Osterman Research

WHITE PAPER

Osterman Research社によるホワイトペーパー
発行： February 2020
スポンサー： IRONSCALES

Robust Email Security Requires Alignment Between Security Practitioners and Decision Makers

強固なメールセキュリティのための経営陣とセキュリティ担当者の連携の必要性

エクゼクティブサマリー

フィッシングはセキュリティの意思決定を行う経営陣やインフルエンサーの主要な関心事であり、フィッシングの大部分はほとんどの組織の電子メールを介して行われます。メールフィッシングがどれほど深刻になったかについては、次のようなデータがあります。

- ベライゾンの調査レポート「2019 Data Breach Investigations Report」によると2018年に発生したデータ侵害の32%は何らかのフィッシング活動の結果でした。しかし、サイバー攻撃の90%以上はフィッシングから始まっています。[i]
- このレポートでは、サイバーインシデントやバックドアのインストールなどの78%はフィッシングに起因していると述べています。
- FBI Internet Crime Complaint Center (IC3) は2019年に467,361件35億ドルの損失があり、これは 2018年から30%増加しています。IC3へ報告された件数は23,775件にしかすぎませんが、ビジネスメール詐欺（BEC）による被害は2019年の損失（17億7000万ドル）の半分以上を占めています。[ii]

キーポイント

実施された調査から得られた主要なポイントは次のとおりです:

- いくつかの問題において、経営陣とセキュリティ担当者の認識の間に深刻なギャップがあることがわかりました。次に例を示します。
  - o フィッシングが組織にとって最優先事項であると考えている経営陣はセキュリティ担当者の４倍である。
  - o セキュリティ担当者はフィッシングの技術的な側面に焦点を当てており、問題に対して何らかの対応力を持っていると考えています。一方、経営陣はフィッシングの結果として生じるビジネススクという「より大きな構図」に焦点を当てています。
- フィッシング対策の必要性は、中規模および大規模な組織にとって重要な関心事であり、経営陣は、担当者が考えているよりもフィッシング対策の優先順位が高いと考えています。また、興味深いことに、米国の組織の方が英国の組織よりに多くのフィッシング攻撃を受けていると回答しているにもかかわらず、英国の組織の方が3倍多くフィッシングを「最優先」として回答しています。
- フィッシング対策をより徹底するためには、リアルタイムの脅威インテリジェンスが必要不可欠です。フィッシングにおける脅威インテリジェンスの現在の利用状況と、それをいつ使用すべきかには、大きなギャップがあります。
- ほとんどの組織はフィッシングの被害を受けており、最も一般的な影響はランサムウェア以外のマルウェアへの感染です。
- セキュリティチームは、フィッシング対応にかなりの時間と労力を費やします。フィッシング対応の人件費だけで、5,000人のユーザ組織に月額8,900ドル近くのコストがかかっています。
- 3/4の組織は、リアルタイムにフィッシング・インテリジェンスを自動処理することはできません。また、90%の組織は、複数のソースからのフィッシングインテリジェンスをリアルタイムで、組織の全体的なメールセキュリティソリューションの環境と統合することができません。
- 多くの組織がフィッシングメールを検出、調査、修正するたにかなりの時間を費やしています。ールを受信してから、フィッシングかどうかを識別するための時間に、30%の組織が6~30分、さらに14%の組織が31~60分費やしています。そして、65%の組織は、フィッシングメールを検出するのに5分以上費やしています。

フィッシングは経営陣とインフルエンサーにとって重要な関心事です。

- 70%の組織が、メールが届いてからクリックするまでの時間が平均82秒であるにも関わらず、組織のメールボックスからフィッシングメールを削除するには5分以上かかっています。
- ほとんどの組織では、フィッシング対策としていくつかのツールを使用していますが、最も一般的なアプローチはゲートウェイでのアプローチです。しかし、ほとんどの組織ではフィッシングに耐えうるツールのすべてを使用しているわけではありません。
- 5社のうち３社が、電子メールセキュリティプロトコルのトレーニングを年2回以下の実施に留めている一方、19%(組織の1/3のみ)の組織は、毎月または継続的にトレーニングを行っています。
- セキュリティスキルの不足は、セキュリティチームがフィッシングを適切に処理する能力に影響を与えています。
- 70%以上の組織が、ユーザから報告されたフィッシングメールを確認するために手動プロセスしか使用しておらず、メールの脅威を大規模に軽減するには、労力と時間がかかりすぎています。

調査について

このホワイトペーパーのための調査は、米国と英国の252名を対象に実施しました。調査の対象となる条件は a) 500人以上の従業員がいる組織で働いていること、b)セキュリティに焦点を当てた役割を持っていること、c)組織がフィッシングメールをどのように扱うかについての知識を持っていること です。調査対象者の所属する組織は幅広い業種となっています。さらに、立場による見解や認識の違いを理解するために、調査対象者を「経営陣」(CIO、CISO、情報セキュリティ担当役員)と「セキュリティ担当者」(電子メール管理者、情報セキュリティアナリスト、ITマネージャ/ディレクター、セキュリティアーキテクト、SOCアナリスト)に分けしました。

本稿では、「経営陣」と「セキュリティ担当者」を区別しています。経営陣にはCIO、CISO、および情報セキュリティのディレクターが含まれています。一方、セキュリティ担当者には、電子メール管理者、情報セキュリティアナリスト、ITマネージャ/ディレクター、セキュリティアーキテクト、SOCアナリストが含まれています。要するに、経営陣と実務者の主な違いは、前者が上位レベルの役割であるのに対し、後者は現場で、フィッシング問題に関してより実践的な日常的な決定を行っています。

英国組織は、米国より３倍多くフィッシングを「最優先」として回答しています。

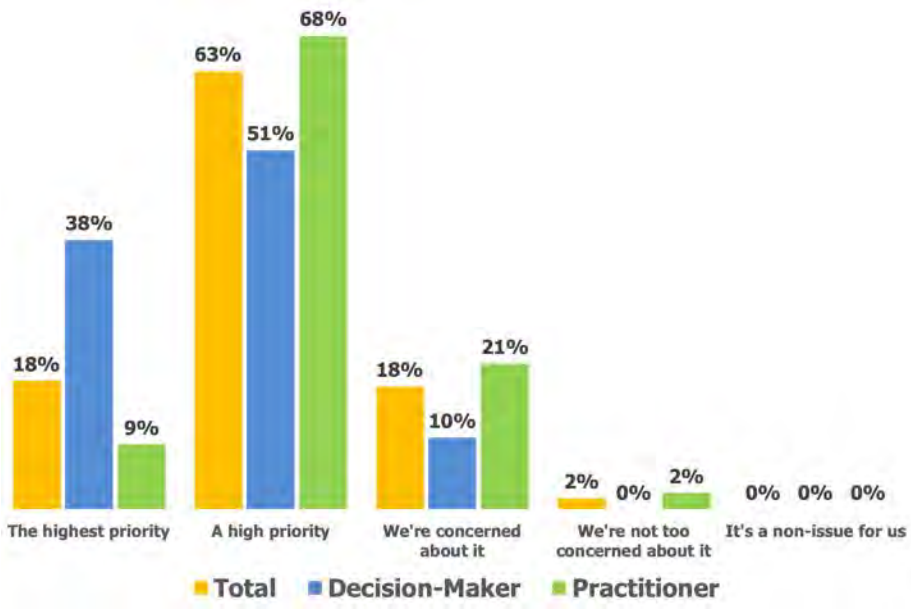
調査結果

フィッシング対策は最重要課題

驚くことではありませんが、この調査で他のキュリティ対策と比較してフィッシングの優先度が高いことがわかりました。表1に示すように、調査対象者の18%はフィッシングを組織の「最優先」と考えています。つまり、5人に3人以上がフィッシングを「最優先」と考えています。また米国組織がフィッシング攻撃をたくさん受けていると回答しているにもかかわらず、英国は３倍多くフィッシング攻撃を「最優先」として回答しています。

これらの結果は、2019年に実施された別のOsterman Researchの調査結果[iii]と一致しており、フィッシングが経営陣およびインフルエンサーにとって重要な関心事であることがわかりました。調査対象者の74%は、フィッシング攻撃を「懸念」または「非常に懸念」があると回答しています。

表1
他のセキュリティ問題と比較したフィッシングの優先順位



Source: Osterman Research, Inc.

データ侵害はフィッシングメールの結果としてよく発生します。

しかし、興味深いことに、経営陣の方がセキュリティ担当者よりも4倍多く、フィッシングが組織にとって最優先事項であると回答しています。さらに、フィッシングの「highest（最優先）」と「high（優先）」のプライオリティをまとめると、経営陣は、この問題について、セキュリティ担当者よりもはるかに（77～89%）関心を持っています。

この違いは、セキュリティ担当者がフィッシングの技術的な詳細に焦点を当てており、問題に対処していると考えているのに対し、経営陣はフィッシングの技術的な側面だけでなく、フィッシングの結果であるビジネスリスクの「より大きな構図」を見ているという事実が原因である可能性があります。

フィッシングの結果として起きる悪い出来事

表2に示すように、フィッシングのリンクや添付ファイルにアクセスした結果、組織の半数以上が何らかの非ランサムウェア感染を経験し、5分の2近くの組織がランサムウェアの大規模感染を経験しています。また、ユーザがフィッシングメールとやりとりした結果、データ侵害が発生することもよくあります。4分の1以上の組織がフィッシングの結果として言及しています(英国組織は、フィッシング攻撃が成功した結果、データ侵害が発生したと米国の組織よりも3倍以上高く報告しています)。アカウントのテークオーバーも一般的で、5つの組織のうち1つ以上の組織で回答しています。

表2
ユーザが、リンクをクリック、資金送金の依頼、クレデンシャル情報（IDなど）の要求、添付ファイルの開封などを行った結果として発生したインシデント

インシデント	合計	経営陣	担当者
エンドポイントがランサムウェア以外のマルウェアに感染	51%	56%	49%
エンドポイントがマルウェアに感染	38%	43%	35%
データ侵害が発生	27%	35%	23%
アカウントの乗っ取り	21%	16%	23%
BECの被害	17%	17%	17%
その他	11%	9%	12%

Source: Osterman Research, Inc.

全体的にセキュリティ担当者の方が経営陣よりもランサムウェア、ランサムウェア以外のマルウェア、およびデータ侵害などフィッシングメールによるインシデントにおいて、否定的な結果な報告が若干少ないことがわかりました。しかしながら、担当者の方が、フィッシングの結果としてアカウントの乗っ取りが発生したと報告する回答がいくぶん高くなっています。ここでも、経営陣はセキュリティインシデントが発生した際のビジネス上の結果に焦点を当てているため、技術的に焦点を当てた実務者よりも、データ侵害などの問題に注目しています。

フィッシングがセキュリティチームの時間を大量に消費

フィッシングメールは、セキュリティチームの時間を大量に消費します。表3に示すように、セキュリティチームの30%は、ランサムウェア以外のマルウェアを含むフィッシングメールを「頻繁に」または「とても頻繁に」対応を行っており、23%はクレデンシャル情報の盗用をめぐる問題に、5人に1人以上がアカウントの乗っ取りに時間を費やしています。

フィッシングメールはセキュリティチームの時間を大量に消費します。

表3
セキュリティチームがフィッシングメール対策に費やす頻度
「頻繁に」または「とても頻繁に」対応する割合

フィッシングメールの種類	合計	経営陣	担当者
ランサムウェア以外のマルウェア	30%	36%	27%
クレデンシャル情報の盗用	23%	31%	19%
アカウントの乗っ取り	21%	27%	19%
ランサムウェア	19%	29%	15%
BEC	15%	24%	11%
上記以外の脅威	12%	19%	8%

Source: Osterman Research, Inc.

ここでも、経営陣は、セキュリティチームがさまざまなタイプの脅威に費やしている時間を多く考えているように思われます。脅威に直接対処しているセキュリティ担当者は、マルウェア、クレデンシャル情報の盗難、その他の脅威に対処するために必要な労力を少なく考えています。明らかに、脅威が解決されたとみなされる時と実際に解決された時は異なります。

フィッシングは多くの場合検出に時間がかかる

良いニュース:
表4に示すように、12%の組織がネットワークに入ってから1分以内にフィッシングメールを特定して削除できるのに対し、33%は5分以内にフィッシングメールを削除できることがわかりました。英国組織は、フィッシング攻撃の検出と修復時間が米国よりも若干長く報告していますが、米国の大半の回答者は、これらの脅威の特定と修復にどれくらいの時間がかかったかを知らないと答えています。

悪いニュース:
67%の組織では、フィッシングメールの識別と削除に6分以上かかっています。その原因は、ユーザの8%がメールを受信してから30秒以内にクリックするという事実です。そして、この数字は最初の60秒以内に30%に跳ね上がります。つまり、大多数の組織では、ユーザの大部分がネットワークに入るフィッシングメールをクリックする前に、フィッシングメールを特定することができず、間違いなく修正できません。これは、リアルタイム脅威インテリジェンスの重要性を示しています。

表4
フィッシングメールがネットワークに入ってから会社のメールボックスから削除されるまでの時間

時間	合計	経営陣	担当者
１分以内	12%	12%	12%
５分以内	21%	17%	22%
６～３０分	30%	30%	29%
３１～６０分	18%	23%	15%
数時間	14%	15%	14%
数日間	2%	1%	2%
１週間以上	0%	0%	0%
わからない	4%	1%	5%

Source: Osterman Research, Inc.

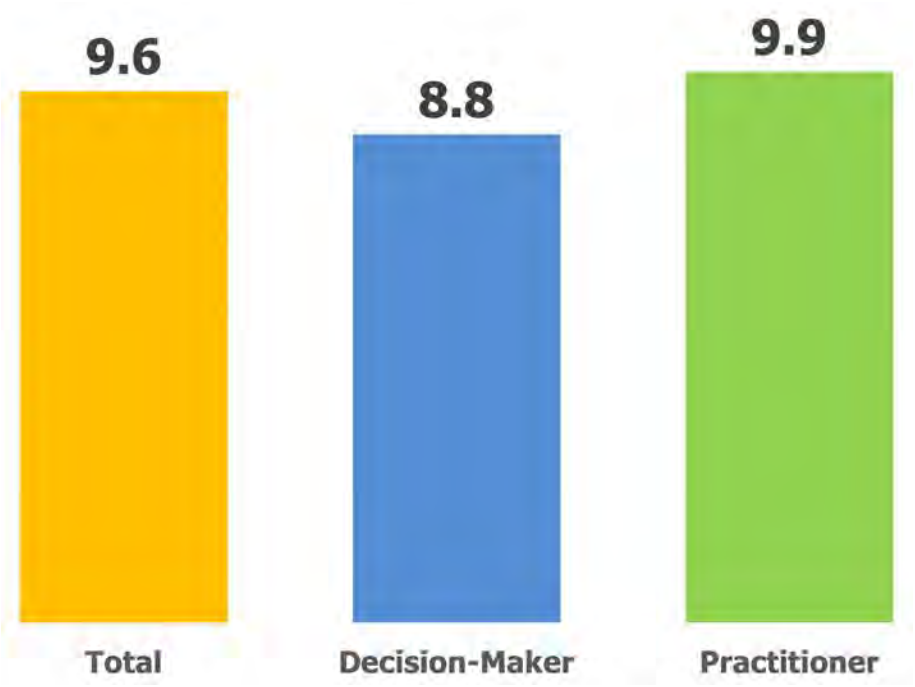
67%の組織でフィッシングメールの識別と削除に6分以上かかっています。

フィッシング対応には時間がかかる

図5に示すように、調査対象の組織はフィッシングメールの調査、検出、修正に1週間で平均従業員1,000人あたり9.6人時間を費やしています。興味深いことに、フィッシングの試みにライフサイクルを通して対処するために必要な時間を経営陣は担当者の想定よりもかなり短く回答しており、フィッシングの問題に対処する「現場にいる」担当者の想定よりも約11%低い結果となりました。また、英国組織の時間投資は、米国の9.9人よりやや低い(週1,000時間あたり9.2人時)ことがわかりました。

これは、典型的な週の勤務時間（40時間）のうち、セキュリティチームの24%の時間（1週間に1日以上）が、フィッシングメールの調査、検出、修正のみに費やされていることを意味します。また、一部のフィッシングメールは検出されず、フィッシングに関する可視性とインテリジェンスが不足しているため、処理に時間がかかっていないことに注意することも重要です。

表5
フィッシングメールを調査、検出、修復するためにセキュリティチームが週に要する時間
従業員1,000人当たりの労働時間



Source: Osterman Research, Inc.

これは、フィッシングメールの調査、検出、修正に専念するリソースを持っていない小規模なセキュリティチームにとって、特に、重要な発見です。たとえば、500人の組織では、これらの活動はセキュリティチーム(多くの組織の場合、担当者は1名)をの10%以上を消費します。

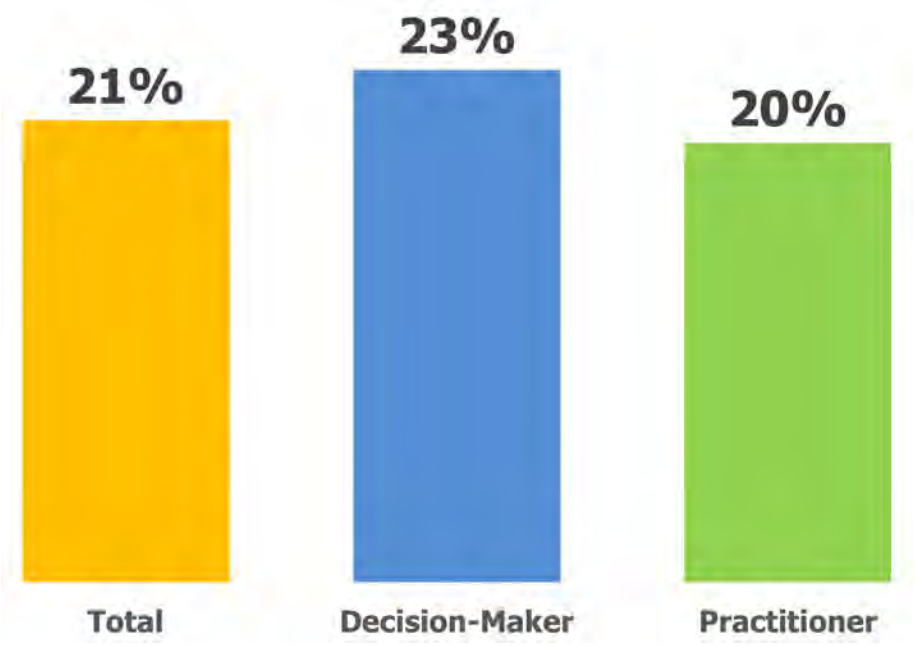
経営陣が、平均してフィッシングに対処するためにセキュリティ担当者が必要とする時間を短く見積もっているという結果は、CIO、CISOなどの人々がフィッシング対応のあらゆる側面に関わっていないという事実を示しています。多くの場合、経営陣は、現在での実践とプロセスがどれほど困難であるか、および現在のフィッシング対策の防御策に存在するギャップを十分に理解していない可能性があります。一部の組織では、セキュリティ担当者がフィッシングの脅威に対処するために必要な予算と人員のサポートを得ることが困難になる場合もあります。

経営陣は担当者がフィッシングに対処するために必要とする時間を短く見積もっています。

フィッシング管理には多大な労力が必要

表6のとおり、セキュリティアナリストの20%以上の時間がフィッシングメールの調査や修正に費やされています。この点に関する経営陣とセキュリティ担当者の推定値の差はわずかでした。

表6
アナリストがフィッシングメールの調査や修復するために週に要する時間の割合



Source: Osterman Research, Inc.

費用のかかるフィッシング対策

セキュリティアナリストの平均給与が年間85,799ドルであると仮定すると、表5に示すようなフィッシングメールの調査、検出、修復に要するセキュリティ担当者の時間を計算すると、従業員1,000人あたり年間515人時間、すなわち総コスト21,235ドルとなります。それは、フィッシングメールの調査、発見、修復に取り組むためだけに、従業員1人当たり月額1.77ドルのコストがかかっています。すなわち、従業員5,000人の組織は、フィッシングメールに取り組むために、人件費だけで年間106,000ドルを超える費用を費やしていることになります。

5,000人規模の組織は、フィッシングメールに対処するために、人件費だけで年間106,000ドルを超える費用を費やしてます。

フィッシング対策に多くがセキュアメールゲートウェイを使用

約3分の2の組織がフィッシングに対処するためにセキュアメールゲートウェイソリューションを使用しています。そして、表7に示すように、セキュリティ担当者は、経営陣よりも若干多く採用していると回答しています。
また、MicrosoftのAdvanced Threat Protection(ATP)やExchange Online Protection(EOP)などの他のソリューションも、主にOffice365がビジネスグレードの電子メール市場に大幅に浸透した結果として広く使用されています(2020年1月現在、Office365のユーザ数は2億人を超えています[vi])。
フィッシング対策ソリューションを使用していないと報告する組織はごくわずかです。米国組織は、英国(51%)よりも、セキュアメールゲートウェイソリューション(82%)を使用していると回答しています。

表7
使用中のフィッシング対策ソリューション

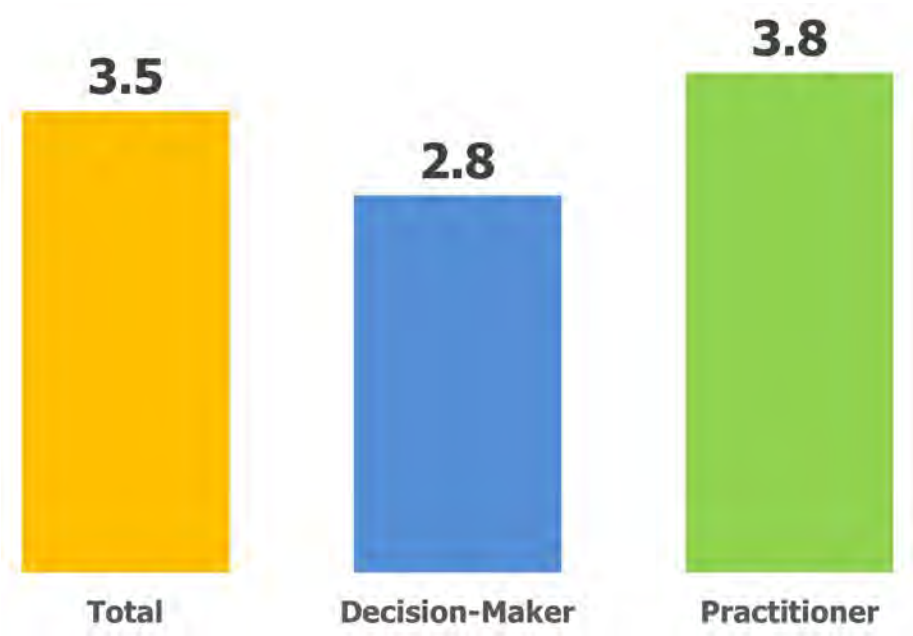
ソリューション	合計	経営陣	担当者
セキュアメールゲートウェイソリューション	67%	63%	68%
Microsoft ATP	48%	55%	45%
Microsoft EOP	33%	37%	31%
Google G Suite	32%	40%	28%
使用していない	1%	0%	2%

Source: Osterman Research, Inc.

表8のとおり、フィッシングメールの検出と応答に平均3.5種類のツールを使用していると回答していますが、経営陣は、実際に現場に携わるセキュリティ担当者よりも大幅に低い回答をしています。これは、多くの組織において、経営陣がフィッシング管理のプロセスに関わっておらず、フィッシングメールの検出、調査、修正に関連して十分に理解していないという事実を反映しています。

フィッシングメールの検出と対応に平均*3.5*種類のツールを使用しています。

表8
フィッシングメールの検出と対応に使用しているベンダーツールの数



Source: Osterman Research, Inc.

組織は高度な技術を採用

表9に示されているように、5社のうち約2社がフィッシング対策の一環としてAIを使用していると回答していますが、半数近くは機械学習を使用しており、71%は自動化を使用していると回答しています。セキュリティ担当者は、フィッシング問題に対処するためにAIや機械学習の使用を回答する比率はやや低いですが、自動化の使用を回答する比率はやや高くなっています。

英国組織は、フィッシング対策のために機械学習の使用を多少増やしていると回答していますが、米国組織は、より高いレベルの自動化を回答しています。

表9
フィッシング対策の一環として各種技術の採用

インシデント	合計	経営陣	担当者
AI（Artificial intelligence）			
使用しています。	39%	46%	36%
使用していませんが、今後使用する予定です。	49%	44%	51%
使用していません。また、今後も予定はありません。	12%	10%	13%
機械学習（Machine-learning）			
使用しています。	49%	55%	47%
使用していませんが、今後使用する予定です。	40%	36%	42%
使用していません。また、今後も予定はありません。	10%	9%	11%
自動化（Automation）			
使用しています。	71%	67%	73%
使用していませんが、今後使用する予定です。	26%	32%	23%
使用していません。また、今後も予定はありません。	4%	1%	5%

Source: Osterman Research, Inc.

組織は、AI、機械学習、自動化を実際に使用していますか? この回答はいいえでもはいでもあります。フィッシングメールの検出、調査、修復において、これらの技術の潜在的な利点のすべてを完全に活用しているフィッシング対策技術はあまり多くありません。しかし、現在使用可能な主要なソリューションの多くは、AI、機械学習、自動化などのアプローチを使用して、フィッシング管理要件の少なくとも一部に対応するために、さまざまなレベルで実際に使用しています。さらに、これは、真の「自動化」や「AI」といった普遍的な定義が存在しないことを示しています。

スクリプトやツール、プレイブック、*YARA*ルールの依存度が高いことは、多くのセキュリティアナリストが信じているほど、実際には真の自動化は使われていないことを意味しています。

セキュリティメールゲートウェイとユーザトレーニングは、さまざまな脅威に対処すると信頼

表10、11、12が示すように、組織が多様かつ変化するメール攻撃、偽のログインページや電子メール、ビジネスメール詐欺(BEC)の試みに対応するために使用される2つの主要な方法は、セキュアメールゲートウェイとこれらの脅威に対処するための訓練を受けたユーザです。これらの問題に対処するために使用するツールに関する回答は、経営陣とセキュリティ担当者の間に大きな差はありませんでした。これは、特にクラウドベースの電子メールがより一般的に使用されるようになるにつれて、セキュリティチームがこれらの脅威への対応について誤った安心感を持っていることを強く示唆しています。しかし、3種類の攻撃/脅威すべてに対して、米国組織は、「これらの脅威を認識する訓練を受けたユーザ」を、英国よりもはるかに高く回答していることがわかりました。

また、次の表が示すように、スクリプトやツール、Playbook、YARAルールへの依存度が高いことは、実際には、多くのセキュリティアナリストが信じているほど、本当の自動化が行われていないことを強く意味しています。これは、セキュリティに重点を置いた経営陣がチームで対処すべきであるという大きな誤解です。

表10
多様かつ変化する電子メール攻撃に対処するためにセキュリティチームが使用するソリューションとプロセス

ソリューション/プロセス	合計	経営者	担当者
シグネチャーベースで検出を行うセキュアメールゲートウェイ	62%	67%	59%
脅威を認識する訓練を受けたユーザ	52%	55%	51%
スクリプトとルール	50%	45%	53%
プレイブック	19%	26%	17%
YARA ルール	11%	14%	9%
この種の攻撃に精通していない	10%	5%	12%
対処不能	6%	10%	5%
その他	2%	1%	2%

Source: Osterman Research, Inc.

表 11
セキュリティチームが偽のログインページや電子メールに対応するために使用するソリューション/プロセス

ソリューション/プロセス	合計	経営者	担当者
シグネチャーベースで検出を行うセキュアメールゲートウェイ	69%	76%	66%
脅威を認識する訓練を受けたユーザ	70%	69%	70%
視覚的類似性検出（コンピュータヴィジョン）	20%	26%	18%
その他	4%	0%	6%

Source: Osterman Research, Inc.

表12
セキュリティチームがBECから保護するために使用するソリューションとプロセス

ソリューション/プロセス	合計	経営者	担当者
シグネチャーベースで検出を行うセキュアメールゲートウェイ	69%	77%	65%
脅威を認識する訓練を受けたユーザ	68%	72%	66%
メールボックスレベルでの異常検出	34%	35%	34%
DMARC	14%	12%	15%
その他	2%	3%	2%

Source: Osterman Research, Inc.

フィッシングやその他のセキュリティ問題を管理するための重要な機能が不足しています。

重要な機能の深刻な欠如

表13のとおり、フィッシングやその他のセキュリティ問題を管理するための重要な機能がいくつか欠けています。たとえば、調査対象の組織の55%が脅威情報フィードを、47%がゼロデイフィッシング攻撃をリアルタイムで可視化していますが、使用していない組織はそれぞれ45%と53%存在します。さらに悪いことに、25%の組織がリアルタイムでフィッシング・インテリジェンスを自動処理できず、13%の組織は、複数のソースからのフィッシング情報をリアルタイムで組織の延滞的なメールセキュリティソリューションの環境と統合できないという事実があります。

これらの結果は、経営陣とセキュリティ担当者の間にほとんど違いが見られませんでした。米国組織は、英国より脅威インテリジェンスデータを利用している傾向にあります(60%対50%)。

表13
"次のうち、あなたの組織に当てはまるものはどれですか?"

インシデント	合計I	経営陣	担当者
脅威インテリジェンスデータを活用している	55%	58%	53%
ゼロデイフィッシング攻撃に対するリアルタイムの可視化を実施している	47%	48%	46%
脅威インテリジェンスデータの誤検出が多い	26%	29%	25%
フィッシングの情報をリアルタイムで自動処理していない	25%	21%	28%
複数のソースからのフィッシング情報をリアルタイムでメールセキュリティソリューションに統合できない	13%	12%	13%

Source: Osterman Research, Inc.

フィッシングメール対策において、脅威インテリジェンスの使用に限界があることに注意することが重要です。これについては、SpyCloudのセキュリティリサーチのバイスプレジデントが次のとおり語っています。「事後対応の組織によって脅威インテリジェンスは有効性を失う。脅威インテリジェンスは攻撃者に対する全体像を形成するように複数のインテリジェンスポイントを混在させて利用しないと失敗におわる。」

フィッシングに関する脅威インテリジェンスをどのように使用するか、また、データをメールセキュリティ対策にどのように統合するかという点において、まだまだ課題があります。

56%の担当者は、フィッシングメールの組織全体への侵入を想定した場合、1日に4通のフィッシングメールを処理することができます。

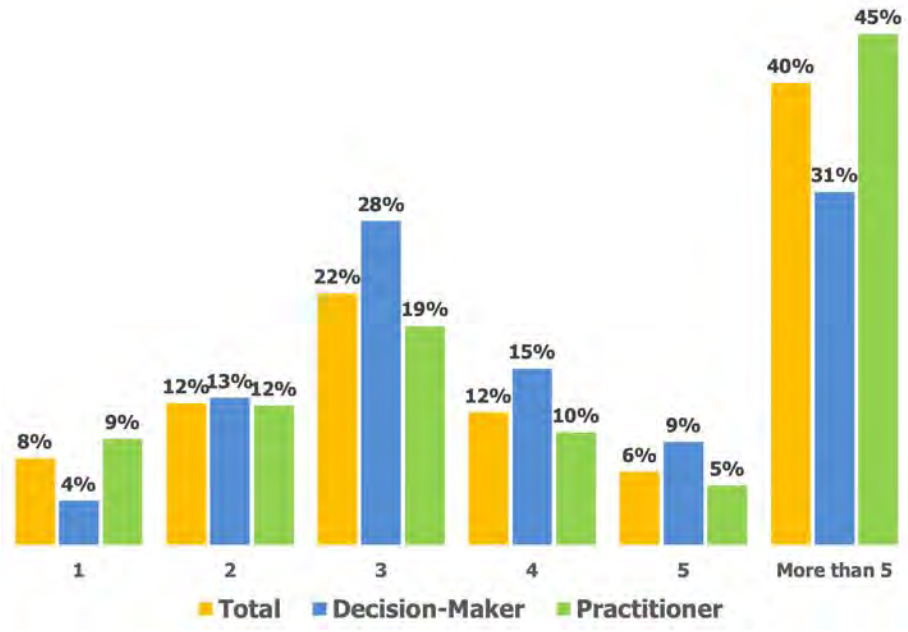
フィッシング管理は労働力によって制約される

表14が示すとおり、大半の組織が、組織内のすべてのメールボックスがフィッシング攻撃の対象となっている場合、セキュリティ担当者が通常１日に処理できるフィッシングメールは5件以下であると回答しています。実際、56%の組織の担当者は、フィッシングメールの組織全体への侵入を想定して、1日に4通以下のフィッシングメールを扱うことができます。これは、SOCアナリストの60%が1日に7~8件の調査を処理できるという別の調査結果[vii]とは対照的です。

それでは、組織内のすべてのメールボックスに日々影響を与える複数のフィッシング攻撃のシナリオとは、どの程度一般的なものなのでしょうか。2019年のIRONSCALESデータを使用したアバディーングループの分析[viii]では、確認された１つのフィッシングメール攻撃に対し、2~40を超えるメールボックスが影響を受けていることがわかりました。さらに、特定のフィッシング攻撃によって影響を受ける組織は、少なく見積もっても5、多い場合は150を超えます。

言い換えれば、標的型攻撃は一般的になりつつあり、すべてのフィッシングメール攻撃は、多くの異なる組織の複数のメールボックスに影響を与える可能性があります。これは、文字どおり、各組織で何百ものフィッシング攻撃を検出する必要があるということです。この分析に基づくと事態はさらに悪化するでしょう。10通のフィッシングメール攻撃のうち4通以上がポリモーフィック（攻撃者が従来のセキュリティソリューションを回避するためにフィッシングの試みを変更する手法）なものとなっています。ポリモーフィックな攻撃は最低でも一度は変化しますが、何百回でも変化することもあり得ます。

表14
アナリストが1日に処理できるフィシングメールの数
組織内のすべてのメールボックスが影響を受けたと想定



Source: Osterman Research, Inc.

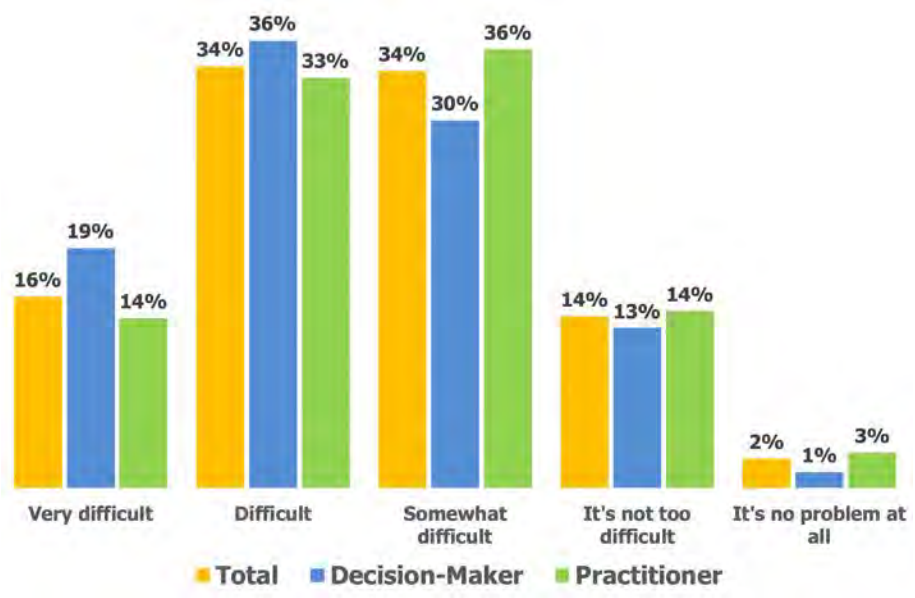
全体的に、経営陣は、フィッシングメールへの対応能力について、セキュリティ担当者よりも若干低く回答しています。たとえば、セキュリティ担当者の45%は、1日には5件以上の組織全体のフィッシングメールを管理できると考えていますが、これが当てはまると考えているのは、経営陣の31%にすぎません。

フィッシング管理機能について経営陣はセキュリティ担当者よりも若干低く見積もっています。

セキュリティスキル不足の現実

組織全体のフィッシング攻撃を管理するための処理能力が比較的低いという問題を深刻化させるのは、多くの組織がセキュリティチームに適した人材を見つけることが難しいという事実です。セキュリティスキルの不足は、業界の出版物やカンファレンスで広く議論されており、われわれの調査は表15に示すように、これらの議論を裏付けています。調査対象者の50%が、熟練したITセキュリティ専門家の採用と維持は「非常に困難」または「困難」であると考えていることがわかりました。一方、セキュリティ人材の採用と維持ついて問題はないと回答した人はほとんどいません。

表 15
高度なITセキュリティスペシャリストの採用・確保の難しさ



Source: Osterman Research, Inc.

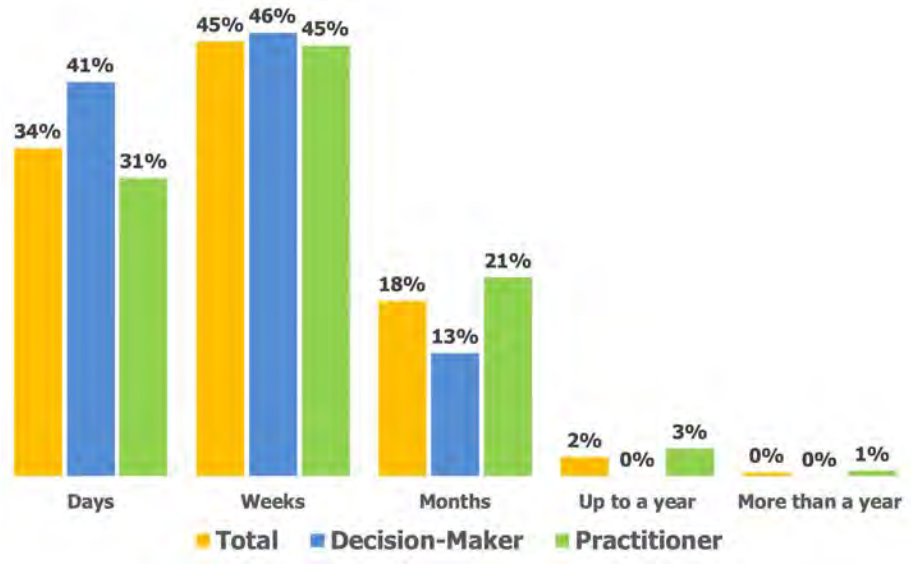
経営陣は、セキュリティのスキルと保持が「非常に難しい」または「難しい」と考えている傾向がありますが、セキュリティ担当者は、この問題がそこまで深刻であるとは考えていないようです。しかし、これは、ほとんどの組織では、熟練したセキュリティスタッフを見つけ、採用し、維持するという負担が、セキュリティ担当者よりも経営陣にかかっているという事実が原因である可能性があります。

トレーニングには時間がかかる

表16に示すように、組織のメールセキュリティソリューションおよびプロセスに携わる新しいセキュリティチームメンバーのトレーニングに要する時間は、かなり異なります。全般的に、組織の約3分の1は、これらの新しいスタッフを訓練するのに要する時間を「日」単位で考えていますが、半分近くは「週」単位で必要だと考えています。
興味深いことに、セキュリティ担当者は、経営陣よりも新しいスタッフのトレーニングには多少時間がかかると考えています。たとえば、10%以上の経営陣は、新しいスタッフを訓練するには「数日」かかると考えています。一方、8%以上の担当者は、適切に訓練するには「数か月」かかると考えています。

メールセキュリティソリューションおよびプロセスに携わる新しいセキュリティチームメンバーのトレーニングに必要な時間は大きく異なります。

表16
メールセキュリティソリューション/プロセスに関わる新しいセキュリティチームメンバーのトレーニングに必要な時間



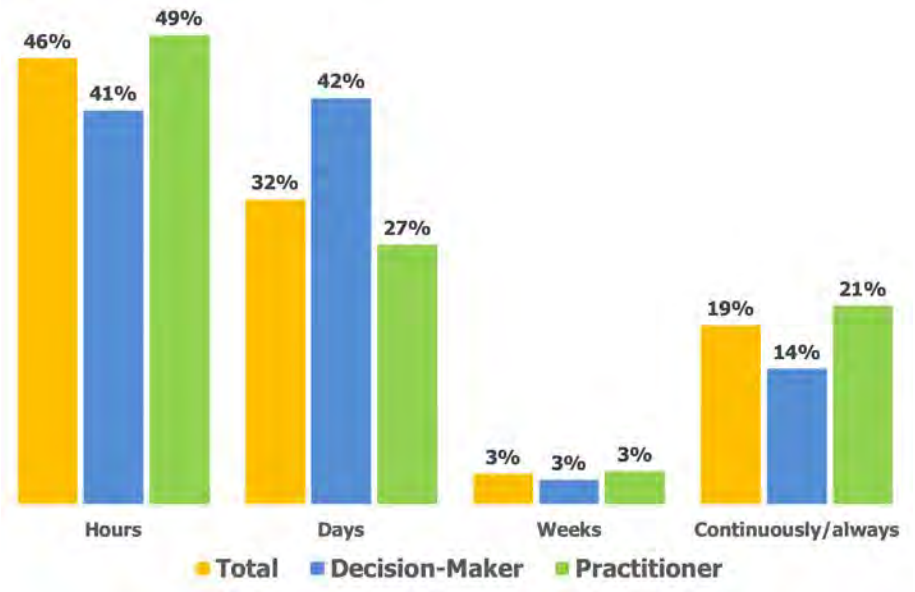
Source: Osterman Research, Inc.

メールセキュリティポリシーの更新はさまざま

調査によると、5分の1程度の組織がメールに関するセキュリティポリシーを継続的に更新、微調整しているのに対し、月に「数時間」しか費やさない組織の割合が大幅に高いことがわかりました。興味深いことに、セキュリティ担当者の多くは、メールセキュリティポリシーの微調整と更新に費やす時間は毎月「数時間」だけが必要であると回答していますが、実際には継続的にそれらを更新している割合が多いことがわかりました。米国組織は、英国(33%)よりも、セキュリティポリシーの調整と更新に「数時間」かかる(60%)と回答しています。

約*1/5*の組織が、企業のメールに関するセキュリティポリシーの更新と調整を継続的に行っています。

表17
セキュリティチームが月に企業のメールセキュリティポリシーを調整、更新する時間



Source: Osterman Research, Inc.

不十分なユーザトレーニング

Osterman Researchの行ったいくつかの調査では、多くのユーザがセキュリティ問題に関して十分な頻度でトレーニングを受けていないことがわかっており、今回の調査も例外ではありません。表18に示されているように、57%の組織は、メールセキュリティプロトコルのトレーニングの受講頻度は年2回以下となっています。そして、毎月もしくは継続的にトレーニングを行っている組織は19%(57%の3分の1)だけでした。 セキュリティトレーニングの頻度に関して、経営陣とセキュリティ担当者の間に大きな違いはありませんでした。ユーザが入社した時点で訓練を受けたとの回答は英国組織は米国（5%）の約４倍（19%）でした。

57%の組織は、メールセキュリティのユーザトレーニングを年2回を超えない範囲で実施しています。

表 18
メールセキュリティに関するユーザトレーニングの頻度

頻度	合計	経営陣	担当者
入社直後	12%	14%	11%
セキュリティインシデント発生後	8%	12%	7%
年１回	18%	19%	17%
年２回	19%	15%	21%
年3～4回	19%	15%	21%
１ヶ月おき	5%	5%	5%
毎月	6%	8%	5%
継続的に実施	13%	12%	14%
実施していない	0%	0%	0%

Source: Osterman Research, Inc.

それでは、エンドユーザ向けのセキュリティ意識向上トレーニングの「正しい」頻度はどのくらいなのでしょうか。すべての業界、組織に適用できる確固たる回答はありませんが、Infosecは原則として90日ごと、つまり年に4回のトレーニングを行うことを勧めています。[ix]

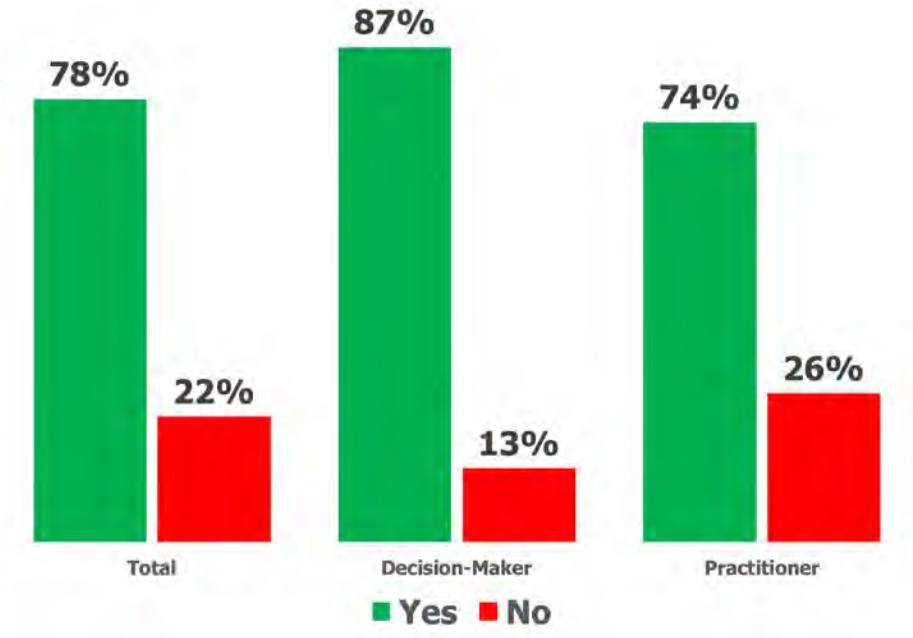
セキュリティの決定権を持つ経営陣が対処しなければならない重要な問題の1つは、さまざまな種類の脅威を防がなければならない環境において、技術ベースのソリューションとトレーニングの役割を決定することです。特に、マルウェアが含まれていない脅威や、BECの試みなどの悪意のあるサイトへのリンクの場合は、適切なバランスを見つけることが重要です。2019年のOsterman Researchの調査[x]によると、セキュリティに関して経営陣の大半は、セキュリティ意識向上のためのトレーニングとテクノロジーベースのソリューションの両方に果たすべき役割があると考えていますが、これは脅威の種類によって異なります。たとえば、40%以上がフィッシングとBEC防御のためのトレーニングを有効なトレーニングとみなしていますが、アカウント乗っ取り防止のためのトレーニングを有効なトレーニングであると考えているのは17%のみとなっています。反対に、スピアフィッシング対策を主に技術に焦点を当てた問題とみなすのは11%にすぎませんが、36%の人々がランサムウェアは主に技術ソリューションを使用して対処すべき問題とみなしています。

これらの脅威はすべて、技術対策とトレーニングの必要性を示すものですが、特定の脅威についてこれらの両方に重点を置くべきであることについては、明らかに異なる見解、そして、おそらくいくつかの誤解が存在します。

フィッシングのシミュレーションが一般的

大多数の組織がユーザを訓練するためにフィッシングシミュレーションを使用していることがわかりました。表19に示すように、78%の組織がシミュレーションを用いたトレーニングをユーザに実施しています。経営陣は、フィッシングシミュレーションが組織で使用されていると回答する傾向が高くなっています。

ほとんどの組織がフィッシングのシミュレーションを用いたユーザトレーニングを実施しています。

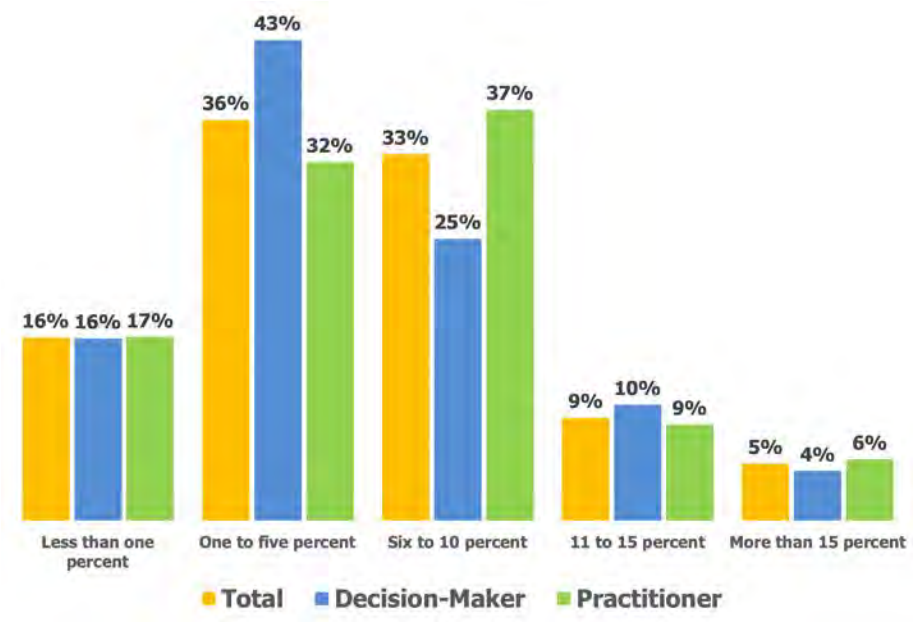


Source: Osterman Research, Inc.

ユーザのクリックレートは異なる

フィッシングシミュレーションを使用してユーザトレーニングを行っている組織では、シミュレーションで用いたフィッシングメールに対し、ユーザがクリックした割合は大きく異なります。表20に示すように、ユーザの半数以上がこれらのメールのクリック率が5%未満であったのに対し、14%のユーザだけがメールの10%以上をクリックしました。経営陣は、シミュレーションでフィッシングメールをクリックするユーザの割合を、セキュリティ担当者よりも低く見積もっている傾向があります。

表20
トレーニングでユーザがフィッシングメールをクリックした確率



Source: Osterman Research, Inc.

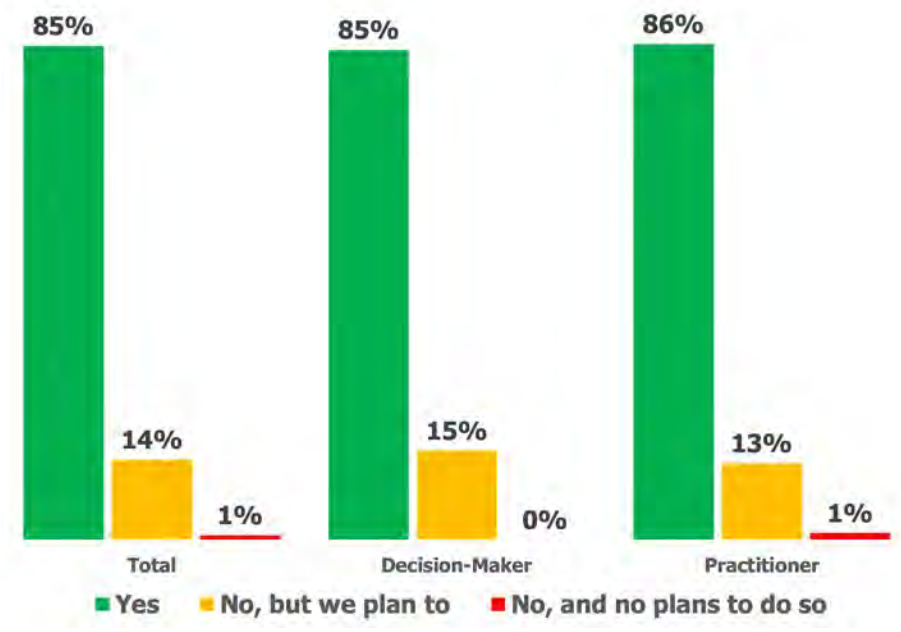
応用型のトレーニングであっても、一部のユーザは騙されてしまいます。

調査の結果、ユーザのトレーニング用にシミュレーションしたフィッシングメールを使用しているにもかかわらず、47%のユーザが悪意のあるリンクをクリックした確率は6%以上でした。シミュレーショントレーニングであるにも関わらず、何人かのユーザは騙されてしまうことが実証されました。その背景には、不十分なフィッシングトレーニング、頻度の問題、トレーニングが身につかないユーザの存在など、いくつかの要因があります。

報告の仕組みは普及している

大多数の組織は、表21に示すように、ユーザがフィッシングを発見した際にITチームやセキュリティチームに報告するための何らかの方法を提供しています。現在、85%の組織がレポート手段を提供しており、現在仕組みを持っていない組織においてもほとんどの組織が、今度仕組みを講じることを計画しています。この質問では、経営陣とセキュリティ担当者の間に差異はありませんでした。米国の組織の94%は、フィッシングを報告するためのメカニズムがあると報告していますが、英国ではたったの76%でした。

表21
“組織内にユーザがフィッシングをITやセキュリティに報告する仕組みはありますか?”



Source: Osterman Research, Inc.

フィッシングメールの報告に対して手動での確認が一般的

表22に示すように、フィッシングメールをITチームやセキュリティチームに報告する仕組みをもつほとんどの組織で、報告されたフィッシングメールをすべて手動で確認しています。ごく一部の組織(29%のみ)では、自動化を使用して、フィッシングインシデントのクラスタ化やトリアージを行ってしています。さらにごく一部の組織は、セキュリティチームがレポートだけで手動で確認を行っています。この質問について、経営陣とセキュリティ担当者の間でほとんど違いがありませんでした。自動化がほとんどの組織の目標であると仮定すると、これらの結果は、多くの組織がフィッシング対策能力を向上させるためには長い道のりとなることを明確に示しています。

ほとんどの組織にとってフィッシング対策機能を向上させることは簡単ではありません。

表22
フィッシングメールの報告があった際の行動

	合計	経営陣	担当者
セキュリティチームが手作業ですべてのレポートを確認する	54%	52%	55%
自動でインシデントを収集し、トリアージする	29%	33%	27%
セキュリティチームはいくつかのレポートを手作業で確認する	17%	15%	18%
何もしない	0%	0%	0%

Source: Osterman Research, Inc.

上記のデータからわかるように、ユーザが報告したフィッシングメールを確認するメカニズム(**70%以上の組織が手動プロセスのみ**を使用しています)は、**労働力に依存しすぎ**ています。メールユーザが5,000人いる組織において、ユーザが 1 週間に平均 1 通のフィッシングを報告したとすると、毎週確認するメールは1,000通となります。多くの組織においてこの作業努力を継続し続けることは簡単ではありません。

まとめ

中規模および大規模な組織では、電子メールフィッシングの処理にかなりの時間と労力が費やされています。しかしながら、それらの現在の技術、慣行、およびプロセスは、しばしば、問題に完全に対処するのに十分ではなく、その結果、フィッシングは、他のセキュリティ問題と比較して、主要な関心事として残されます。現在のプロセスを使用して調査できるフィッシング攻撃の平均数が少ないことを考慮すると、この調査のデータは、ユーザが報告したフィッシングメール(70%以上の組織が手動プロセスのみを使用しています)を確認するためのメカニズムは、労働集約的すぎることを示しています。平均ユーザが1週間に1つのフィッシングメールのみを報告する5,000人のメールユーザの組織では、結果は毎週レビューする必要がある1,000件のメールになります。多くの組織においてこの作業努力を継続し続けることは簡単ではありません。

IRONSCALESについて

IRONSCALESは、サイバーセキュリティの世界トップベンチャープログラムより投資を受け、イスラエル国防省インテリジェンス・テクノロジー・ユニットのメンバーによって設立された、フィッシング対策の未来型企業です。セキュリティプロフェッショナルおよびエンドユーザに、明日のフィッシング攻撃を今すぐ阻止するための包括的なソリューションを提供するAI駆動の自己学習型メールセキュリティプラットフォームを提供しています。世界で最も分散化された脅威防御ネットワークを使用して、当社のプラットフォームは、メールボックス内にあるフィッシング攻撃の防御、検知、および修正を、数分や数時間単位ではなく、数秒で行います。あらゆる規模の組織に、あらゆるタイプのフィッシング攻撃に対する完全なフィッシング対策を今すぐ提供します。
詳しい情報は**www.ironscales.com** もしくは*The Power of Now*をご覧ください。

参考文献

[i] https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

[ii] https://www.darkreading.com/fbi-business-email-compromise-cost-businesses-$17b-in-2019/d/d-id/1337035

[iii] *New Methods for Solving Phishing, Spearphishing and BEC and Other Security Threats*, Osterman Research, Inc.

[iv] https://www.infosecurity-magazine.com/opinions/phishing-time-matters-1-1/

[v] Source: Indeed as of January 17, 2020

[vi] Source: Microsoft

[vii] https://www.infosecurity-magazine.com/news/socs-are-overwhelmed-and-face-deep/

[viii] *Email Security is Ineffective, and Getting Worse: What You Can Do About It*, Aberdeen

[ix] https://resources.infosecinstitute.com/security-awareness-course-design-best-practices/#gref

[x] *New Methods for Solving Phishing, Spearphishing and BEC and Other Security Threats*, Osterman Research, Inc.

本書は、Osterman Researchのレポート「Robust Email Security Requires Alignment Between Security Practitioners and Decision Makers」を和訳したものです。
和訳はあくまでも便宜的なものとして利用し、適宜、英文の原文を参照していただくようお願いします。
また、翻訳による誤解から生じたいかなる損害についても責任を負いません。