬業**では、ベースライン時の35.8%からトレーニング後90日以内には20.3%と**43.3%** 低下しました。中規模では最もリスクの高い業界として首位にいた医療・介護 & 製薬業がたった90日のトレーニングでこの結果を達成しました。大規模 (従業員数1,000人以上)**保険業**は、トレーニング前のベースラインPPPで最高値となる53.2%を記録した後、トレーニング90日後には18.2%と**65.7%の低下**を達成しました。中堅規模のケースのように、全体のPPPが最も悪かった業界でも、わずか90日のトレーニングでPPPが大幅に改善されることもあります。
- この結果では、フェーズ2において全業種でPPPが**33.2%から18.5%**へと大幅に低下しました。継続的なテストやコミュニケーションを含む総合的なセキュリティ意識向上トレーニングプログラムを受講すれば、企業や組織は、ユーザーの悪意ある行為の検知・報告能力を適切に向上させることができることを実証しています。トレーニング開始後わずか90日で強力な人的防御レイヤーを形成することが可能であり、企業・組織のセキュリティを大幅に向上することができます。

考察: 「New School」(セキュリティ意識向上トレーニングと模擬フィッシングセキュリティテストの組み合わせ) の実施後90日足らずで、すべての業種と組織規模において従業員の「悪意あるメールの見極め力」が大幅に強化されました。準備フェーズを終え、実際にリスクを低減するにはやはり90日程度の期間が必要です。どんな大きな変化でもそうですが、古い習慣を断ち切り、新しい習慣を生み出すには時間がかかります。しかし、いったんこれらの新しい習慣が形成されると、それが新しい常識となり、組織文化の一部となって他の人の行動に影響を与えます。特に新入社員は、組織で何が社会的、文化的に受け入れられているかを他の人から習得しようとします。

フェーズ2

18.5% トレーニング開始後90日までのベンチマーキング

組織の規模	90日後のPPP
1-249	18.6%
250-999	19.1%
1000+	18.2%

業界	1-249 従業員数	250-999 従業員数	1000+ 従業員数
銀行	12.9%	15.3%	16.1%
ビジネスサービス	19.6%	21%	19.5%
建設	20.6%	21.7%	18%
コンサルティング	19.2%	20.4%	21.7%
消費者サービス	20.2%	20.7%	16.5%
教育	18.4%	19.1%	18.7%
エネルギー・公益事業	17.9%	17.9%	17.3%
金融サービス	16.4%	17.4%	19.7%
官公庁	16.9%	16%	15.5%
医療・介護 & 製薬	20.7%	20.3%	17.5%
ホテル・観光	20.1%	20.4%	15.8%
保険	19.6%	18.1%	18.2%
法務	17.6%	18%	18.5%
製造	18.7%	19%	17.8%
NPO	20.6%	19.9%	16.5%
その他	20.2%	21.6%	21.3%
小売・卸売	19.5%	19.8%	19.7%
テクノロジー	19.7%	20.1%	18.6%
運輸	19.9%	21.1%	19.6%

トレーニング開始1年後からそれ以降のベンチマーキング

このステージでは、12か月以上の継続的なトレーニングおよび模擬フィッシングセキュリティテストを実施した際のセキュリティ意識向上スキルを測定しました。少なくとも1年前にトレーニングを完了したユーザーを対象とし、直近の模擬フィッシング攻撃テストの結果を分析しました。その結果、一貫性のある成熟した意識向上トレーニングプログラムによって平均PPPが**33.2%**から**5.4%**まで低下しました。これは前年比で見ても劇的な成果です。これらの結果は、すべての業界規模と業種で一貫して実証されました。

小規模組織 (従業員数1～249人) としてPPPが最も低かったのは、3年連続で**銀行業**の**3%**でした。銀行業は規制を重視する一方で最も攻撃を受けやすい業界の一つですが、この業界がサイバー犯罪を経験してきたこと、そしてトレーニングに取り組んできた努力が報われたことが紛れもなくこの数値にあらわれています。中堅企業 (従業員数250～999人) のカテゴリーでは、**ホテル・観光業**が12か月後のPPPで**3.8%**を記録しました。これは中堅企業カテゴリーにおけるホテル・観光業の90日のPPPと同様の結果となっています。

大規模企業 (従業員1,000人以上) のカテゴリーでは、**法務業**が**1.8%**の最も低いPPPを記録しました。法律事務所は極めて機密性の高い情報へアクセスする機会が多いため、今後も犯罪者の標的となることは間違いないでしょう。 このようなデータを多く有する組織に対する攻撃は、今後も絶え間なく執拗に続くことが推測されます。法律事務所は攻撃を受ける可能性を全体的に減らすべく、セキュリティ意識向上トレーニングやスマートテクノロジーの導入を増やしています。

データを比較した結果、全体的な改善が最も顕著に見られたのはいずれも大規模企業 (従業員数1,000人以上) でした。**保険業界**のベンチマークPPPは、12か月以上に渡るセキュリティ意識向上トレーニングの結果、**53.2%**から**5.7%**へと89.2%も低下しました。**エネルギー・公益事業**業界は、**51.1%**から**4.5%**へと91.2%減を実現しています。重要な電力システムに対する攻撃は、すぐに有効で長期的、かつ永続的な損害をもたらす可能性があることから、エネルギー・公益事業業界は、サイバー犯罪者にとっては今もなお利益の高いターゲットとなっています。

また、エネルギー・公益事業の企業では、リモートワークが多く、ひと昔前のテクノロジーに依存しています。重要かつ機密性の高い情報がグローバルなネットワーク網を介してやり取りされるため、サイバー攻撃が成功する確率は高くなります。敵対関係にある国は、機会があればいつでも攻撃できる状況にあると言えるでしょう。

フェーズ3

5.4%

トレーニング開始1年後からそれ以降のベンチマーキング

組織の規模	12か月後のPPP
1-249	4.4%
250-999	5.5%
1000+	5.9%

業界	1-249 従業員数	250-999 従業員数	1000+ 従業員数
銀行	3%	4%	4%
ビジネスサービス	4.7%	5.9%	5.4%
建設	4.5%	6.1%	7.3%
コンサルティング	4.4%	7.5%	10.2%
消費者サービス	4.8%	6%	6%
教育	4.6%	5.5%	5.4%
エネルギー・公益事業	3.8%	5.6%	4.5%
金融サービス	4.1%	5.9%	5.5%
官公庁	4%	4%	6.1%
医療・介護 & 製薬	4.6%	5.3%	5.4%
ホテル・観光	4.8%	3.8%	8.8%
保険	4.5%	5.3%	5.7%
法務	4.1%	4.7%	1.8%
製造	4.1%	4.9%	5.9%
NPO	5.5%	6.1%	4.9%
その他	5.4%	7.1%	7.3%
小売・卸売	4.1%	5.6%	5.9%
テクノロジー	4.9%	6.4%	6.5%
運輸	5.4%	8.5%	8%

すべての業種および組織規模での平均改善率

1年以上にわたり、模擬フィッシングテストと継続的なセキュリティ意識向上トレーニングを繰り返し実施した結果、規模や業種に関係なくPPPが大幅に改善されました。中小規模 (従業員数1～249人) の企業/組織では全体の改善率が**84%**にのぼり、19業種のうち12業種で平均以上の全体的に高い改善率を維持し続けています。

中堅規模 (従業員数250-999人) では15業種で**80%以上**を達成し、2業種で80%を若干下回りました。改善率が減少した理由のひとつに、トレーニング前のベースラインがそれほど悪くなかった業種があったことが考えられます。つまり、PPP34%から32%へのベースラインの変化であれば、12か月間の変化率は全体的に低くなります。これは、フィッシング詐欺に対する一般的な認知度が上昇したことでベースラインに影響を大規模(従業員数1,000人以上) では、平均**82%**の改善率を達成し、**銀行、エネルギー・公益事業、法務**の3業種では90%以上の改善率を記録しています。

あらゆる業種や規模において、ベースラインテストから1年以上の継続的なトレーニングとテストに至るまでの平均改善率は**82%**であり、十分に確立されたセキュリティ意識向上トレーニングのプログラムを作成する必要性を改めて浮き彫りにしています。

KnowBe4調べ：トレーニングを受けていないユーザーがフィッシング詐欺に遭う割合は業種全体で**33.2%**

継続的にトレーニングに取り組むことにより、スピーディーな改善を実現することができます。最初のKnowBe4のトレーニングを受けてから90日以内にフィッシングテストに不合格となったユーザーはたったの18.5%でした。KnowBe4プラットフォームを少なくとも1年間使用した後、不合格率は5.4%にまで減少しました。

平均改善率

82%

すべての業種および組織規模での平均改善率

業界	1-249 従業員数	250-999 従業員数	1000+ 従業員数
銀行	88%	86%	91%
ビジネスサービス	83%	80%	83%
建設	84%	81%	80%
コンサルティング	84%	76%	79%
消費者サービス	84%	81%	77%
教育	85%	81%	82%
エネルギー・公益事業	86%	83%	91%
金融サービス	84%	80%	85%
官公庁	86%	85%	76%
医療・介護 & 製薬	86%	85%	88%
ホテル・観光	82%	87%	70%
保険	83%	83%	89%
法務	84%	84%	95%
製造	86%	84%	84%
NPO	80%	79%	83%
その他	83%	80%	68%
小売・卸売	87%	81%	86%
テクノロジー	81%	77%	80%
運輸	80%	70%	76%

2023年度 グローバルフィッシングベンチマーク

グローバルレベルでは、さまざまな規模の企業や組織のフィッシングベンチマークを地域別に特定するために、これとは若干異なるデータを用いています。データは業界別でなく、顧客アカウントに関連付けられた特定の地域別にまとめられて分析されています。グローバルなデータセットには、業種間のPPPの測定に用いたのと同じベンチマーキングフェーズを使用しています。

フェーズ1
ベースラインフィッシングセキュリティテスト結果

フェーズ2
トレーニング開始後90日までのベンチマーキング

フェーズ3
トレーニング開始1年後からそれ以降のベンチマーキング

		ベースライン			90日			1年		
	組織の規模	1-249	250-999	1000+	1-249	250-999	1000+	1-249	250-999	1000+
地域	北アメリカ	28%	30.1%	37.1%	18.5%	19%	18.4%	4.2%	5.1%	5.7%
			合計: 33.1%			**合計: 18.6%**			**合計: 5.1%**	
	アフリカ	30%	29.4%	33.3%	25.2%	22.7%	19.3%	9%	10.5%	5.7%
			合計: 32.8%			**合計: 20.5%**			**合計: 6.6%**	
	アジア	32.6%	33.2%	28.8%	20.9%	19.6%	13%	7.3%	7.4%	6%
			合計: 30%			**合計: 14.9%**			**合計: 6.5%**	
	オーストラリア・ニュージーランド	27.1%	30.9%	41.1%	21.1%	19.9%	15.3%	6.3%	7.7%	5.4%
			合計: 34.8%			**合計: 17.8%**			**合計: 6.4%**	
	ヨーロッパ	26.5%	28%	36.2%	19.1%	19.7%	19.4%	6.7%	7.6%	6.1%
			合計: 32.9%			**合計: 19.4%**			**合計: 6.5%**	
	南アメリカ	34%	27.7%	49.5%	23%	25.8%	18.7%	6.4%	10.2%	5.1%
			合計: 41.1%			**合計: 21.3%**			**合計: 6.9%**	
	英国・アイルランド	26.3%	28%	39.6%	18.5%	18.1%	17.6%	6.1%	8.1%	4.9%
			合計: 35.2%			**合計: 17.8%**			**合計: 5.8%**	

北アメリカ

Erich Kron

最も一般的な問題

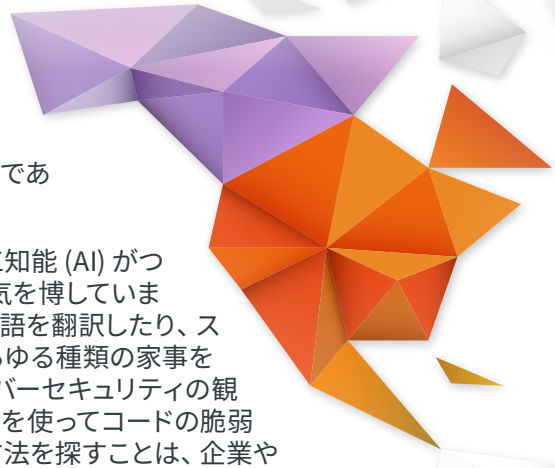
北アメリカにおいて、ランサムウェアは、あらゆる規模および業界の企業にとって最大のサイバー脅威です。ここ数年のランサムウェアを見てみると、サイバー犯罪者はその手口を大きく変えることなく、有用で収益性の高いビジネスモデルを作り続けていることが分かります。北米で成功した攻撃では、サービスとしてのランサムウェア (RaaS) モデルがかなりの部分を占めていることが確認されています。

多くの企業/組織が感染データの復旧に対応できるようになってきたため、2019年、ランサムウェア攻撃者たちはデータを流出させ、これを新たな手段として利用し始めました。今や、これは暗号化よりも大きな問題となっています。悪質な行為者は、情報は力であることをよく理解しており、情報を公開することで相手を脅迫し、金銭を得ようとします。企業や組織にとってはその評判を損なうだけでなく、監督官庁から罰金を科されることも大きな痛手となります。身代金要求額がここ2、3年で急増している理由のひとつに、このような恐喝が増えていることが挙げられます。

BlackFogによると、こうした場合に「集団訴訟」されてさらに追い打ちがかかる場合があるそうです。最近、Dish Networkは、数日間にわたるネットワーク故障により株主に損害を及ぼしたとして6つ以上の法律事務所から集団訴訟を起こされました。

一般にはあまり知られていませんが、サイバー犯罪の一種として壊滅的な被害をもたらすビジネスメール詐欺 (BEC) は、非常に効果の高い攻撃タイプとして表面化してきています。他のタイプのサイバー犯罪と異なり、BECには通常、人が疑問に思ったり、技術的なツールの導入などにより警告することができる添付ファイルやリンクなどの要素が含まれていません。その代わりに、BECはソーシャルエンジニアリングや感情操作を利用して、攻撃者の意図する行動を取らせるようにします。また忘れてはならないのは、VEC (ベンダー電子メール侵害) の増加です。これは、サプライチェーン内のベンダーになりすました悪質な行為者が電子メールを利用し、その顧客から搾取するという手口です。組織や企業間にはすでに信頼関係がある上、悪質な行為者がこれまでに行われていた会話に便乗するため、この種の攻撃は特に成功しやすいようです。

新型コロナウイルス (COVID-19) によるパンデミックの混乱がようやく落ち着きを取り戻しつつある一方で、多くの企業は今もリモートワークへの変更の対応に苦慮しており、パンデミック発生時に発生した技術的負債に対処しています。多くの企業/組織は不確定な状態にある中で、「ノーマル (通常の状態)」とは何かを理解しようとしています。パンデミックと景気低迷の影響で、技術系企業は大量に従業員を解雇しており、すでに世界で変化の波が起こり始めています。企業や組織が不確定であればあるほど、悪質なサイバー犯罪者にとってチャンスであると言えるでしょう。



さらに、多くの人が関心を寄せる人工知能 (AI) がついに主流となり、ChatGPTなどが人気を博しています。ChatGPTがコードを書いたり、言語を翻訳したり、スペルや文法の誤りを訂正したり、あらゆる種類の家事をこなしたりできるという事実は、サイバーセキュリティの観点からは特に憂慮すべきことです。AIを使ってコードの脆弱性を見つけること、検知を回避する方法を探すことは、企業や組織が考慮すべき現実的かつ深刻な脅威です。AIが生成した攻撃が技術的なセキュリティ管理をすり抜ける方法を見つけることがあるかもしれません。しかし人間は、適切に教育されていれば、電子メールやテキストメッセージ、または電話であっても異常を発見し、技術的な管理をはるかに超えることができるはずです。

経済効果

Cybereasonが2021年に実施した調査によると、米国では58%の企業/組織がランサムウェア攻撃の直接的な結果として大きな収益損失を被っています。さらに、米国企業の56%が、ランサムウェア攻撃によってそのブランドが悪影響を受けたと報告しています。また回答者の46%が、攻撃後、データへのアクセスは回復されたが、データの一部またはすべてが破損していたと答えました。

北米および世界中で、BECのように簡単に発生する攻撃が、組織から多額の資金を吸い上げ続けていることになります。FBIによると、2022年、BECの被害額は27億ドルまで激増。それと比べるとクレジットカード詐欺は約2.64億ドルにとどまっています。サイバー犯罪に関して言えば、北アメリカ、特に米国は極めてひどい状況だと言えるでしょう。FBIの報告によると、サイバー犯罪被害者はメキシコで1,119人、カナダは5,517人でしたが、米国だけで479,181人となっています。米国内では、カリフォルニア州の80,666人を筆頭に、次に多かったフロリダ州は42,792人でした。明らかに、サイバー犯罪者は米国をターゲットとしているようです。

主な事業内容

北アメリカにおける主な事業内容は、小規模な個人経営からフォーチュン500に入る企業まで、多岐にわたります。通常、大規模な組織ほどサイバーセキュリティの取り組みに多くの資金を投入できますが、従業員とのつながりが希薄になるため、ある種のサイバー犯罪が発生しやすくなります。ギフトカードの購入や電信送金をさせるには、依頼者とフィッシングのターゲットとなる人物が同じ部屋にいない方が簡単です。

文化の受容と一般的な意識

良いニュースとしては、北米ではサイバー攻撃による脅威の認識が進んでおり、その対処法も成熟しつつあるという点が挙げられます。これは単に問題を認識させることから、企業/組織の文化に直接セキュリティを組み込むことへとシフトしてきています。企業/組織は、自らのセキュリティカルチャー全体を真剣に捉え、改善に取り組みつつあります。機械の操作中やその他の物理的な危険への対処中に怪我をしないためのポスターや看板などの物理的な安全プログラムと、サイバーセーフティプログラムとの間の類似点に気付き始めているようです。物理的な安全性についてのメッセージと同じように、サイバーセキュリティの重要性を従業員に浸透させるためには、常に一貫したメッセージが必要です。うまくいけば、「すべてのメッセージのURLを確認しよう」というメッセージが、「職場に戻る前に手を洗いましょう」や「ヘルメット着用」などと同じように、従業員にとってなじみ深いものになるでしょう。

若い頃からテクノロジーに囲まれてきた新しい若い世代が労働力の一部となる中、テクノロジーに馴染みのない世代に比べ、若い世代にはデータ保護やサイバーセキュリティにおける自分の役割をよく理解している人が多くいます。だからといって、新しい世代が自動的にサイバーセキュリティを理解するわけではありませんが、テクノロジーに慣れ親しんでいる分、適切な教育を受ければ、その役割を把握しやすいかもしれません。

北アメリカ	ベースライン	90日	1 年
1-249	28%	18.5%	4.2%
250-999	30.1%	19%	5.1%
1000+	37.1%	18.4%	5.7%
全組織規模での平均PPP	33.1%	18.6%	5.1%

サイバー犯罪は今後も続くことが予想され、中でも北アメリカは主要なターゲットです。AIなどのツールと同様に、攻撃者はより高度になっていますが、幸いなことに、防御ツールや制御機能も進歩しています。しかしながら、すべての攻撃を阻止できているわけではありません。技術的な管理と人的レイヤーの両方を含む多層的な防御アプローチを用いることが、組織にとって決定的に重要であることに変わりはありません。

サイバー犯罪を阻止するための特効薬はありません。予算が削減され、経済が懸念される中、企業/組織はより少ないリソースで最高の投資対効果が得られるセキュリティ対策に投資することが、かつてないほど重要視されるようになっています。これには、可能な限りの自動化、そして技術的ツールまたは非技術的ツールであるかを問わず、効率的なワークフローなどが含まれます。毎年、データ漏洩やマルウェア感染の原因として、あらゆる形態のヒューマンエラーが上位を占め続けていますが、この問題は、ユーザー教育や組織内の効果的な方針と手順の策定によって劇的に改善することができるでしょう。

BEC攻撃を防御するためには、多額の資金移動や、従業員の記録・知的財産など、組織内の機密情報の移動に対しさらなる承認を必要とする強力なポリシーを導入すべきです。これが、従業員に潜在的なBEC攻撃を素早く発見し報告する能力を植え付け、この種の攻撃に対抗する上で大いに役立ちます。

ランサムウェアによる被害は今後も続くことが予想されますが、企業/組織がデータ損失防止 (DLP) 対策を確実に実施し、バックアップを定期的にテストしてオフラインで安全を確保し、ランサムウェアが拡散する可能性のある方法について従業員を教育することは大きな助けになるでしょう。さらに、ランサムウェアのケースを含まないインシデント対応計画は、もはや選択肢にありません。

トレーニングの方法がより成熟し、教育やトレーニングをユーザーにとってより適切で親しみやすいものにできれば、家庭でも職場でもサイバー犯罪や詐欺から身を守る能力は向上し続けるでしょう。私たち全員が直面しているリスクを理解するために、従業員に適切な教育を行うことが不可欠です。世界中のあらゆる地域において、教育やフィッシングのシミュレーションプログラムの一環として、ポジティブなメッセージを発信することがかつてないほど重要になっています。

結論

- ✓ **北アメリカのPPPは、ベースラインおよび90日では約1ポイントの上昇が見られますが、1年ではわずか数パーセントしか上昇していません。これはトレーニングが有効であることを示しています。**クリック率33%といった高い数字からスタートしても、わずか90日で約18.5%まで劇的に下げることができるということです。1年後のクリック率が5.4%というのは、スタート時点からすれば驚くべき成果です。これは、質の高いトレーニングや模擬フィッシングテストのシミュレーションを行うことで、データ漏洩やランサムウェア感染の第一の原因に真の改善が可能であることを示しています。

- ✓ **興味深いのは、あらゆる規模の組織でクリック率の大幅な低下が確認できているという点です。**変化が最も顕著だったのは大規模企業/組織で、37.1%だったクリック率が1年以内に5.7%に低下しました。もちろん、小規模な組織にあまりメリットがないわけではありません。従業員250人未満の企業/組織では、28%から4.2%へと大幅に低下し、北アメリカの組織規模では最も低いPPPとなりました。

- ✓ **フィッシングメールを発見し報告する能力は、あらゆる規模の組織において、質の高いセキュリティ意識向上トレーニングと模擬フィッシングプログラムを実施することで、わずかな時間で大幅に向上させることができます。**
組織の規模やそれぞれの業種に関係なく劇的な変化が生じており、サイバー犯罪との戦いにおける教育の重要性を裏付けています。

英国・アイルランド（UK&I）

Javvad Malik

最も一般的な問題

英国・アイルランドは、複数の危機と同時に闘う困難な時期にあります。世界的なパンデミックは、公衆衛生と経済の両面に大きな被害をもたらし、失業と経済活動の低下を招きました。英国の欧州連合 (EU) 離脱もまた、この地域に大きな課題を突きつけ、企業経営者にサプライチェーンの問題や大きな不確実性をもたらしました。さらに、現在も続くロシアとウクライナの紛争はサイバーセキュリティのリスクを増大させ、この地域で活動する企業/組織にとっては最大の関心事となっています。

サイバーセキュリティの観点からは、かなり厳しい状況であると言えるでしょう。ランサムウェアによる被害は後を絶たず、ランサムウェアが組織にどれほど永続的な影響を与えるかが浮き彫りになっています。特に政府機関や重要インフラが狙われるケースが増えています。

グローバルサプライチェーンに対する脅威としては、攻撃者がサードパーティのベンダーやサプライヤーを経由して被害組織のネットワークやシステムにアクセスするケースが見受けられました。一方、Log4Jの脆弱性が公開され、ITシステムの弱点が悪用されて攻撃が成功するという課題が浮き彫りにされました。

犯罪者は、政府のエネルギー補助金や確定申告などに関する問題を利用し、ソーシャルエンジニアリング攻撃をさらに強化、SMSや音声ベースのフィッシング攻撃 (スミッシングやビッシング) をますます利用するようになったと見られています。

国家サイバー・セキュリティ・センター (NCSC) の年次レビューでは、当然のことながら、市民や小規模企業が直面する最も重大な脅威はフィッシングなどのサイバー犯罪であり、ソーシャルメディアアカウントのハッキングも依然として問題であると指摘されています。

経済効果

報告指標が定まっておらず、存在しないこともあるため、真の経済効果を定量化するのは難しいと言われています。しかし、私たちが知っている限り、報告されている費用は実際の数字のほんの一部です。

Sophosの報告によると、ランサムウェア攻撃が最も顕著で、英国の企業/組織の13%が身代金を支払っており、その平均金額は882,409ポンド (110万ドル) にのぼります。

しかし、問題はその直接的な金額だけではありません。2020年10月にランサムウェア攻撃を受けたハックニー評議会は、そのランサムウェア攻撃からの回復を支援するためにロンドン当局が1,200万ポンド (1,170万ドル) 以上を負担したことを示す決算を公表しました。その中には、ITコンサルタント費用44万4,000ポンド (55万3,488ドル) 、社会的ケアシステムの回復費用15万2,000ポンド (18万9,482ドル) 、住宅登録費用57万2,000ポンド (71万3,052ドル) などが含まれています。

他の議会ではさらに悪い状況になっており、2021年に打撃を受けたグロスター市議会は、市内の博物館が現在までその館蔵品データベースにアクセスすることができていません。攻撃全体により100万ポンド (120万ドル) の損害を被ったと推定されていますが、利用できなくなったシステムに対する長期的な潜在的損害ははるかに大きいと考えられます。

今回の攻撃は、政府が地域のサービスにもっと投資し、重要な国家インフラに目を光らせる必要性があることを浮き彫りにしています。

攻撃の他に、罰金と報告書による大きな経済的影響もあります。2022年1月から2023年1月にかけて、英国では一般データ保護規則 (GDPR) に基づく個人情報漏えいの届け出が1万件を超えました。

2022年の「National Fraud and Cyber Crime Dashboard」によると、報告件数は28万9330件、被害総額は37億ポンド (約4,600億円) と報告されています。その大半がサイバー犯罪とは対照的な詐欺行為でしたが、攻撃のほとんどはサイバー攻撃に関連するものでした。

主な事業内容

昨年度と比較すると、全組織全体のPPPは30%から35.2%へと大きく増加しています。最も多かったのは従業員1,000人以上の大企業で、32.7%から40%近くまで上がりました。この増加には、ハイブリッドワーキングモデルやスタッフの離職など、多くの要因があることが推察できます。暗い見通しでスタートしましたが、頻繁な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を実施することによって、わずか90日でベースラインを17.6%、1年後には5%以下にまで激減させることができました。初めの状況にかかわらず、定期的で適切なトレーニングがいかに効果をもたらすか、この数字が証明しています。

文化の受容と一般的な意識

脅威が英国・アイルランドに影響を与える一方で、両国はサイバーセキュリティに対する警戒を強めており、社員や個人が自身や組織を守るために果たすべき役割について教育することの重要性が高まっています。

フィッシングは今も最大の脅威ベクトルであり、ランサムウェアは組織に侵入する上で最も一般的な方法となっています。技術的な管理は必要ですが、こうした技術的な変更に必要なコストと時間は、特に資金不足の政府省庁では大きな負担になるでしょう。リスクを軽減するためには、適切かつタイムリーなセキュリティ意識向上とトレーニングの実施が不可欠です。

英国政府は以前から中国のリスクについて話題にしてきました。しかし、ファーウェイのような企業やTikTokのようなアプリを公式な目的で使用することを禁止しようとしていることから、英国・アイルランドのサイバーセキュリティの将来は、中国の対応に大きく左右される可能性があります。また、中国ほどではないとはいえ、イランと北朝鮮もデジタル上の脅威を与え続けていることも忘れてはならないでしょう。

結論

サイバーセキュリティは、英国・アイルランドにとってさまざまな面で大きな懸念事項となっています。ソーシャルエンジニアリングは最大の攻撃ベクトルであり、セキュリティを維持するために果たすべき役割に関する組織や個人の意識を高めるために一層の努力が必要です。

AIやディープフェイク技術の進歩により、ソーシャルエンジニアリング攻撃がより巧妙になることは想像に難くありません。

重要なポイントは次の3つです。

- ✓ ランサムウェアが脅威であり続ける一方で、**サプライチェーンの問題や地政学的な情勢により、企業や組織がこれに先手を打つのはますます困難な状況になっています。**
- ✓ **侵害の影響は、コストと時間という点で、以前考えられていたよりも広範囲に及ぶことが分かっています。** 企業/組織は今後何年にもわたって、情報漏洩の負債を返済し続けることになるかもしれません。そのため、とにかく攻撃を阻止することが重要になってきます。
- ✓ スタート地点において十分ではない組織もあるかもしれませんが、**全体的なセキュリティカルチャーを変え、強固なセキュリティ意識向上やトレーニング戦略に投資することで、短期間で投資回収を実現し、リスクを大幅に低減することができるでしょう。**

英国・アイルランド	ベースライン	90 日	1 年
1-249	26.3%	18.5%	6.1%
250-999	28%	18.1%	8.1%
1000+	39.6%	17.6%	4.9%
全組織規模での平均PPP	35.2%	17.8%	5.8%

ヨーロッパ

Jelle Wieringa

最も一般的な問題

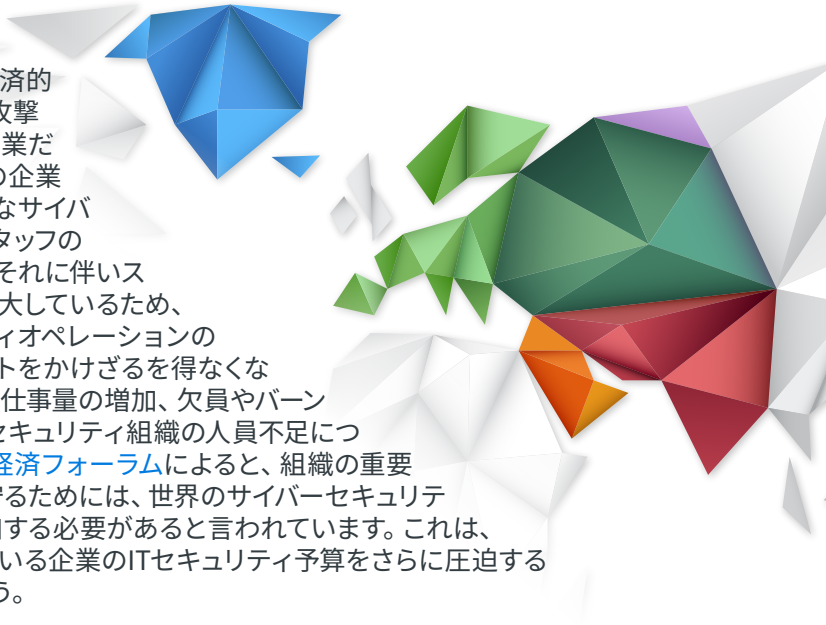
ロシアとウクライナの紛争により、ヨーロッパの社会が大きな影響を受けています。ENISA脅威ランドスケープレポート2022では、この紛争におけるハクティビスト活動の増加、その動員、国家グループによる援助について記述されています。この紛争のせいで、サイバー戦争では偽情報がよく使われるようになりました。ジェネレーティブAIや機械学習など、AIの分野では大きな技術的進歩が見られ、悪意のある行為者がこれらをより身近に利用するようになっています。AIを活用したソーシャルエンジニアリング攻撃、偽情報、ディープフェイクは、今や組織が防御しなければならない事実上の脅威となっています。

最も一般的なサイバー脅威には、ランサムウェア、マルウェア、ソーシャルエンジニアリングなどがあります。IOT-Analyticsの最新レポート「What CEOs talked about (CEOの言葉)」によると、組織のリーダーが最も懸念する事項は、インフレ、景気後退、金利といった経済の不確実性にあるようです。これらは非常に重要なトピックであるにもかかわらず、経営陣はサイバー犯罪の継続的な脅威にも一層注意を払わなければなりません。これを無視すれば、脅威行為者が、準備のできていない組織に対し悪質な活動を続けることを手助けすることにつながりかねません。

経済効果

ヨーロッパにおけるサイバー犯罪の経済的影響を正確に判断することは難しいですが、その影響が財政的に壊滅的な結果をもたらす可能性があるという考え方は広く受け入れられています。

データ漏洩の被害に遭った企業や組織は、GDPRに基づき、影響を受けた顧客に対し賠償請求の支払いを強いられることがあります。弁護士費用、コンプライアンス違反費用、事故調査費用は数百万ドルに上る可能性があり、生産の縮小 (または中止) 、注文の遅延、サプライヤーや顧客に対する評判の低下といった影響を及ぼすことは言うまでもありません。



サイバー犯罪の経済的影響は、サイバー攻撃の犠牲になった企業だけでなく、すべての企業に及びます。有能なサイバーセキュリティスタッフの不足が深刻化し、それに伴いスキルギャップが拡大しているため、企業はセキュリティオペレーションの維持に多くのコストをかけざるを得なくなっています。また、仕事量の増加、欠員やバーンアウトはすべて、セキュリティ組織の人員不足につながります。世界経済フォーラムによると、組織の重要資産を効果的に守るためには、世界のサイバーセキュリティ人材を65%増加する必要があると言われています。これは、今すでに逼迫している企業のITセキュリティ予算をさらに圧迫することになるでしょう。

主な事業内容

ヨーロッパを対象とした今年のPPPデータによると、残念ながら、サイバー犯罪対策への取り組みを改善すべき企業が数多くあることがわかっています。ヨーロッパでは全体的に、小規模企業 (従業員数1～249人) が最も優れた結果を示しており、研修前のPPPは全産業平均で26.5%でした。次いで、中堅企業(従業員250～999人)のPPPが業界平均で28%、大企業(従業員1000人以上)のPPPが平均36.2%となっています。

この結果は、2022年に発表された、大規模な組織の方がサイバー攻撃に対してより脆弱であるという結果と一致しています。欧州連合 (EU) の管理機関の努力により、ネットワークおよび情報セキュリティ指令 (NIS2) のような新しいポリシーが更新され、作成されていますが、すべての国がEU加盟国ではないため、これがすべての企業や組織に適用されるわけではありません。

文化の受容と一般的な意識

ヨーロッパ全域でサイバー犯罪が増加し、企業/組織と消費者を同様に保護するための法律、規制、法規制が整備されたことで、多くの企業がサイバーセキュリティの成熟度に積極的に取り組まざるを得なくなりました。ISACAの「State of Cybersecurity 2022」によると、66%の企業がサイバーセキュリティの成熟度を積極的に評価し、その評価の頻度を年1回以上に増やしています。

サイバー犯罪の増加やITセキュリティスキルの格差の拡大から、セキュリティにかかるコストは増大し、企業は「同等または少ない金額でより多くをカバーする」ことを強いられています。技術費だけでは、組織のセキュリティ態勢を十分にカバーすることはできないのが現状です。したがって、セキュリティ組織は、より効率的で費用対効果の高い他の防御方法を探す必要があります。この動きが引き金となり、強固なセキュリティカルチャーの重要性への関心が高まりました。セキュリティカルチャーとは、組織のセキュリティに影響を与える考え方、慣習、社会的行動と定義されます。組織は、セキュリティカルチャーを積極的に形成し、セキュリティ態勢を整備するための中心的な指針として、この定義を使用し始めています。これにより、既存の労働力 (例えば、人材・プロセス・テクノロジーの三位一体における「人材」の要素) は、セキュリティ戦略においてより重要な位置を占めることになります。

ヨーロッパの多くの組織にとって、デジタルトランスフォーメーションは重要な焦点であるため、セキュリティカルチャーがもたらすビジネスイネーブラーとしてのセキュリティへの最重要アプローチは、多くのセキュリティ組織にとって魅力的なものとなっています。デロイトの2023年版レポートGlobal Future of Cyber Surveyによると、サイバーセキュリティ、リスク管理、事業部門の連携は、サイバー脅威の無力化、事業価値の保護、顧客の信頼の維持に不可欠であることが示されています。そのため、セキュリティカルチャーはあらゆる組織にとって理想的な手段となっています。

結論

サイバーセキュリティは、ヨーロッパ全土の企業/組織の事業継続にとって最大の懸念事項の一つです。平均PPPは32.9%で (2022年の29.9%から増加) 、ヨーロッパのすべての業種と国において、企業/組織はソーシャルエンジニアリング攻撃に対して脆弱であることがわかっています。レジリエンスをさらに高め、リスクポジションを低下させる努力を継続することが肝要であることに変わりはありません。

ヨーロッパ	ベースライン	90 日	1年
1-249	26.5%	19.1%	6.7%
250-999	28%	19.7%	7.6%
1000+	28%	19.4%	6.1%
全組織規模での平均PPP	32.9%	19.4%	6.5%

重要なポイントは次の3つです。

- ✓ **ヨーロッパの企業/組織のレジリエンスを高める努力を強化する。** 地政学的、経済的な脅威のため、人々の関心はサイバーセキュリティから離れてきています。そして、組織のデジタル化が進むにつれ、サイバー攻撃の影響も増大する傾向にあります。
- ✓ **AIを活用したサイバー攻撃の脅威と影響についてユーザーを教育することを重視する。**ディープフェイクや音声バイオメトリクスなど、機械学習の高度化と発展により、脅威行為者は、強力なツールを入手し、危険な攻撃を強化するために誤解を招くコンテンツを作成しています。既存の攻撃形態に変わり、新しい攻撃形態が現実に発生する可能性が高まっているため、これについての教育が不可欠となります。
- ✓ **強固なセキュリティカルチャーを構築するための取り組みを強化する。**セキュリティ意識を組み合わせた、安全な行動を形成するための総合的なアプローチは、リスクを低減すると同時にビジネスを可能にすることが実証されています。

アフリカ

Anna Collard

最も一般的な問題

成長地域であるアフリカでは、テクノロジーと接続性の利用が急速に進んでいます。しかし、成長、繁栄、デジタル化には、発展を弱体化する新たなリスクや脆弱性がついて回ります。

KnowBe4 and IDC Report on Cyber Extortion in Africa (アフリカにおけるサイバー恐喝に関するKnowBe4およびICDレポート)によると、アフリカ南部全域の企業・組織の60%近くが、今後12か月間に接続性とIoTの強化を計画しています。残念ながらこの発展は、攻撃対象エリアが拡大することを意味するものです。スマートフォンの普及、オンラインバンキングのモバイル決済ネットワーク、暗号資産の台頭によって、犯罪者はアフリカ全土において新たなターゲットと資金調達手段を手に入れています。アフリカ大陸のGDPとサイバー犯罪の間には、一方が増加すれば他方も増加するという直線的な関係があり、その結果、アフリカではここ数年、特に中小組織の間でサイバー犯罪が急増しています。

一部のアフリカ諸国では増加するサイバー犯罪に対処するため、厳格な規制遵守法を課していますが、大半の国では行われていません。現在、アフリカ55カ国のうち、データ保護とサイバー犯罪に対する一般的なセーフガードを促進するための法的枠組みであるアフリカ連合マラボ条約を批准しているのはわずか15か国のみです。また、11か国には部分的な法律しかなく、30か国は意義のあるサイバー犯罪法がまったく適用されない状況です。それぞれの政府も、脅威の監視、デジタルフォレンジックの証拠の収集、コンピュータ犯罪の起訴などを適切に行わないことがよくあります。

昨年の報告書で述べたように、アフリカのサイバーセキュリティの最大の問題の1つは、スキル不足です。アフリカでは、サイバーセキュリティ認定を受けた専門家の不足が深刻化しています。多くの組織、機関、消費者はサイバーに対する意識が低く、組織は基本的なサイバーセキュリティ対策を実施していないのが現状です。

サイバー恐喝グループやサイバー犯罪シンジケートは、米国のような成熟した国から、デジタルネットワークに大きく依存しながらもサイバー犯罪を適切に防止、修復、起訴するためのリソースが不足しているアフリカのような新興経済圏を含む他の地域へと関心を移していくことが予想されます。

経済効果

各インシデントや経済的影響が公式に開示されないため、サイバー犯罪が実際にどの程度アフリカ経済に影響を与えているのかは明確には分かっていません。実際、ほとんどのサイバーセキュリティインシデントが未報告です。

国際犯罪に対抗するグローバル・イニシアティブによる2022年の調査報告書「デジタル革命の弊害」によると、「デジタル技術の普及は、新たな組織的サイバー犯罪ネットワークの形成をもたらし、現在ではアフリカの企業に対する脅威の上位にランクされている。また、この地域の経済に年間数十億ドルの損害を与えていると推定される」ことが示されています。

また、南アフリカ科学産業研究評議会 (CSIR) は、政府部門や重要インフラに対するサイバー攻撃が増加し、民間組織だけでなく社会や国の経済にも影響を及ぼすことを予測しています。2021年に起こった南アフリカの国営港湾局企業トランスネットに対するランサムウェア攻撃は、同国の重要な海上インフラに影響を与え、新型コロナウィルスのパンデミックからの経済回復を弱体化させました。重要インフラに対する攻撃は、被害を受けた組織が経験する直接的な損失にとどまらず、壊滅的な経済的影響をもたらす可能性があると言えます。

主な事業内容

アフリカは地理、言語、文化、経済などの点でかなり多様性に富んだ地域です。この地域におけるサイバーセキュリティの状況を掘り下げる際には、このような多様性を考慮に入れる必要があり、国やセクターによってセキュリティの成熟度が大きく異なるということがある程度理解できると思います。

ビジネスにおける成長市場としてのアフリカの潜在力は過小評価されており、多くの誤解が生じています。例えばアフリカの400社以上が年間10億ドル以上の収益を上げていますが、これは世界の同業他社と比べても平均的に成長が早く、収益も高いと言えます。

今年のKnowBe4の業界別フィッシングベンチマークレポートは、アフリカの企業412社に対して行われた合計33万7,937件のフィッシングシミュレーションテストの結果に基づいて作成されました。参加企業の内訳は、それぞれ従業員数1～249人の中小企業が58%、250～999人の中堅企業が26%、1,000人以上の組織が16%でした。データセットの大部分は南アフリカの企業から集められており、次にケニア、ナイジェリア、ボツワナと続きます。

アフリカのベースラインフィッシングセキュリティテストの結果は平均32.8%でした。つまり、トレーニングを受ける前は、従業員の3人に1人が不審なリンクや電子メールをクリックしたり、不正な要求に応じたりする傾向にあったということです。体的なPPPはアフリカのセクターや国によって大きく異なります。

文化の受容と一般的な意識

多くのアフリカ諸国は、独特で複雑な社会経済的状況に直面しており、国際的な課題は、地域レベルにおいてはさらに複雑なものとなっています。

例えば、南アフリカは世界で最も不平等な国のひとつであり、その結果、貧困率や失業率が高く、犯罪率も増加しています。

アフリカは世界で最も若い人口を擁する地域であり、年齢の中央値はわずか19.7歳です。アフリカの若者たちはインターネットを通じて世界とのアクセスを求めており、テクノロジーの導入とデジタル化を推進しています。モバイル・スマートデバイスの所有率は飛躍的に増加し、ソーシャルメディアや暗号資産の利用も増えつつあります。国際通貨基金（IMF）によると、サハラ以南のアフリカは、世界で唯一、国内総生産の10%近くがモバイルマネーによって生み出されている地域です。給与の受け取り、日々の支払い、請求書の確認、買い物などにモバイル端末が活用されています。

アフリカ	ベースライン	90 日	1 年
1-249	30%	25.2%	9%
250-999	29.4%	22.7%	10.5%
1000+	33.3%	19.3%	5.7%
全組織規模での平均PPP	32.8%	20.5%	6.6%

KnowBe4による2023年度アフリカのエンドユーザーによるサイバーセキュリティと意識調査レポート

- アフリカ8カ国の回答者の71%がモバイルデータを使ってインターネットにアクセスし、63%がモバイルバンキングと決済に携帯電話を使用していることが示されました。
- また回答者の68%がサイバー犯罪に懸念を示していましたが、どのような脅威にさらされているのか基本的な理解を持つ人は少数でした。
- 57%がランサムウェア攻撃とは何かを知りませんでした。21%が電話によるソーシャルエンジニアリング攻撃 (ビッシング) を経験し、32%が詐欺の被害にあって金銭を失ったことがありました。
- さらに、36%が暗号資産詐欺の被害に遭ったことがあり、57%がそのような詐欺の被害に遭った人を知っていると答えました。

KnowBe4とITWebが南アフリカで実施した調査 (2022年) によると、フィッシングメールをクリックしてしまうなどのセキュリティ上のミスを犯す理由の第1位は「認識不足やトレーニング不足」 (52%) 、第2位は「注意散漫、マルチタスク、認知過多」 (38%) でした。

結論

✓ **この地域の企業・政府はどちらもサイバーセキュリティに対する優先順位付けと投資の不足に対処する必要があります。**政策立案者の意識を高め、能力開発の努力を支援することが優先されるべきでしょう。

✓ **アフリカのサイバーセキュリティの課題を支援するためには、官民の提携が必要です。**この地域の企業は最も基本的なセキュリティ対策ですら賄えないことが多く、 投資が可能な企業はサイバーセキュリティのスキルを持つ人材を探すのに苦労しています。民間企業、特に金融サービス部門は、政府にはないサイバーセキュリティに関する人的資本、インフラ、能力、専門知識を有しています。

✓ **この地域の企業は最も基本的なセキュリティ対策ですら賄えないことが多く、**政府や教育機関は、セキュリティ専門家の能力拡大に向けて投資するとともに、サイバーセキュリティ意識を社会に出るすべての若者のライフスキルにすることが求められています。

ビジネスにおける成長市場としてのアフリカの潜在力は過小評価されており、多くの誤解が生じています。**アフリカの400社以上が年間10億ドル以上の収益を上げています...**

... これは世界の同業他社と比べても平均的に成長が早く、収益も高いと言えます。

南アメリカ

Rafael Silva

最も一般的な問題

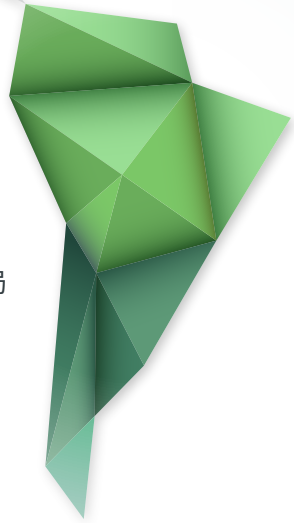
ランサムウェア、フィッシング、携帯電話の盗難は、中南米の企業および個人の双方にとって、2022年の上位にあがる脅威です。ブラジル通信庁 (Anatel) の報告によると、ブラジルのサンパウロだけで、毎日553台の企業や個人の携帯電話が盗まれていることが明らかになりました。

中南米では、2022年にランサムウェア攻撃が大幅に増加しましたが、ほとんどの企業が代金を支払っておらずデータのアクセスを取り戻していません。サイバーセキュリティ企業のSophosが実施した「The State of Ransomware 2022」と題する調査によると、ブラジルの調査対象200社のうち55%が昨年ランサムウェア攻撃の標的になっていることがわかりました。(2020年は38%)。

2022年、フィッシング攻撃は中南米の企業や個人にとって大きな懸念事項でした。新型コロナウィルスの流行によるリモートワークの増加やオフィス勤務に戻る動きの増加により、サイバー犯罪者がその脆弱性を悪用し、新たに無防備なユーザーを標的にする機会を作り出しました。サイバー犯罪者は、常にログイン情報、財務情報、個人識別情報など、重要かつ機密性の高いデータを求めています。カスペルスキーの報告によると、今年、サイバー犯罪者は暗号資産フィッシングに相当数手を出しており、その数はわずか1年で40%増加しています。

ソーシャルメディアと暗号資産に特化したアカウントの乗っ取りは、中南米全域で大幅に増加しています。これは主に、ソーシャルメディアと暗号資産が詐欺行為者や攻撃者の間で急速に有名になっていることが理由にあります。ソーシャルメディアアカウントや暗号資産に不正アクセスし、それを使ってさらなる詐欺や偽装を行おうとするサイバー犯罪者の数は著しく増加するでしょう。

経済効果



ランサムウェアは中南米の企業に財務の面で大きな影響を与え続けており、大きな損失をもたらしています。2022年だけでも、ブラジルのeコマース企業がランサムウェア攻撃の被害に遭い、1億8,300万ドルという途方もない損失を被りました。この数字は年々一貫して上昇傾向にあります。

2022年、ブラジルは一般データ保護法 (LGPD) を遵守するため、プライバシー侵害に対する罰金を課し始めました。これにより、セキュリティ侵害やプライバシー侵害により、国家データ保護局 (ANPG) に数百万ドルが支払われると推定されています。

デジタル環境が進化し続ける中、中南米の政府と企業はサイバーセキュリティへの投資を優先し、将来の攻撃を防止し、その経済的影響を軽減するための強固な戦略を共同で開発する必要があります。

主な事業内容

セキュリティカルチャーを推進するにあたり、テクノロジー業界と保険業界は、医療・介護 & 製薬業界、小売・卸売業界よりも優れています。また、PPPが軒並み高いことからもわかるように、南米には大きな改善の余地があります。特に、小規模組織 (従業員数1～249人) と大規模企業 (従業員数1000人以上) のベースラインPPPは、世界の大半の他の地域と比較して高くなっています。

KnowBe4は、業界ごとの標準的な年間フィッシング統計に加え、毎年恒例のセキュリティカルチャーレポートも作成しています。 このデータは、さまざまなセクターに関する興味深い視点と背景を提供してくれます。ホテル・観光業界、教育業界、建設業界は最低の (70点) にとどまり、セキュリティカルチャーがあまり発展していないことを示しています。小売・卸売部門は (71点) と若干高いスコアとなりました。テクノロジーや保険といった業界は、それぞれ76点を記録し、より先進的で進化したセキュリティカルチャーを示しています。

総合スコアが (73点) の中南米は、セキュリティカルチャーの面で大きな課題に直面しています。しかし、チリ (71点) 、コロンビア (77点) 、ブラジル (72点) が高い得点を獲得しており、他の国よりも高いレベルのセキュリティカルチャーを示していることは注目に値するでしょう。

中南米で活動する企業は、ほとんどの国でセキュリティスコアが低いことから、セキュリティカルチャーを改善するための積極的な対策を講じる必要があります。セキュリティの脅威が進化し、より巧妙になるにつれ、人と資産の安全と保護を確保するためのセキュリティ対策を優先することが極めて重要です。

文化の受容と一般的な意識

中南米のサイバーセキュリティでは、文化の受容と一般的な意識が重要な役割を果たしています。近年、この地域ではサイバー攻撃が大幅に増加しています。この増加は、企業と個人のセキュリティ態勢を強化するために、積極的なセキュリティカルチャーを醸成することの重要性を浮き彫りにしています。

文化の受容とは、人々や組織がサイバーセキュリティの慣行や技術を受容し、利用する度合いを意味します。中南米では、サイバーセキュリティの脅威に対する認識と理解が一般的に不足しており、その結果、文化の受容レベルが低いという結果を生み出しています。

しかし、この地域では、サイバー攻撃に関連するリスクを認識する人が増えるにつれ、サイバーセキュリティに対する考え方が変わりつつあります。政府や企業はサイバーセキュリティ対策への投資を増やし始めており、個人もオンライン上で身を守るための対策を講じ始めています。

コスタリカの法律のように、健全かつ有益な取り組みが生まれつつあります。これは、サイバー社会に法的保護を提供するために改正されたもので、この法によって、これまで法律で対処されていなかった違反行為を個人が報告できるようになりました。

結論

- ✓ **2022年の中南米で増加する携帯電話の盗難に関する問題は、モバイル機器に保存された機密データを保護する必要性を浮き彫りにしています。**個人は、強固なパスワードや生体認証を使用し、リモートワイプ機能を有効にし、セキュリティアプリをインストールしてデバイスを保護すべきでしょう。さらに、政府と法執行機関は協力して、携帯電話の盗難に関連する組織犯罪に取り組み、国民にリスクと防止策を知らせる啓発キャンペーンを行うべきです。
- ✓ **高度な暗号化技術、二要素認証 (2FA) 、ハードウェアキーの導入は、デジタル資産の保護を大幅に強化し、**サイバー犯罪の成功がますます困難になります。便利で使いやすいハードウェアキーは、さまざまなシステムやプラットフォームに簡単に統合できるため、あらゆる技術的背景を持つユーザーにとって利用しやすい選択肢となります。
- ✓ **セキュリティ意識向上への投資は、強固なセキュリティカルチャーを醸成し、**潜在的なサイバー脅威を特定・回避・報告するための知識とツールを従業員に提供することで、最終的にセキュリティ侵害のリスクを最小限に抑えることができるため、組織にとって極めて重要なものです。包括的なトレーニングと継続的な教育を提供することで、企業はヒューマンエラーや過失の可能性を大幅に減らすことができます。

南アメリカ	ベースライン	90 日	1 年
1-249	34%	23%	6.4%
250-999	27.7%	25.8%	10.2%
1000+	49.5%	18.7%	5.1%
全組織規模での平均PPP	41.1%	21.3%	6.9%

アジア

Jacqueline Jayne

最も一般的な問題

2023年 IBM脅威インテリジェンス・インデックスでは、「アジア太平洋地域が2022年中に最も多くのサイバー攻撃に遭遇し、2022年に監視された全インシデントの31%をアジア太平洋地域が占めた」ことが報告されています。

中でもトップである日本は、2022年にEmotet（エモテット）というマルウェアの攻撃を受け、大きな打撃を被りました。警察庁の発表によると、2022年のサイバー犯罪件数は12,369件（2021年の160件から増加）と過去最高を記録しています。

ビジネスメール詐欺（BEC）や分散型サービス妨害攻撃（DDOS）を介した恐喝などが、日本全体で多く報告されています。

2022 Thales Data Threat Report, APAC Edition (2022年タレス データ脅威レポート APAC版)によると、回答者の45%が攻撃件数の増加を報告し、興味深いことに77%が、企業が自分の個人データを扱うことに信頼を寄せていると回答しています。世界の他の地域と同様、データ漏洩は一般的に起こっており、回答者の50%がデータ漏洩を経験したことがあると報告、そのうちの32%が2022年に発生しています。

全体のPPPを見ると、すべての企業規模において、世界の割合に近い結果が出ています。従業員数1,000人以上の大企業が、日本全体の割合よりも高いスコアでリードしているのは心強いことです。これは、企業の規模が大きくなるほどIT部門を備え、サイバーセキュリティチームが機能しているという事実に起因するものでしょう。これら2つの要因により、サイバー脅威の状況に対する理解が深まり、より良い意思決定を行うためのエンドユーザーのスキルアップの必要性に注目が集まると思われます。

経済効果

The State of Financial Crime 2022では、Key Takeaways for Asia Pacific Firms (金融犯罪の現状2022：アジア太平洋地域の企業に関するまとめ)の中で、国連薬物犯罪事務所（UNODC）は、日本のサイバー犯罪が600%増加したと報告されています。

東南アジア（インドネシア、マレーシア、フィリピン、シンガポール、タイ、ベトナム）については、PWCs Global Economic Crime and Fraud Survey 2022において、インシデントの3分の2が従業員を巻き込んだものであり、そのうち34%が5万ドル未満、10%が100万ドルから500万ドルの間、9%が500万ドル以上の損失を被ったと報告されました。

主な事業内容

アジア太平洋地域は43億人の人口を擁しています。10か国以上から成る世界で最も多様な地域の一つであり、世界のデジタルと社会の発展の頂点に立つ経済圏を有しています。事業内容は、個人経営、中小企業、大規模企業などがあり、世界中のあらゆる企業と同じ課題を抱えています。

文化の受容と一般的な意識

2022 Thales Data Threat Report, APAC Edition (2022年タレス データ脅威レポート APAC版) でアジア地域全体の一般的な見解を探ったところ、リモートワークの時代は今後も続き、それに関連するリスクも続くことがわかりました。リモートで働く従業員のセキュリティリスクは2022年においても続いて見られ、、回答者の33%が「非常に懸念している」、47%が「ある程度懸念している」と答えています。

結論

以下の項目に関しては、達成すべき課題が多くあると考えられています。

- ✓ 数の多いことは強みであり、官民は地域全体で協力する必要がある
- ✓ すべての企業/組織は、その規模にかかわらず、一貫した指導と支援が必要である
- ✓ 継続的な模擬フィッシングメール機能のある適切かつ学習意欲を高めるセキュリティ意識向上トレーニングを実施することで、望ましい結果をもたらすことができる

全体のPPPを見ると、すべての企業規模において、世界の割合に近い結果が出ています。従業員数1,000人以上の大企業が、日本全体の割合よりも高いスコアでリードしているのは心強いことです。

アジア	ベースライン	90 日	1 年
1-249	32.6%	20.9%	7.3%
250-999	33.2%	19.6%	7.4%
1000+	28.8%	13%	6%
全組織規模での平均PPP	30%	14.9%	6.5%

オーストラリア・ニュージーランド

Jacqueline Jayne

最も一般的な問題

例年と同様、フィッシングはサイバー犯罪の最も成功した攻撃ベクトルであり、その中でもランサムウェア、詐欺、金融・個人情報窃盗、ビジネスメール侵害 (BEC) が最も高い割合で行われています。

オーストラリアン・サイバー・セキュリティ・センター (ACSC) の Annual Cyber Threat Reportは、76,000件以上のサイバー犯罪の報告を受けています。これは7分に1件の割合で発生しており、前年度の67,500件から13%増加しています。

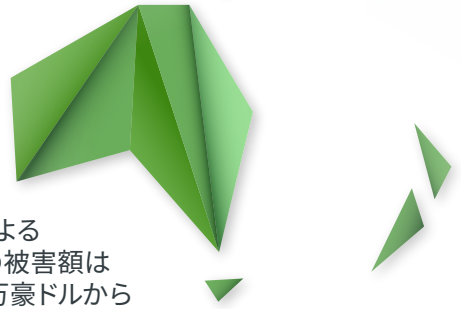
オーストラリア情報委員会 (OAIC) によると、2022年7月1日から2022年12月31日までの間、データ漏洩の届出が26%増加しています。届出の多かった上位5部門は、医療サービスプロバイダーで71件、金融 (スーパーアニュエーションを含む) で68件、保険で42件、法律・会計・管理サービスで37件、人材紹介会社で35件であったと発表されました。情報漏洩に関与する個人情報の中で最も一般的なのは連絡先情報となっています。

ニュージーランド

CERT NZによると、2022年に報告されたインシデントは8,160件で、2021年から8%減少しています。ニュージーランド全体では個人、中小企業、大規模企業でインシデントレポートが提出されています。

上位のインシデントを見ると、フィッシングとクレデンシャル・スタッフィングが2021年から16%増加、詐欺行為は2021年から15%増加、不正アクセスは2021年から23%増加しています。興味深いことに、2021年以降、マルウェアの報告は88%の減少を見せました。2021年は、FluBotマルウェアの攻撃が非常に多く発生したことが報告されています。

最近では、100万件を超えるニュージーランドの記録がサイバー犯罪者によって入手されたというデータ流出が注目を集め、プライバシーとデータ保持が大きな問題として浮上しています。



経済効果

オーストラリア

オーストラリア競争・消費者委員会 (ACCC) によると、2022年にオーストラリアで発生した詐欺の被害額は5億2,629万2,444豪ドル (2021年の3億2,300万豪ドルから増加) であったという驚くべき金額が報告されています。なお、これらはACCCに報告された詐欺に過ぎず、実際の総額はもっと多い可能性があるでしょう。

ビジネスの観点から、ACSCのAnnual Cyber Threat Reportは、サイバー犯罪報告1件あたりの平均コストが、中小企業で3万9,000豪ドル以上、中堅企業で8万8,000豪ドル以上、大企業で6万2,000豪ドル以上に増加したことも指摘しています。BECによる財務上の損失は9,800万豪ドル以上に増加し、オーストラリアの企業は全国のサイバーセキュリティ事件による損失を330億豪ドルであったと自己申告しています。

オーストラリア・ニュージーランド	ベースライン	90 日	1 年
1-249	27.1%	21.1%	6.3%
250-999	30.9%	19.9%	7.7%
1000+	41.1%	15.3%	5.4%
全組織規模での平均PPP	34.8%	17.8%	6.4%

ニュージーランド

ニュージーランドの銀行の報告によると、今年 (2022年) 、詐欺によって顧客が被った被害総額は1億8,350万ニュージーランドドルで、これは昨年 (2021年) より40%増加しています。

国家サイバーセキュリティセンターの2021/2022 Cyber Threat Reportによると、国家サイバーセキュリティセンターは、ニュージーランドの国家的に重要な企業や組織に対する3,300万ニュージーランドドル相当の被害を未然に防いでいます。さらに、「記録された350件のインシデントのうち23%が、犯罪行為や金銭的動機のある行為者との関連を示していた」ということです。

主な事業内容

オーストラリア

2022年6月30日現在、オーストラリアでは256万9,900の企業や組織が活動し、その大半を中小企業 (SME) が占めています。オーストラリア統計局によると、中小企業の内訳は、97.5%が小規模企業 (従業員0〜19人) 、2.3%が中規模企業 (従業員20〜199人) で、従業員200人以上の企業は残りの0.2%となっています。

ニュージーランド

2022年2月現在、ニュージーランドには59万2,700の企業があります。その中でも従業員数が0〜19人の小規模企業が97.13%と大半を占め、従業員20〜49人の企業が1.85%、50〜99人が0.57%、100人以上が0.45%となっています。

文化の受容と一般的な意識

オーストラリア・ニュージーランド

2022年はデータ漏洩が大きなニュースとなり、オーストラリアとニュージーランドでは何百万人ものデータが重大な事件に巻き込まれました。しかしながら、このインシデントの発生後も、IT部門の意思決定者は企業に及ぼすリスクについて考え方をほとんど変えていないようです。最新の調査でも、オーストラリアでは37%、ニュージーランドでは32%のIT意思決定者が、フィッシングが企業のリスクとなることを懸念していると回答しています。サイバー犯罪において、フィッシング攻撃を使って企業に侵入する割合が極めて高いことを考えれば、この数値はもっと高くあるべきでしょう。

結論

サイバーセキュリティ責任者の回答を見ると、オーストラリアとニュージーランドのITリーダーおよび企業が、セキュリティ問題に関する指針を求めていることは明らかです。
以下の項目に関しては、達成すべき課題が多くあると考えられています。

- ✓ 基本的なサイバー衛生についてすべての人を教育することは、意識を高めるための最重要課題である
- ✓ 企業や組織の規模にかかわらず、すべての企業/組織が対象であるため、一貫した指導と支援を行う
- ✓ 継続的な模擬フィッシングメール機能のある適切かつ学習意欲を高めるセキュリティ意識向上トレーニングを実施することで、望ましい結果をもたらすことができる

結論

新しい形態のセキュリティ意識向上トレーニング「NEW SCHOOL」の価値

調査の3つすべてのフェーズの結果から、いくつかの結論を得ました。

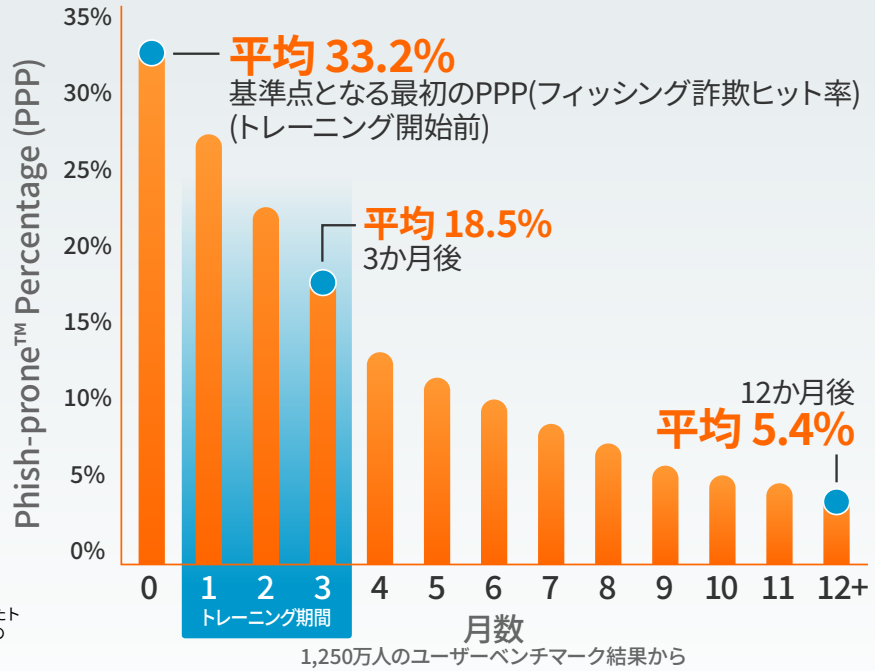
- **「New School」と呼ばれるセキュリティ意識向上トレーニングを実施しなければ、どんな組織でも重大なリスクが発生します。**トレーニング前の全業種の平均PPPが33.2%ということは、組織の1/3の従業員がいつ何時、ソーシャルエンジニアリングやフィッシング攻撃の被害を受けるか分からないということです。
- **どんな組織でも3か月あれば、エンドユーザートレーニングを通してセキュリティ強化を達成できます。**効果的なトレーニングプログラムを持っている組織では、急ピッチで模擬フィッシング攻撃とソーシャルエンジニアリング教育を定期的に実施することが可能です。
- **セキュリティ意識向上のためのトレーニング計画を効果的に進めることで、全組織は短期間で大きな成果を上げることが可能です。**
企業リーダーの中には、組織内でセキュリティトレーニングを思うように進められずに苦慮している人もいますが、これはたいして驚くことではありません。トレーニングを展開する前に、リーダー側で目標の分析・評価と組織全体の計画策定を行うことで、導入に向けての準備をしっかりと整えることができます。

リーダー側での確認ポイント

セキュリティ／リスク管理リーダーの方々は、組織内でのセキュリティ全体に対する行動を良い方向に変えるために、導入するプログラムには以下の要素が必要であることを理解しておきましょう。

- 指示が明確に定義・伝達されていること
- 組織のセキュリティポリシーと足並みがしっかり揃っていること
- セキュリティカルチャー全体とセキュリティの人的レイヤーに密接な関わりを持っていること
- リーダーからの充実したサポートがあること

リーダーからの手厚いサポートが日常的に得られない企業や組織内では、セキュリティに対する意識を向上させることはまず不可能です。

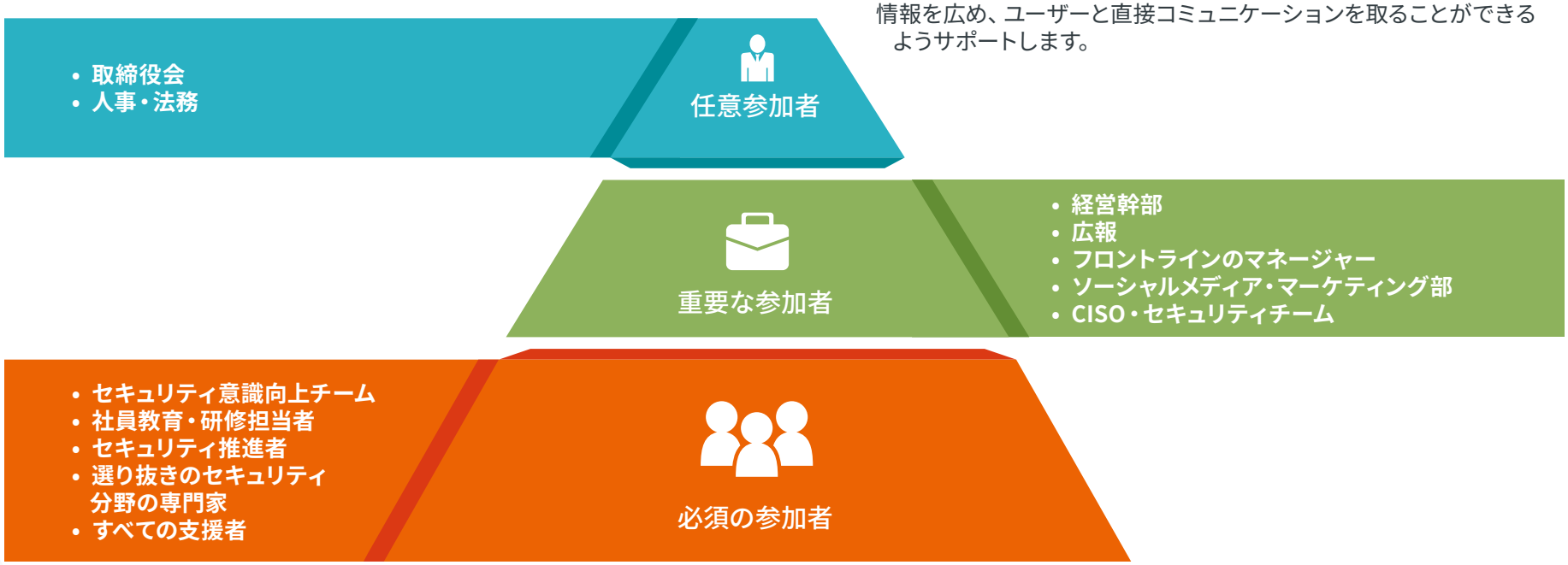


出典：2023年のKnowBe4業界別フィッシングベンチマーキングレポート

注： PPPの初期値は、評価対象の全ユーザーに基づいて算出されています。これらのユーザーは、評価前にKnowBe4コンソールを使ったトレーニングを一切受けていません。その後の各期間の数値は、全ユーザーのうちKnowBe4コンソールでトレーニングを受けたユーザーのPPPを反映しています。

プログラム成功のカギを握るポイント

- **セキュリティカルチャーを醸成する:** 組織のセキュリティインフラにおいて、最も重要なのは人的要因です。すべての従業員は、サイバー攻撃から組織と自分自身を守るために自分の役割と責任が何であるかを理解する必要があります。KnowBe4が定義する「セキュリティカルチャー」とは、組織のセキュリティに影響を与える考え方、慣習、社会的行動のことです。経営陣は、セキュリティ意識向上プログラムとトレーニングプログラム、ユーザーの準備レベルの両方に投資することで、セキュリティに対応できる環境を作り上げなければなりません。
- **模範を示す:** 組織に正しい行動を求めるのであれば、リーダーが率先して範を示す必要があります。組織全体でセキュリティ意識向上を推進させるために、あらゆる面に積極的に関わることが重要です。他の従業員と同じようにセキュリティ意識向上トレーニングを受けて終了するなどの要件を満たす必要があります。
- **プロに任せる:** セキュリティ意識向上に関するコンテンツは他に類を見ないものです。専門知識があるプロを起用することで、コンテンツの設計がうまくいくだけでなく、それを通じて前向きで楽しめる学習体験が生まれ、最終的には従業員が自らセキュリティ上安全な行動を取れるという望ましい状態を作り出すことができます。コンテンツが極めて重要な役割を果たす業界では、さまざまな学習スタイルにアピールできるバリエーションに富んだ多種多様なコンテンツを配信するベンダーと連携することをお勧めします。選べる学習スタイルが1つに限られていると、ユーザー体験、習得できる知識量、全体的な知識保持率などはどうしても低下します。このようなプログラム開発には、社内のトレーニング組織を活用するか、あるいは万能なアプローチを提供するベンダーと提携するなどの策を講じると良いでしょう。どちらのオプションも、学習者のセキュリティ関連の思考や行動を形成するまでにはそれなりの期間がかかります。
- **マーケティング的思考を持つ:** コンテンツおよび模擬フィッシングキャンペーンと並行して、補助教材 (ポスター、デジタルサイネージ、ニュースレターなど) の形で関連メッセージを頻繁に発信し、異業種間の会議やプレゼン中にも適切なタイミングで重要なチェックポイントを繰り返し折り込みましょう。従業員向けの「ランチミーティング」やリーダーシップ会議中の「机上演習」を行うことで、出席者が気軽に意見交換しながら情報を広め、ユーザーと直接コミュニケーションを取ることができるようサポートします。



- **セキュリティの「カルチャーキャリア」プログラムを動かす:** セキュリティ／リスクプログラムの大半は、グローバル組織と適切に対応する上で必要なリソースが欠如しています。セキュリティの「カルチャーキャリア」プログラムは、「セキュリティ チャンピオン」、「セキュリティ アンバサダー」、「セキュリティ リエゾン」、「セキュリティ インフルエンサー」など別の名前でも知られています。名前はどうであれ、カルチャーキャリアプログラムは、組織内にアドボケイトチームを分散させることで、地域レベルでセキュリティメッセージと学習を強化するための取り組みです。誰が責任を持ってプログラムを進めるのかも重要になります。従業員の多くは、より良いセキュリティ行動を推進するのは自分以外の誰かの責任であると思い込んでいます。マネージャーによる推薦またはボランティアを通してローカルインフルエンサーを登録することで、頼れるセキュリティネットワークチームを形成し、地域に密着したセキュリティカルチャーの醸成を開始することができます。
- **模擬フィッシングテストをプログラムに追加する:** この調査からもわかるように、定期的な模擬フィッシングキャンペーンをセキュリティ意識向上プログラム全体に加えることで、従業員の不審メールの見極め力を高め、攻撃被害を減らすことができます。
- **テストの頻度を増やす:** セキュリティは、どんなときも強化されているか脆弱になっているかの2択しかありません。当社の調査では、望ましい行動変容が見られない大半の組織は、プログラム (コンテンツと模擬フィッシングの両方) の実施頻度が年一回、年二回、または年四回に限られていました。テスト頻度が極端に少ないと、その時点でのベースラインテストを実施しているに過ぎず、有意義な比較結果は得られません。従業員には、コンテンツと模擬フィッシングキャンペーンを月一回 (高リスクの標的に対しては月二回) 配信することをお勧めします。サイバー攻撃かどうかを見極めるための適切な条件付けを従業員に習得してもらい、そこから行動変容を定着させるためには、定期的なペースでのテスト実施が不可欠です。セキュリティ／リスク管理チームは、「この頻度は多すぎないか」と不安を抱くかもしれませんが、実際には、頻繁にテストを行うことでセキュリティのマッスルメモリーを効果的に鍛えることができます。これにより、絶えず変化を続ける現代および将来的な攻撃手法に対処することが可能となります。さらに、人間の検知と対応は、セキュリティ意識のリアルタイムコーチングの一部であり、人間のセキュリティ上の危険な行動をその都度検知し、対応することを重視します。セキュリティ意識向上トレーニングを強化し、リスクのあるユーザーの行動を追跡することで、企業はセキュリティリスクを把握することができます。
- **適切な人材を雇用する:** セキュリティ意識向上プログラムは、多くの場合、誰もしたがらない仕事を任せられたか、少し時間に余裕があってこの「トレーニング」に付き合わされることになったセキュリティ実務者によって進められるケースが多くあります。しかし、このようなプログラムの運営には一定の経験とノウハウが必要です。学習を通して組織開発と行動変容を促進する方法について意識をしっかりと持ち、順応性が高いクリエイティブな候補者を採用しましょう。
- **目標を定義する:** プログラムの成功基準は何か、そしてそれに対してどのように測定するかを前もって判断しておきましょう。そうでなければ、プログラムの効果を測定し、固有の価値を判断することはできません。
- **効率よく測定する:** システムや従業員、データを保護する上では、望ましい行動を強化する指標を用いることが重要です。測定基準はついつい多く選んでしまいがちですが、その場合、時に関係のない領域を測定したり、組織的成果が期待外れに終わってしまうことがあります。頻繁に数値化し、要件を満たすことができる測定可能データとトレーニングを活用することが最も重要です。さらに、プログラムに使用する指標が、組織全体のセキュリティ目標だけでなく、企業目標にもつながっていることを確認しておきましょう。
- **従業員のモチベーションを上げる:** 従業員が必要なトレーニングを完了し、セキュリティポリシーを遵守し、安全に関して望ましい行動を継続するよう促すために、正の強化と負の強化を意図的に一貫した方法で実践しましょう。動機づけを行うことで説明責任を向上させ、より安全な企業文化を推進するための従業員の全体的な役割を高めることができます。

さあ始めよう！

KnowBe4は、金融、エネルギー、ヘルスケア、保険など多数の分野においてサイバーセキュリティを改善するために、何万人ものITプロフェッショナルを支援しています。

KnowBe4は、業界一のフィッシングシミュレーションとトレーニングプラットフォームを利用し、組織の防御の最終ラインである**ヒューマンファイアウォール**（「人」による防御壁）の改善を目指しています。

私たちは、お客様である企業の従業員が、毎日セキュリティに関してより賢明な判断を下せるようにサポートします。データドリブンなITセキュリティ対策プランの実現に向けてまずなすべきことは、組織内で「発生する」可能性の高い脅威に対処することです。この脅威こそが実は従業員なのです。KnowBe4を採用すれば、こうした脅威に立ち向かうことができます。では早速始めてみましょう。

ユーザーへのフィッシングテスト実践のための4つのステップ

テストとトレーニングを通して企業・組織のセキュリティの脆弱性を大幅に削減し、エンドユーザーの行動を変えていくことができます。次に示すステップに従い、ヒューマンファイアウォールを形成してセキュリティ体制を強化しましょう。

1. **ベースラインテストの実施:** セキュリティ意識向上トレーニングの必要性を上層部に訴えるための最初のステップは、ベースラインテストを実施することです。このベースラインテストによって、ユーザーのPPP（フィッシング詐欺ヒット率）を分析・評価します。これは、今後改善されたどうかを測定するのに必要なデータでもあります。

2. **ユーザーのトレーニング:** 旧式のPowerPointスライドではなく、学習意欲を高めるインタラクティブなコンピューターベースのオンデマンドトレーニングを使用します。意識向上モジュールと動画を利用することで、フィッシングやソーシャルエンジニアリング攻撃がどのように発生する可能性があるかについて、ユーザーへの教育を行います。

3. **ユーザーへのフィッシング:** 少なくとも月に一度は全ユーザーにフィッシングテストを実施してトレーニングを強化し、学習プロセスを継続します。考え方を訓練し、新しい習慣を身につけることがポイントです。新しく学んだことを実行に移すまでには少し時間がかかります。模擬ソーシャルエンジニアリングテストを少なくとも月に一度実施すれば、ユーザーの行動を効果的に変えていくことができます。

4. **結果の測定:** トレーニングとフィッシングテストの両方に対する社内での成果を追跡します。目標はPPPの値をできるだけゼロに近づけることです。

マーケター目線で計画し、攻撃者のごとくテストする

リスクを低減するための鍵は、従業員のPPPをターゲットにして施策を推進することです。以下では継続的な変化をもたらすことができるベストプラクティスをいくつかご紹介します。

実社会で起こりうる攻撃方法を使用する

模擬フィッシング演習は実際の攻撃と手口を模倣したものでなければ意味がありません。そうでないと、「トレーニング」であっても、組織に間違った安心感を植え付けるだけです。

単独では行わない

人事やIT、コンプライアンスチーム、さらにはマーケティングなど他のチームとエグゼクティブにも参加してもらい、組織全体で信頼できるセキュリティカルチャーを構築しましょう。

すべてをトレーニングしようとしない

どのような行動を形成したいかを決め、上位2、3位に優先順位をつけます。その上で、選んだ行動を12～18か月かけて変えることに意識を集中します。

関連性を持たせる

誰でも自分にとって意味があることに関心があるものです。模擬テストが従業員の日々の業務に影響を与える要素を含んでいるかを確認しましょう。

プログラムをマーケティングキャンペーンだと見なす

セキュリティを強化するには、従業員に知ってほしいことを伝えるだけでなく、行動自体を変えることに焦点を当てる必要があります。必要に応じて重要な情報を従業員に与えてもかまいませんが、反射的に行動に移せるように調整することを意識し続けましょう。従業員が、サイバー攻撃を防御するための効果的な最終ラインであることを忘れてはいけません。

著者

Anna Collard KnowBe4 Africaコンテンツ戦略 シニアバイスプレジデント兼エバンジェリスト

Joanna Huisman KnowBe4戦略的インサイト & リサーチ シニアバイスプレジデント

Jacqueline Jayne (JJ) KnowBe4 アジア太平洋地域担当セキュリティ意識向上アドボケート

Erich Kron KnowBe4 セキュリティ意識向上アドボケート

Javvad Malik KnowBe4ロンドン セキュリティ意識向上アドボケート責任者

Rafael Silva KnowBe4 情報セキュリティ シニアディレクター

Jelle Wieringa KnowBe4 ヨーロッパ、中東・アフリカ (EMEA) 担当セキュリティ意識向上アドボケート

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訓練・分析を組み合わせた世界最大の統合プラットフォームのプロバイダーです。サイバーセキュリティにおいて人的要素は見落とされがちです。KnowBe4は、このことを察知し、包括的な新しい形態のセキュリティ意識向上トレーニングプログラム (当社では「New School」と呼んでいます) を通して、企業や組織がソーシャルエンジニアリングの問題を管理できるようにするために設立されました。

これは、本番さながらの偽装攻撃によるベースラインテスト、学習意欲を高めるインタラクティブなトレーニング、模擬フィッシング攻撃を通した継続的なアセスメント、およびエンタープライズクラスの最強のレポーティングを組み合わせた統合型のアプローチです。

金融、医療・介護、エネルギー、官公庁、保険業など規制の厳しい分野を含むあらゆる業界で、多くの企業や団体がKnowBe4のプラットフォームを採用し、防御の最終ラインとしてヒューマンファイアウォールを構築して、日々求められるセキュリティ上の的確な意思決定を可能にしています。

その他のリソース

無料のフィッシング攻撃テスト
ユーザーをテストし、フィッシング攻撃の被害に遭いやすい従業員の割合を、無料のフィッシングセキュリティテストで調べましょう。

自動セキュリティ意識向上プログラム
各企業向け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を作成します。

無料のPhish Alertボタン
従業員がフィッシング攻撃を発見した場合、このボタンをクリックするだけで安全に報告することができます。

無料不正メールチェック
攻撃者に発見される前に、流出したメールを特定できます。

無料ドメインスプーフテスト
組織のドメインを使うメールアドレスがスプーフィング攻撃を受けてないかを確認できます。

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
電話: 03-4586-4540 | www.KnowBe4.jp/www.KnowBe4.com | Email: Info@knowbe4.jp