KnowBe4

効果的なセキュリティ意識向上トレーニングは、データ侵害を減少させる

Effective Security Awareness Training Really Does Reduce Breaches

ロジャー・A・グライムス、
マーティン・クレーマー博士
共著

効果的なセキュリティ意識向上トレーニングは、データ侵害を減少させる

目次

人的リスクの軽減

KnowBe4は、70,000社を超えるユーザー企業／組織から得た10年以上の実データから模擬フィッシングキャンペーンを含む優れたセキュリティ意識向上トレーニング（SAT）プログラムが、人的サイバーセキュリティリスクを大幅に低減することを確認しました。また、多くのエンドユーザーにとって、セキュリティトレーニングや模擬フィッシング演習はなるべくなら受けたくないという傾向がありますが、KnowBe4は効果的なSATプログラムがこのようなエンドユーザーの抵抗感を解消すると同時に、継続的なSATトレーディングが生み出す効果的なヒューマンリスク管理プログラムが組織の現実世界での侵害の可能性を減らすとデータで示しています。

本稿では、人的リスクを低減することの重要性、特に効果的なSATプログラムを使用することの重要性を示し、実際のユーザーから得られたデータ分析により、人的リスク要因を大幅に低減する効果に加えて、効果的なSATプログラムを実施することで、現実世界のデータ侵害リスクを低減できることを紹介します。

サイバー攻撃の70%～90%はソーシャルエンジニアリングによるもの

サイバーセキュリティのインシデントのほとんどは、ソーシャルエンジニアリングや、より具体的にはフィッシングなど、人為的なミスが関わっています。これは新しいことではありません。コンピューターが誕生して以来、ソーシャルエンジニアリングは悪意のあるハッキングを実行するための、悪意のある行為者の第一の方法でした。

ソーシャルエンジニアリングとは、誰か（またはグループ）が、誰か（友人、など）、何か（警察、税務）、または有名なブランド（マイクロソフト、PayPal、銀行など）を装って、悪意を持ってあなたをだまし、あなたの利益を損なうような行為をさせようとすることです。ログイン機密情報を提供させたり、仕掛けられた文書をダウンロードさせたり、マルウェアを実行させたりします。

ソーシャルエンジニアリングとフィッシングの違い

ソーシャルエンジニアリングとフィッシングの違いとは？ ソーシャルエンジニアリングとフィッシングについて、世界的に合意された「公式」な定義はありませんが、ソーシャルエンジニアリングは、「人」の心理的な隙や行動のミスを利用して、攻撃者が巧みに仕掛ける不正工作と定義されています。一般に、人と人との社会的関係を悪用する騙しの手口の総称をソーシャルエンジニアリングと呼ぶことから生まれたものです。一方、フィッシング(Phishing)は、メールを餌にして釣ることから、「fishing(釣り)」が語源となっていますが、「餌」として利用されているメールなどの騙すための手口が洗練されていることから「sophisticated(洗練された)」の「ph」を「fishing」の「fi」と置き換えて「Phishing」と綴ったことがフィッシング(Phishing)の由来です。フィッシングは、ソーシャルエンジニアリング攻撃の1つです。電子メールやSMSを利用して、人の心理的な弱点を突き、機密情報を漏えいさせたり、悪意あるリンクをクリックさせたりするサイバー攻撃です。フィッシングという言葉は、インターネットのデジタル時代に生まれました。また、悪意のあるサイバー攻撃の根本原因の分析では、ほとんどの情報ソースはフィッシング（多くの場合、オンラインデジタルメディアを含む）をソーシャルエンジニアリングのサブセットとして分類しています。また、ソーシャルエンジニアリングは物理的な紙の郵便物やその他のデジタルでない方法を使って人為的に起こりえます。数十年にわたる調査研究により、悪意のあるデータ侵害の70%から90%がソーシャルエンジニアリング(https://www.knowbe4.jp/blog/if-social-engineering-is-70-90-of-attacks-why-arent-we-acting-like-it)とフィッシングに関与していることが一貫して示されています。悪意のあるサイバー攻撃の他の根本原因（例えば、パッチが適用されていないソフトウェアやファームウェア、盗聴、暗号攻撃、物理的な攻撃など）は、これには全く及ぶものではありません。実際、サイバー攻撃を成功させる他の原因をすべて合計しても、ソーシャルエンジニアリングとフィッシングに達するものではありません。

注：ソーシャルエンジニアリング、フィッシングに次いでサイバー攻撃を成功させる2番目の要因が、ソフトウェアやファームウェアの脆弱性の悪用です。GoogleのMandiantによると、ソフトウェアやファームウェアの脆弱性の悪用は全データ侵害の33%を占めています(https://www.action1.com/patching-insights-from-kevin-mandia-of-mandiant/)。しかし、この2番目の要因は、他のすべての初期アクセス攻撃手法を合計しても10%にも達しません。

実施された調査、使用された分類法、対象者によってはソーシャルエンジニアリングがサイバー攻撃に関与している割合は40%程度と少ないという報告や研究を目にすることがあります。しかし、ソーシャルエンジニアリングとフィッシングは、たとえその割合が70%～90%より少ないとしても、攻撃者が使用する悪質なハッキングの最も一般的な手法であることが、ほぼすべての調査で示されています。

KnowBe4のリードセキュリティアウェアネスアドボケイトであるJavvad Malikは、Kaspersky、Securelist、ESET、McAfee、Trend Microなど、セキュリティ業界の有名企業による調査レポートを含む4の異なるベンダーと情報ソースから脅威インテリジェンス情報を含む100種類のサイバーセキュリティレポートをダウンロードし、メタ分析を行いました。KnowBe4のJavvad Malikは、その結果をホワイトペーパー（英文）にまとめています。(https://www.knowbe4.com/hubfs/UsingThreatIntelligencetoBuildDataDrivenDefense.pdf) が、これらのレポートのほとんどすべてが、ソーシャルエンジニアリングとフィッシングを第一位のサイバー脅威であると報告していると指摘しています

その他、多くのレポートがソーシャルエンジニアリングとフィッシングの脅威について報告しています。以下に、そのいくつか紹介します。

- 2023年8月、コムキャストは、同社の顧客に対する攻撃の89.46%がフィッシングから始まったと報告しています。このレポート全体はこちらで読むことができます。https://business.comcast.com/community/docs/default-source/default-document-library/ccb_threatreport_071723_v2.pdf.
- ソーシャルエンジニアリングとフィッシングは世界的な問題でとなっており、英国の政府公式統計サイバーセキュリティ侵害調査2022（https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022）は、「..最も一般的な脅威のベクトルは、フィッシングの試み（83%）であった」と報告しています。
- InfoBloxの2022 Global State of Security Report (https://files.scmagazine.com/wp-content/uploads/2022/05/Infoblox-Main-Report.pdf) は、「最も成功した攻撃手法はフィッシング（58%）」と報告しています。
- 2023年5月、バラクーダネットワークスは（www.barracuda.com/reports/spear-phishing-trends-2023）、スピアフィッシングがメールベースの攻撃全体の0.1%に過ぎないにもかかわらず、侵害成功の66%を占め、これは単一の根本原因としては最大である」と報告しています。

これは驚くべきことではありませんが、ハッカーやマルウェアの攻撃を受けたほとんどの人々や組織はソーシャルエンジニアリングやフィッシングが関与していたことを認識しています。

ランサムウェアとデータ侵害が最も被害の大きい攻撃である

マルウェア攻撃、認証情報盗難、データ流出、サービス妨害、物理的な盗難など、企業が被る可能性のあるサイバー攻撃にはさまざまな種類があります。しかし、この10年近く、ランサムウェア攻撃は、最も恐れられ、被害が大きい攻撃の1つとなって進化してきています。ほとんどのCISOは、ランサムウェア攻撃を最大の懸念事項として挙げており、この進化をたどれば、これは当然の経緯であると言うことができます。

ランサムウェア攻撃は、しばしば数週間から数ヶ月の業務中断を引き起こします。なかには、1年以上完全復旧に時間を要しているケースもあります。また、身代金を支払った場合、平均で数十万ドルから数百万ドルかかっているのが現状です（https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024 ）。ランサムウェアの復旧費用には、付帯経費として、さらに何百万ドルもかかることが稀ではありません。これに加えて、ランサムウェアは、長期的な風評被害、訴訟、規制当局からの罰金、さらには継続的なビジネスへの懸念など、他のどのタイプのサイバー攻撃よりも深刻な問題を引き起すのです。

ランサムウェア攻撃のほとんどはデータ侵害である

現在、ほとんどのランサムウェア攻撃は、機密データの流出（データ侵害など）を伴います。初期のバージョンのランサムウェアは、単にファイルを暗号化し、暗号化されたファイルを解除するための復号化キーを提供するために支払いを求めてきました。しかし、2019年11月から、ランサムウェア攻撃はデータ流出フェーズを含むようになり、関与する攻撃者は暗号化フェーズを実行する前に一部の機密データを流出させています。

そして、次のステップとして、攻撃者は、身代金を支払わなければ、盗んだ機密データを世界中、少なくとも他の攻撃者や被害者の競合他社に公開すると被害者を脅してきます。この「二重脅迫型ランサムウェア」攻撃は、バックアップが十分にあり、ランサムウェアの復号化得るために身代金を支払う必要性を感じていない被害者に身代金の支払いを強いるために考え出されました。権限のない第三者によって暗号化されていない機密データが流出することは、データ侵害にあたります。

今日、多くのサイバーセキュリティ企業によれば、ほとんどのランサムウェアはデータの流出も行っています。例えば、Artic Wolf (https://arcticwolf.com/resource/aw/the-state-of-cybersecuri-ty-2024-trends-report)によると、ランサムウェア攻撃の91%がデータの流出を含んでいます。また、Coveware社によると、この数字は75%と若干低くなっています（https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024 ）。言い換えれば、今日、データ流出が発生しなかったランサムウェアのインシデントは、幸運だと考えるべきです。

Coveware社は2024年7月30日付の四半期報告書の中で、身代金を支払うランサムウェア被害の43%は、被害者が攻撃中にデータを暗号化されたわけではないにもかかわらず、純粋にデータ流出を防止する理由に身代金を支払っていると解説されています（blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024）。

ランサムウェア攻撃の大半はソーシャルエンジニアリングが原因

ランサムウェアがデバイスやネットワークに侵入するあらゆる方法の中で、ソーシャルエンジニアリングは第一の方法です。KnowBe4は、これににについて、Ransomware Hostage Rescue Manual 2024（2024年度ランサムウェアレスキューマニュアル：ランサムウェア攻撃に備え、復旧するために知っておくべきこと）https://www.knowbe4.jp/hubfs/J_Ransomware-Rescue-Manual.pdf で解説しています。このランサムウェアの根本原因については、他の多くの情報ソースも同じ結論に達しています。例えば、最も普及している初期アクセス手法について、同様に、「2024 Microsoft Digital Defense Report」（https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/ja-us/microsoft-brand/documents/Microsoft%20)では、ソーシャルエジニアリング（メールフィッシング、SMSフィッシング、ボイスフィッシング）がトップであり続けるおり、個人情報の漏洩、公開アプリケーションやパッチが適用されていないオペレーティングシステムの脆弱性の悪用が続くと解説しています。

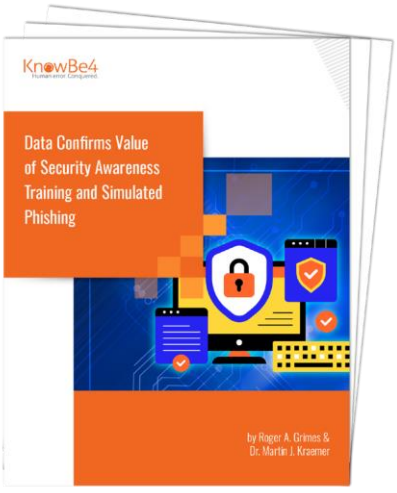
人的リスクは、セキュリティポリシー、テクノロジー防御（コンテンツフィルタリング、ファイル添付ブロッキング）、セキュリティ意識向上トレーニングを組み合わせることで、軽減することができます。この数十年にわたる試行錯誤を経て、ソーシャルエンジニアリングやフィッシングをブロックするには、ポリシーや技術的な防御だけでは不十分であることが証明されています。ソーシャルエンジニアリングとフィッシングがこれほど大きな割合で攻撃に関与しているという事実は、この種の攻撃がいかに簡単にポリシーや技術的突破してしまうかを示しています。

人的リスク、特にソーシャルエンジニアリングやフィッシング攻撃を減らすことは、どのような組織にもできるサイバーセキュリティ対策の一つであることは明らかだ。

この抜本的な対策プロセスとして、すべてのユーザーは、ソーシャルエンジニアリングやフィッシング攻撃の脅威に対するセキュリティ意識の向上のためのトレーニングを受け、それらを軽減し、適切に報告する方法を学ぶ必要があります。セキュリティ意識向上トレーニング（SAT）は、人的リスクを軽減する方法の一つに過ぎませんが、このプロセスの重要な部分です。

効果的なセキュリティ意識向上トレーニング（SAT）は人的リスクを軽減する

私たちは以前、「Data Confirms Value of Security Awareness Training and Simulated Phishing（データが実証する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演習の価値）」と題したホワイトペーパーで、模擬フィッシングを含む効果的なSATプログラムが模擬フィッシング演習で誤って反応する人の割合（私たちがPhish-prone™ PercentageまたはPPPと呼ぶもの）を減らすのに効果的であり、組織内でSATと模擬フィッシングが頻繁に行われれば行われるほど、PPPが下がることを示しました。詳細は、日本語版https://www.knowbe4.jp/hubfs/Data-Confirms-Value-of-SAT-WP_JP.pdf を参照してください。



また、以下に示すように、優れたSATプログラム（頻繁なフィッシング詐欺の模擬演習を含む）を実施している組織は、実際の人的リスクを低減し、現実世界でのサイバー攻撃被害が少ないことを証明するデータを提示しました。また、模擬フィッシングキャンペーンを頻繁に訓練、実施すればするほど、実際の人的リスクは減少することをデータで示しました。

注：KnowBe4は、効果的なSATプログラムとは、少なくとも毎月トレーニングが実施されるものであると考えます。KnowBe4は、さらに頻繁にトレーニングを行い、模擬フィッシング演習を行うことで、さらにリスクを軽減できることを実証しています。

問うべき究極の質問

SATプログラムの効果については、様々な考え方がありますが。問うべき質問は、ひとつしかありません。

模擬フィッシング演習を含む優れたセキュリティ意識向上トレーニング（SAT）プログラムは、実際の攻撃によって組織が危険にさらされるリスクを減らすことができるのだろうか？

他のあらゆる尺度では、なぜ効果的なSATプログラムが必要なのかという究極の目的を正確に反映できません。もし効果的なSATプログラムが私たちの期待通り本当に人的リスクを低減するのであれば、効果的なSATプログラムを実施している組織から、人的リスク低減による現実世界での被害が減少したという物証が得られるはずです。

この質問に客観的に答える最善の方法は、ある期間にデータ侵害を受けた組織と受けなかった組織に関する世界規模の大規模データを収集し、その調査結果を、人的リスクを軽減するために攻撃前に優れたSAT使用していたか、使用していなかったかと比較することです。

もし、有効なSATが実際に組織の侵害を回避するのに役立ったのであれば（相関関係と因果関係が証明されている場合）、有効なSATプログラムを導入している組織は、インシデントが発生する前にSATプログラムを導入していなかった、あるいはまったく導入していなかった組織よりも侵害される可能性が低いはずです。

> 注：効果的なSATプログラムを受けた対象者と、セキュリティトレーニングやテストを行わないよう指示されていない対象者から無作為に抽出して、構造化して比較分析を行わない限りは、確固とした科学的相関関係や因果関係を最終的に確認することは依然として困難です。

KnowBe4のチャレンジ

残念ながら、「データ侵害を受けたか受けていないか」、「データ侵害の前に適切なSATプログラムを導入していたかどうか」をAND条件で示す大規模なグローバル・データセットは存在していません。というのも、SATや模擬フィッシング演習をどの程度利用しているか、あるいは利用していないかを示す内部データはあるものの、通常、いつデータ侵害に見舞われたか、またそのデータ侵害がソーシャルエンジニアリングやフィッシングに関連するものであったかどうかは公開されないからです。さらに、顧客以外の企業については、データ流出があったかなかったか、SATプログラムや模擬フィッシングキャンペーンが充実していたかどうかの関連性を示すデータも存在していていません。

KnowBe4がチャレンジしたことは、私たちは入手可能なデータで構築できるこの種のデータセットを創出することでした。

> 注：この究極質問に答える最良のデータ分析を実施しましたが、すべての人を100%満足させるものではないことは承知している。しかし、この分析調査を通して、最も価値のある、最大のデータセットを作り出せたと考えています。

KnowBe4が実施したこと

最初に、Privacy Rights Clearinghouse (https://privacyrights.org/)から、公に知られている最大の漏洩組織リストを購入しました。Privacy Rights Clearinghouse (PRC)の情報漏洩データベースには、2005年以降に米国の組織が公表した17,500件以上の情報漏洩の記録が含まれており、誰でも450ドルで購入できます（https://privacyrights.myshopify.com/products/ data-breach-chronology-data-set）。

世界中に顧客を持つグローバル企業として、私たちはむしろ米国以外の組織や侵害を含むグローバルなデータベースを使いたいのですが、この米国だけのコレクションは、利用可能な公開侵害データベースとしては唯一最大のものです。ほぼ10年間にわたる侵害の、これほど近いものは他にはありません。当社がこのデータベースを購入した時点では、35,000件以上の個別のデータ侵害通知（17,500件の固有のデータ侵害イベント）がありました。多くの組織では、同じデータ侵害で複数のデータ侵害が公表されたり、複数のデータ侵害が公表されたりしています。

注：PRCのデータベースに登録されている1つの組織が異なるサイバーセキュリティインシデントによって複数の侵害を被ることは頻繁に起こることです。一度侵害を受けた企業は、繰り返し侵害を受けています。セキュリティ対策やセキュリティ対策の不備により侵害を受けた企業が、セキュリティ対策を徐々に改善していく中で再び侵害を受けることは想像に難くありません。

次に、私たちのはるかに大きな顧客リストをダウンロードし、PRCのレコードと比較分析しました。

分析と結果

KnowBe4を利用する米国顧客の大半（97.6%）は、（少なくとも2005年以降）公開されたデータ侵害に見舞われていません。分析実行時点で、KnowBe4の米国および海外の顧客数の合計は63,347社でした。

KnowBe4顧客分類	顧客数	%
米国内のKnowBe4顧客	50,010社	79.94%
米国外のKnowBe4顧客	13,337社	21.06%
KnowBe4顧客合計	63,347社	100.00%

注：現在2024年末現在のKnowBe4の顧客数は70,000人を超えています。

PRCのデータベースには、米国内の組織および米国内でのデータ侵害に関するデータしか含まれていないため、米国内の顧客50,010社だけを用いて分析を行う必要がありました。

PRCデータベースとKnowBe4顧客ベースとの名寄せ・照合

最初の分析は、KnowBe4の米国顧客がPRCのデータベースに何社掲載されているかを調べることでした。これは、PRCのデータベースに掲載されている顧客とKnowBe4の米国顧客が同一企業であるかを照合するための作業でした。組織名称による照合では、その社名にわずかな不一致があったり、逆に非常によく似た社名であっても別企業であったりすることがよくありました。この名寄せクエリーを通して、いくつかのバリエーションがあることを発見しました。この照合プロセスでは、名寄せのクエリーを何度か改良し、結果が正確かどうかをテストする必要がありました。私たちは、可能な限りベストな名寄せ精度を保証するためにこのプロセスを繰り返し実行しました。以下がその最終結果です。

KnowBe4顧客内訳	顧客数
KnowBe4 の米国顧客	50,010社
PRCデータベースに掲載のあるデータ侵害を受けたKnowBe4の米国顧客数	1,189社
PRCデータベースに掲載のあるデータ侵害を受けたKnowBe4の米国顧客%	2.37%

KnowBe4の顧客は侵害される可能性が極めて低い

この2.4%という調査結果は、ランサムウェアを含む何らかのデータ侵害を経験した組織の割合が、年や情報ソースにもよりますが、数十年前から報告されている調査結果（単年で約20%～69%）と比較すると、驚くべきものです。

データ侵害に見舞われているKnowBe4の米国顧客は僅か2.4%しかいません(2005年以降で)。

＜サイバーセキュリティ企業他社からのこれを裏付けるデータ例＞

- GetAppの2024年データセキュリティレポート(https://blog.knowbe4.com/44-us-organizationsexperienced-more-ransomware-attacks-last-year)によると、米国内企業の44%、米国外企業の51%が過去12カ月間にランサムウェア攻撃を経験しています。
- PonemonInstituteのA Crisis in Third-Party Remote Access Security Report（https://security.imprivata.com/rs/413-FZZ-310/images/IM_Report_Third-Party-Remote-Access-Security.pdf）には、回答者の52%が過去12ヶ月間にデータ侵害を経験したと記載されています。
- フォーチュン1000企業の40%が毎年データ侵害に見舞われるとの調査結果（https://www.bitdefender.com/en-gb/blog/businessinsights/40-of-fortune-1000-companies-will-suffer-a-breach-every-year-new-research-suggests)
- 2022年のCymulate社の調査（https://cymulate.com/news/breach-survey-pr-2022/）によると、回答者の40%が過去12ヶ月間に侵入されたことを認めています。一度侵入された後、侵入された回答者の66%がさらなる攻撃を受けたと回答しています。攻撃は主に（56%）エンドユーザーによるフィッシングから発生しました。

注:データ侵害のインシデントの総計は、これらのインシデントよりもはるかに大きいと考えられています。データ侵害の多くは公に報告されないません。その理由は報告義務がないためか、関係組織が単に報告しないことに決めたか、報告を怠ったためであると思われます。本レポートと以降の関係者比較では、データ侵害のインシデントを報告しない世界の企業の割合はKnowBe4の顧客ベースと同程度であると想定しています。

データ侵害を受けた組織の割合が最も低い20%という数字を例にとれば、KnowBe4の米国顧客がデータ侵害に見舞われる可能性は公開データ侵害リストに載るデータ侵害の可能性よりも、どの年度を見ても、8.3倍低い。

これは様々な理由によるものであり、KnowBe4のサービスとの関連や原因がある場合もあれば、ない場合もあります。しかし、どのような理由であれ、KnowBe4の米国顧客は、平均的な米国の組織よりも公に危険にさらされる可能性がはるかに低いのです。

SATのサービスを利用している顧客は、そうでない企業よりも人的リスク、ひいてはすべてのサイバー攻撃を軽減することに長けている可能性があります。ただし、顧客によっては顧客になる前にすでに優れたヒューマンリスク軽減の実績を持つこともあります。これを明確にするためには、KnowBe4の顧客になる前または後にヒューマンリスク管理の実績を向上させたかを尋ねることが最善でしょう。この質問に対する答えを測定するための利用可能なデータはありません。しかし、これまでの分析によると、何らかの理由で、KnowBe4の顧客は公開情報漏洩リストに掲載される可能性が大幅に低いといえます。

調査結果の精度を知るための信頼区間の計算

KnowBe4の米国の顧客のわずか2.4%しか、公開情報漏洩データベースのリストに載っていません。これはかなり驚くべき統計です。読者の中には、KnowBe4の米国顧客リストが、米国の公開情報漏洩リストに掲載される可能性のあるすべての米国企業を網羅しているのか、それともKnowBe4の顧客リストがあまりにも少ないために掲載されていないのか、疑問に思われる方もいらっしゃるかもしれません。

例えば、顧客が10社しかいない企業であれば100%の顧客は公開情報漏洩リストに載っていないと正確に言えるかもしれない。しかし、その結果はおそらく、顧客が10社しかいなかったからであり、それ以外の理由ではないでしょう。55,010社のKnowBe4の米国顧客リストは、公開データ侵害リストに掲載される可能性のあるすべての米国企業をどれだけ正確に反映しているのでしょうか？統計学でその答えを見つけることは、信頼区間として知られています。そこで、KnowBe4は、米国の公開データ侵害に掲載される可能性のあるすべての米国企業をカバーしているかをKnowBe4の米国顧客信頼区間を計算しました。

米国の顧客リスト50,010社（つまりサンプル数）を、米国の全企業3230万社（つまり母集団）と比較することができます。また、KnowBe4の顧客リストと従業員数500人以上の米国企業33,200社とを比較することができます。なぜなら、これらの企業やKnowBe4の顧客は、データ侵害の報告義務を負っている可能性が高いからです。KnowBe4の50,010社の米国顧客リストを、信頼区間95%（KnowBe4の顧客リストが最大リストの95%を正確に表している可能性が高いことを意味する）で3,220万社の米国企業すべてと比較した場合の誤差は1%未満です。33,200社という少ない母集団では、誤差はその10分の1です。したがって、KnowBe4の顧客リストは、米国企業およびその企業が米国の公開データ侵害リストに掲載される可能性を高い信頼性で正確に反映していると考えられます。

データ侵害を受けた組織の分析

KnowBe4が提供するサービスとの相関関係を把握するために、KnowBe4の顧客になる前に1件以上のデータ侵害に見舞われた組織を調べ、KnowBe4の顧客になった後に同じ顧客が見舞われた漏洩件数と比較しました。KnowBe4 の顧客である企業が、顧客である間に受けたデータ侵害の件数が、KnowBe4の顧客になる前よりも少なかった場合、その結果は、優れた SAT プログラムが人的リスクを低減するという考えを裏付けることになります。

データ侵害を受けた米国内の1,189社の顧客のリストが、PRCデータベースとKnowBe4顧客ベースとの名寄せ・照合の結果、作成できました。これをベースに、データ侵害を受けた組織の分析を行い、対象組織がKnowBe4の顧客になる前にデータ侵害を受けたのか、またはKnowBe4の顧客になった後にデータ侵害を受けたのかを判定する必要がありました。

サイバーセキュリティとはリスク管理である

優れたSATプログラムによってデータ侵害のリスクが軽減されるとはいえ、KnowBe4の顧客の中には、（ソーシャルエンジニアリングを含むあらゆるデータ侵害の原因によって）データ侵害に見舞われるケースが起きることを覚えておいてください。

ここで考えるべきことは、持続する業務環境でいかなるサイバーセキュリティへの迅速な対応を実施したとしても、あらゆるサイバー攻撃のリスクを完全にゼロ（0%）にすることは不可能です。ゼロリスクの世界やビジネス環境を想定する人はほとんどいないでしょう。ほとんどのサイバーセキュリティの目標は、最も重大で高額なリスクと、そのリスクの発生や影響を許容可能なレベルまで軽減することです。サイバー攻撃のリスクを完全に 排除できないからといって、リスク軽減策を推奨したり、実行したりしないということではないのです。

例えば、GoogleのMandiant（https://www.action1.com/patching-insights-fromkevin-mandia-of-mandiant/）によると、パッチが適用されていないソフトウェアやファームウェアの脆弱性がデータ侵害の約33%に関与しているとのことです。すべての組織や個人は、すべての重要なパッチを適時に適用すべきであることは理解していますが、ほとんどの企業が完璧なパッチ適用を行っているとは言えません。とは言っても、サイバーセキュリティリスクを軽減するために適切なパッチ適用を推奨しないということにはなりません。重要なのはリスクの軽減です。言い換えれば、適切なパッチ適用を行う企業は、パッチ適用を行っていないソフトウェアやファームウェアが原因でセキュリティ侵害に見舞われるリスクが低くなります。

データ侵害を受けたKnowBe4顧客の分析

次に、KnowBe4のサービスがデータ侵害を低減させる効果をもたらしているかを分析するには、KnowBe4を採用する前よりも現在の方が侵害されることが少なくなっているかを検証することです。KnowBe4の導入効果を裏付けることになります

下の表はその検証結果です。

データ侵害を受けたKnowBe4の米国企業合計	KnowBe4導入前のデータ侵害件数	KnowBe4導入前のデータ侵害%	KnowBe4導入後のデータ侵害件数	KnowBe4導入後のデータ侵害%
1,189	866	72.83%	390	32.80%

注：データ侵害%の合計が100%を超えているのは、データ侵害を受けた顧客の中には、KnowBe4導入前・導入後に1回以上のデータ侵害を受けているためです。

このデータから、KnowBe4の米国顧客が被害にあったデータ侵害のほとんどは、KnowBe4導入前に発生していることが分かります。KnowBe4の現行の米国顧客のほとんど（97.6%）は、データ侵害の遭遇を報告していません。しかし、データ侵害を受けたことがある場合、その73%はKnowBe4の顧客となる前にデータ侵害を受けています。

データ侵害を受けたKnowBe4の米国顧客は、KnowBe4導入後にデータ侵害を受ける可能性が65%（72.83% - 32.8%）低いことが分かります。

これは、適切なSATを採用しているKnowBe4の顧客は、データ侵害を起こしにくいということをさらに裏付けるものです。また、言い換えれば、ソーシャルエンジニアリングやその他の人的リスクによるデータ侵害に見舞われた顧客が、SATプログラムを導入する（またはSATプログラムを改善する）ためにKnowBe4に来社してきていると思われます。いずれにせよ、適切なSATプログラムがデータ侵害を減少させたことを否定するデータは見当たりませんでした。

KnowBe4の顧客のうち、2.4%しかデータ侵害に見舞われていないことを考えると、この2.4%に対して33%のみのデータ侵害がKnowBe4の製品やサービスを採用後に発生していないことを意味します。要約すると、KnowBe4の顧客は、KnowBe4導入後に公開データ侵害を受ける可能性が極めて低いことが分かります。

データ侵害を経験したKnowBe4顧客は再度データ侵害に見舞われる可能性はさらに低い

データ侵害を経験した組織が、再び1回以上データ侵害を受けることは珍しいことではありません。このような場合であっても、KnowBe4の顧客は、以下の表が示すように、KnowBe4導入前に比べてデータ侵害の件数はお幅に減少しています。

KnowBe4顧客分類	KnowBe4導入前のデータ侵害件数	KnowBe4導入後のデータ侵害件数	KnowBe4導入前の頻度	KnowBe4導入後の頻度
現行顧客	2553	752	2.95	1.93

顧客となる前に侵害を受けたKnowBe4の米国顧客は、平均してほぼ3件の侵害を受けています。その一方でKnowBe4の顧客になった後にKnowBe4の米国顧客が受けた件数は、平均2件未満に減少しており、全体として37%［(2.97-1.88)/2.97］改善しています。見方をかえれば、データ侵害に遭った顧客はデータ侵害に遭わない顧客の97.6%であることを考えると、データ侵害に遭う可能性がKnowBe4の顧客になる前より58%［(2.97-1.88)/1.88］低くなっていることになります。

また、現在、KnowBe4の米国顧客の大半（97.4%）は、公開データ侵害に遭っていません。KnowBe4の顧客がKnowBe4のサービスを利用中にデータ侵害を受けたとしても、その件数は平均して少ないこと（1.93件対2.95件）が分かります。

サイバー保険契約はSATプログラムの実施を求めてきている

サイバー保険業界とその保険契約業務担当者は個別ではありますが、KnowBe4のこの調査結果を支持しています。その背景には、サイバー保険契約において、保険会社は保険契約者に有効なSATプログラムを実施することを条件とするようになってきています。そもため、SATプログラムを導入していないで、サイバー保険に加入することは難しくなっています。また、SATプログラムを導入していないで、サイバー保険を加入できたとしても、ほとんどの場合、保険料は割高になります。

＜この現状を裏付ける関連リンク＞

- 「すべてのサイバー保険はセキュリティ意識向上プログラムを必要とする（https://hoxhunt.com/blog/cyber-insurance-and-security-awareness--training)
- 「サイバーセキュリティ保険のプロバイダーは保険を提供する前に、従業員がセキュリティ意識向上トレーニングを修了していることを期待することが多い（https://expertinsights.com/insights/security-awareness-training-for-cyber-insurance/）
- サイバー保険に入るための5つの条件（https://aldridge.com/5-requirements-to-get-cyber-insurance/）
- サイバー保険に求められる7つの要件（そしてそれを満たす方法）（https://www.strongdm.com/blog/cyber-insurance-requirements）
- AIG サイバーセキュリティ・チェックリスト（https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cybersecurity-program-checklist.pdf）

サイバー保険業界では、保険料率・支払保険金額の算定のために数理計算を行っていますが、その結果として、サイバー保険の適用を受けるためには、SATプログラムの実施が不可欠であることが増えてきています。

本レポートの注意事項

本レポートに示したKnowBe4のデータと分析が、効果的なSATプログラムが実際のデータ侵害を防止することを、確証された相関関係と実証された因果関係をもって、揺るぎない証明するものではないことを十分承知しています。対比分析するために、無作為に選ばれたいくつかの大組織に効果的なSATを実施するよう指示し、他の無作為に選ばれたSATを実施しないよう指示する実験をいくつか計画しない限り、このレポートを証明または反証することは不可能です。仮に大規模な組織がこの実証実験に参加してくれたとしても、様々なリスク要因を無視して、年間を通してSATトレーニングと模擬フィッシング演習を全く実施しないことに同意することはないと考えています。これに加えて、真の効果を測定するために、複数の異なる研究者が長期間にわたって異なる集団でその実験を実施する必要があります。

そのことを認めた上で、私たちはSATプログラムとデータ侵害防止の相関関係と因果関係を裏付け、データ侵害リスクを低減するために入手可能なデータを分析することに全力を尽くしました。ここでご理解いただきたいのは、私たちがもっと多種多様なデータを入手し、より確実な実験を行ったならば、本レポートでの私たちの結論は異なるものになっていたかもしれないことです。

私たちは、以前にも、SATプログラムの効果についてのリサーチを行っています。効果的なSATプログラム、フィッシングの模擬テストを含むPhish-prone™ Percentages（https://www.knowbe4.jp/press/security-awareness-training-simulated-phishing-effective-in-reducing-cybersecurity-risk）に関するこのリサーチでは、効果的なSATプログラムが、十分に訓練されテストされた従業員がフィッシングの模擬テストに否定的な反応を示す可能性を減少させることを裏付けています。

その他の注意点と考察

SATプログラムの単独な効果がもたらす因果関係を完璧に証明することはできないと言えます。効果的なSATプログラムを実施している組織は、おそらく他のこと（ポリシー、技術的管理など）も実施しており、それらすべてが実際のデータ侵害のリスクを低減する要因となっていると考えなければなりません。私たちが言えるのは、KnowBe4の現行顧客は、平均的な米国組織よりもデータ侵害の頻度が低く、データ侵害を受けても被害が少ないということだけです。

最後に、PRCデータベースのデータ侵害は、人為的ミスや物理的窃盗など、あらゆる根本的原因によるものである点を注意しなければならなりません。PRCデータベースのデータ侵害の大部分は「不明」として報告されています。また、他の多くは、誤った分類がされていると思われます。これについては、別途議論したい。

これまで述べてきたように、私たちが決定的に述べることができるのは、何十年もの間、ほとんどすべての独立したデータが一貫して、ソーシャルエンジニアリングとフィッシングがデータ侵害のハッキング原因のトップであることを示しているということです。また、PRCのデータベースに掲載されているデータ侵害は、他の信頼できる情報源の調査結果と大きく乖離することはないでしょう。

まとめ

KnowBe4には50,010社を超える米国内の顧客がいます。その大多数（97.6%）は、公開データ侵害に見舞われていません。また、このレポートの分析から、データ侵害を受けたKnowBe4の米国顧客は、KnowBe4導入後にデータ侵害を受ける可能性が65%低いことが分かります。

さらに、本レポートのために分析されたデータおよびその他の裏付けとなる分析によると、効果的なSATプログラムは人的リスクおよび現実世界でのデータ侵害の可能性を大幅に低減できることが示されています。

その他の関連情報

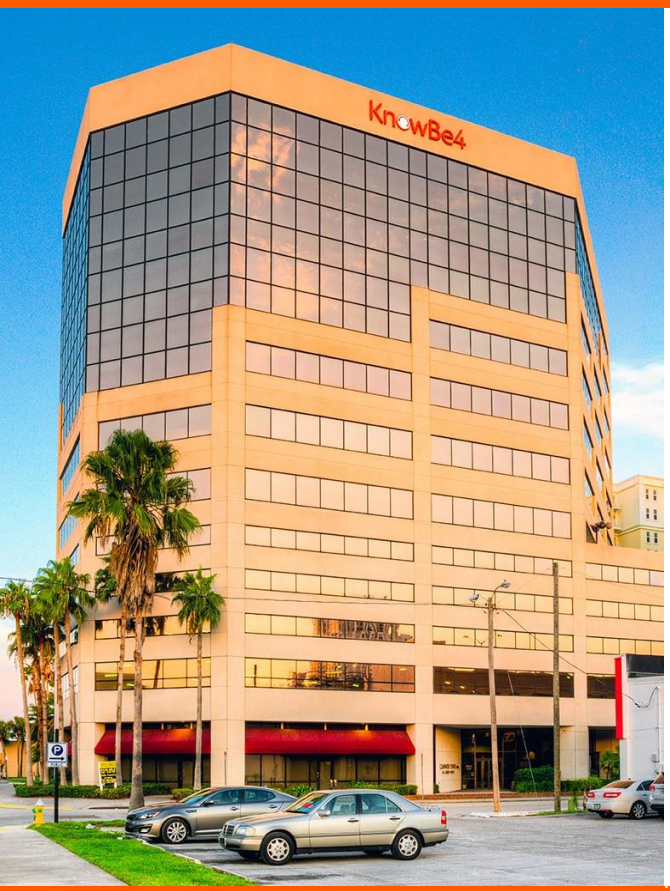
フィッシングセキュリティテスト
あなたの企業や組織の従業員の何パーセントがフィッシング攻撃に引っかかるかをスコア化することができます。.

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、ビッシング、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。

金融機関、製造業、エネルギー産業、医療機関、官公庁、生損保などで、7万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.com／www.KnowBe4.jp |