Cyber Secure:

従業員のセキュリティ習慣を考える

A study commissioned by CompTIA

企業にとって最大の脅威となるのは、従業員のIT習慣かもしれない

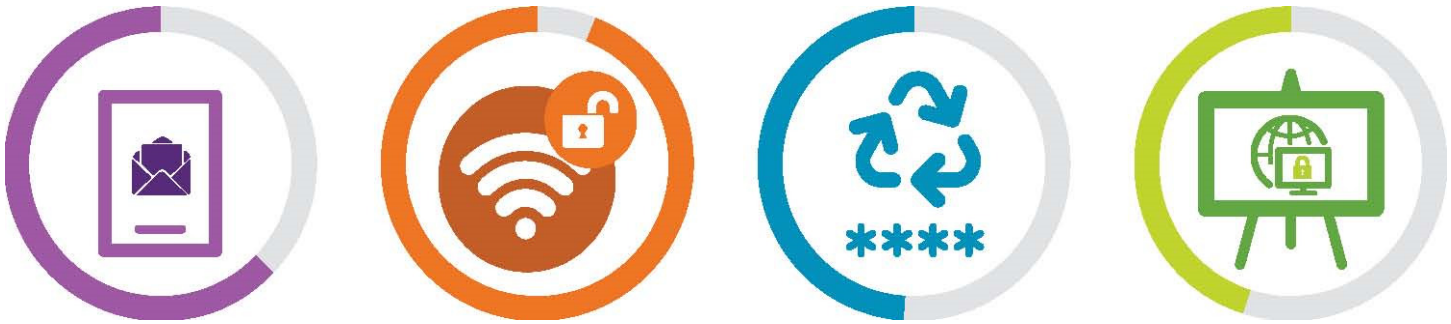
多くの企業は、内外部からのサイバーセキュリティ脅威を回避するため、長い道のりを歩いてきました。しかし、テクノロジー改革のペースは加速することから、状況は複雑化しています。デバイスやオンラインデータの監視は、継続的な取り組みとして実施されているのが現状です。2015年10月半ばの時点では、606件ものデータ侵害が報告され、1.75億以上ものデータが危険にさらされてしまいました。企業は、自社データのみならず、顧客、従業員の情報保護を最優先に行わなければなりません。

しかし残念ながら、従業員のサイバーセキュリティに関する知識や習慣は、遅れを取っているといえます。セキュリティインシデントの一部は、標準に満たないプランニングやシステムに起因しますが、多くは従業員のミスが原因で起こります。ITのベストプラクティスを意識するだけでは十分ではありません。サイバーセキュリティは、従業員が日々何気なく行うテクノロジー上の「決定」に反映されます。そうした決定事項には、ログイン情報の定期的な変更、予測可能なパスワードの回避、フィッシングの回避など日常的なことが含まれます。2014年、米国インターネット犯罪苦情センターは、269,422件の苦情件数を確認し、それらの損失額は8億ドル以上であったことを報告しました。エンドユーザーはこれまで以上にテクノロジーに精通していますが、危険を顧みない習慣は存続しています。

調査方法

従業員のサイバーセキュリティに関する意識の現状を探るため、CompTIAは、米国の従業員1,200人を対象に、日常のテクノロジー使用、サイバーセキュリティに関する意識、セキュリティ習慣などに関するオンライン調査を実施しました。同時に、実世界における消費者の行動を直接観察し、特定の行為がいかにITセキュリティリスクにつながるかを実証するため、実験を実施しました。

調査から見られた重要所見:



63%

仕事用のモバイルデバイスを、私用用途にも使用している従業員の割合

94%

ノートPCやモバイルを、公共Wi-Fiネットワークに接続して使用したことがある従業員の割合

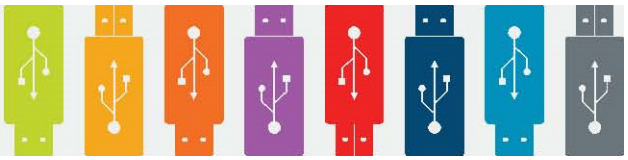
49%

ログイン（ID+PW）を少なくとも10セット所有している従業員の割合。しかし、この中で、一致なくユニークログインを使用している割合はわずか34%

45%

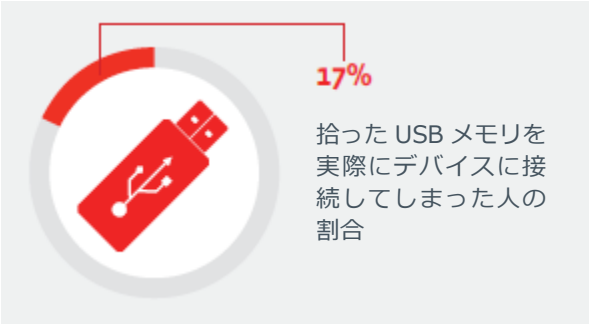
勤務先企業からサイバーセキュリティトレーニングの提供がない従業員割合

USBの落し物 - 実証実験



消費者向けテクノロジーの脅威として注目されたサイバーセキュリティインシデントの一つに、Stuxnetがあります。USBウイルスは、この悪名高きワームに拡散され、2010年には米国とイスラエルは、イランの核遠心分離機に侵入するため意図的に使われたといわれています。マルウェアがプログラムされたUSBメモリは、デバイスや重要インフラを素早く感染させることが可能です。

2015年8月から10月の間、CompTIAでは、USBメモリを発見した消費者のサイバーセキュリティ習慣を観察するため、実証実験を行いました。調査では、頻発するサイバーセキュリティ攻撃やデータ侵害、それらの公表にもかかわらず、消費者のセキュリティ意識は低く、無意識に自身のデバイスやデータを危険にさらしている、という仮説を検証します。



実験では、200個のUSBメモリが用意され、シカゴ、クリーブランド、サンフランシスコ、ワシントンDCを含む空港、コーヒーショップ、ビジネス街の公共広場といった交通量の多い場所に置かれました。USBメモリにはテキストファイルがプログラムされています。USBメモリが接続されると、指定されたアドレスへのメール送信や、追跡可能なリンクのクリック（接続）を行うよう指示が出る仕組みです。

数週間の実験の後、全体の17%がUSBメモリを拾い、自身のデバイスに接続、テキストファイルを開封、見覚えのないリンクへの接続または、指定されたアドレスへのメール送信といった一連を行ったことが確認できました。また、消費者のテクノロジーリテラシは、USBメモリの扱われ方に無関係であることが分かりました。その例に、サンフランシスコ国際空港では、多くのIT業界で働く人たちがUSBメモリを接続してしまいましたし、多国籍企業のオフィスビルにあるセキュリティ会社においてもメール送信を行ってしまったのです。送信されたメールの中には、拾ったUSBはウイルス感染しているか聞いてくるものもありました。つまり、リスク自体は理解しながら、自身のデバイスを危険にさらしているという矛盾があるのです。見も知らぬUSBメモリ - または保護のないWi-Fiネットワークや、特定できない相手からのメール - を盲目的に信用してしまうことは、個人だけのリスクにとどまりません。上の所見で見られるように、IT知識のあるエンドユーザーであっても、疑わしいテクノロジーに対して、安全といえない意思決定を行いかねないのです。これは、（知識のみならず）強固なサイバーセキュリティ習慣を身につけることがいかに難しいかということを表しています。

従業員のテクノロジー使用 & サイバーセキュリティの意識

モバイル使用は、従来テクノロジーの使用をしのぐ勢いです。多くのモバイル導入により、生産性の向上が望まれる一方で、企業やエンドユーザーが保護しなくてはならないエンドポイントが派生します。多くの従業員は、仕事上でデスクトップコンピュータおよびスマートフォンに依存（それぞれ78%）、その次にノートPC（73.5%）に依存しています。また、新しいテクノロジーにも前進が見られます。従業員の半数以上（54%）が、定期的にタブレットを使用し、5分の1近く（20%）がウェラブルデバイスを使用しています。

さらに、仕事用とされるモバイルデバイスは、オフィスを越え使用されます。3分の2近くの従業員（65%）は、勤務先から提供されたモバイルデバイスを使って自宅で仕事をしています。61%は、コーヒーショップ、空港、その他の公共の場所などの外出先で使用しています。また、63%は、ショッピングからソーシャルメディアのアクセス、ネットバンキングといった私用目的のために仕事用モバイルデバイスを使用しています。

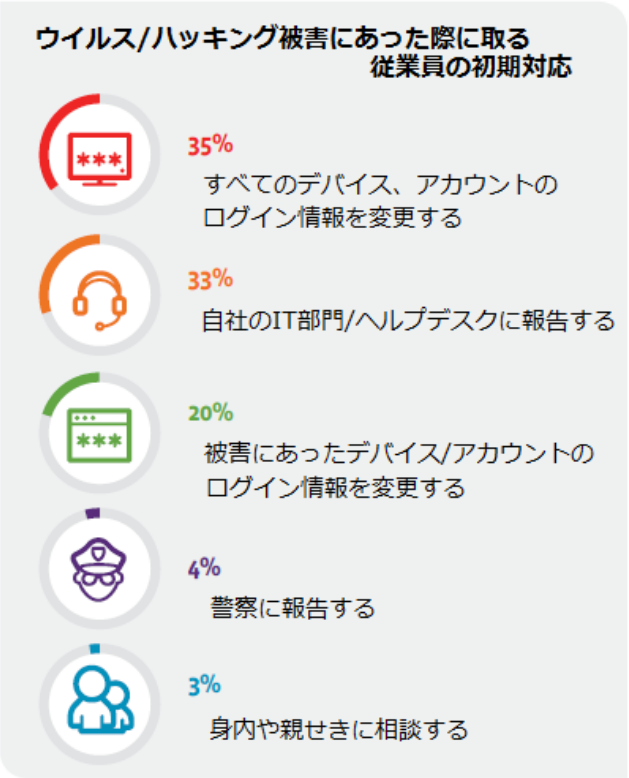
すべての従業員が同じような状況とは限りませが、IT部門は従業員のデバイス習慣に備える必要があります。男性は、女性と比較して、自宅（73%）および外出先（68%）で仕事用のデバイスを使用する傾向が強いことが分かっています（女性はそれぞれ、59%、55%）。ミレニアル（21歳から34歳）は、他のどの世代と比較しても、自宅（74%）、外出先（73.5%）での使用、私用目的の使用（79%）が高くなります。

サイバーセキュリティに対する認識から、従業員が最も恐れるサイバー脅威を垣間見る

サイバーセキュリティは、ITに関連するあらゆる出来事や人物、プラクティスすべてを包括します。従業員のサイバーセキュリティに対する印象は様々であることから、彼らが恐れるリスクや脅威を見ることができます。また、彼らのサイバーセキュリティに対する認識や、経験にはギャップがあることも分かります。

従業員は、サイバーセキュリティを「個人情報の盗難」（36%）と関連付ける傾向があり、その差は「ハッカー」（18%）と比較して倍になります。「マルウェア」と関連した割合はわずか8%でした。また、従業員の5分の1近く（19%）が、過去2年間にハッキング被害にあったことを報告しています。Ponemon Instituteでは、2014年だけ見ても47%の米国成人がハッキング被害にあったと発表しています。さらに、おおよそ3分の1（32%）の従業員が、過去2年間における仕事用デバイスの感染を報告しています。ミレニアル世代は、データ侵害（27%）、デバイス感染（42%）の被害が高い傾向にあります。

データ侵害にあった際、多くの従業員は、自身で何らかのアクションを取る、またはIT部門に報告すると回答しています。ハッキング被害にあった場合、3分の1以上の従業員が、すべてのデバイスおよびアカウントのログイン情報を変更するとしています。これは、多くの従業員がパスワードを複数のサービスに再利用していることから、正しい選択といえるでしょう。一方で、5分の1は、被害や感染のあったアカウントのみログイン情報を変更するとしています。また3分の1が、自社のIT部門に状況を報告するといいます。



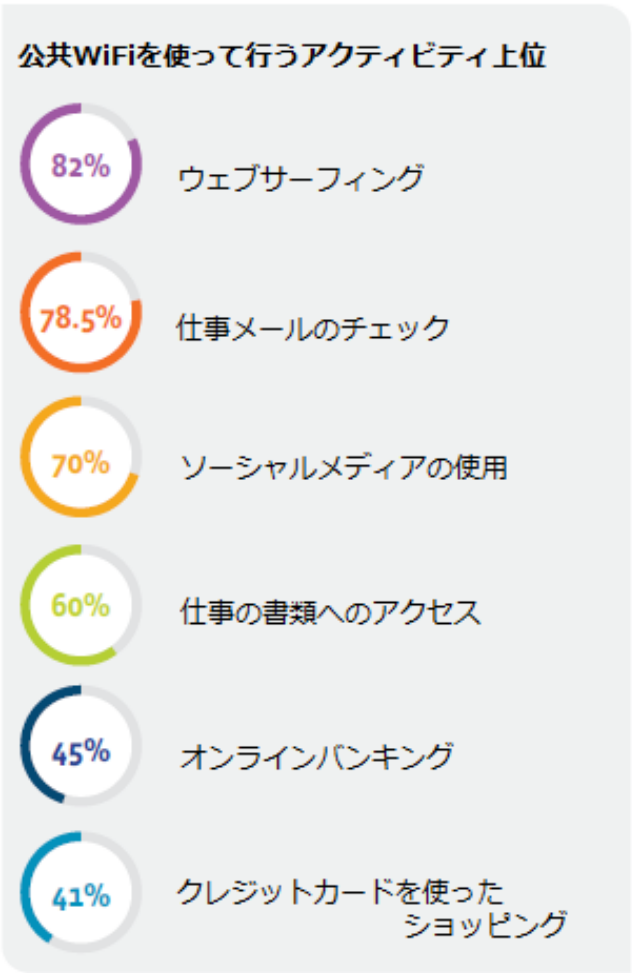
従業員の日常のセキュリティ習慣 & 予防対策

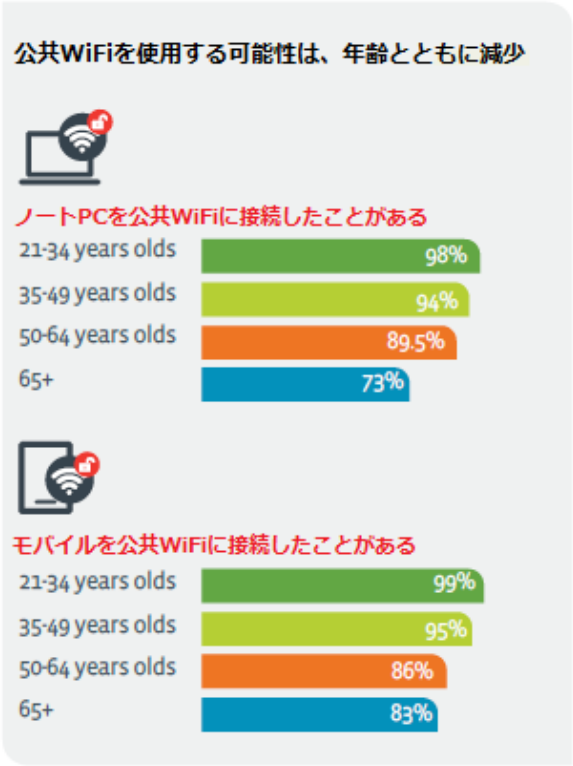
従業員の大部分は、誤ったセキュリティ習慣が引き起こすリスクを認識しているものの、そうした知識を適用していないのが現状です。WiFi接続からオンラインアカウントの管理まで、彼らのIT全般における行動は、脆弱性の程度を反映しています。

従業員の間で広まる公共WiFiの使用

従業員は、内在するセキュリティリスクにもかかわらず、保護されていないWiFiネットワークへのデバイス接続を行っています。ほぼすべての従業員（NET94%）が、ノートPCまたはモバイルデバイスを公共WiFiネットワークに接続したことがあり、そのうちの69%は、接続中に仕事に関連するデータを処理したことがあると答えました。テクノロジーの性質からか、非セキュアなネットワークの使用は、年齢に関連します。

さらなる懸念に、非セキュアネットワークに接続しながらの機密性の高い個人または企業データの扱いがあります。エンドユーザーが行うアクティビティの上位には、比較的安全なものから、明らかにリスクの高いものが含まれます。





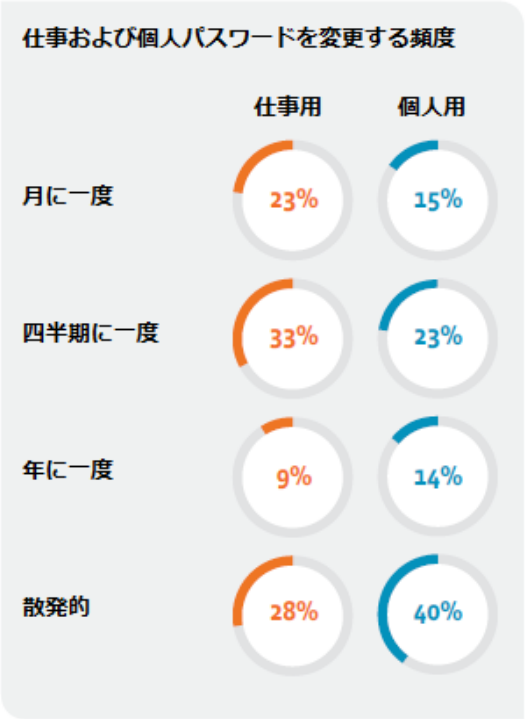
不適切なパスワード習慣

私たちは、まさにパスワードの世界に生きていて、従業員はアカウントの管理や対応に追われています。増加するオンラインアカウントに、パスワードの再利用という問題がある環境では、個人や企業のデータ防御は必然的に悪化の一途をたどってしまいます。

従業員の半数（49%）は、少なくとも10のログイン（ID+PW）を所有していますが、その中で一致なくユニークログインを使用している割合はわずか34%にとどまります。さらに、36%は、私用アカウントに仕事のメールアドレスを登録していて、38%は、私用アカウントに仕事で使うパスワードを使用していることが分かりました。

つまり、いくらかの従業員は、仕事上アカウントのログイン情報を、複数の個人向けサービスに再利用していることです。これは、組織にとって漏えいとなるポイントを増加させることとなり、こうした従業員の行動を変えるには、トレーニングなしに対処することは困難となります。

アカウント管理に関しては、従業員は全般に企業データにより多く注意を払い扱っているようです。彼らは、仕事のパスワードの更新には、個人用ログインよりもより安全なアプローチを取っています。しかし、全体の37%が、パスワードの更新を「一年に一度」または「散発的」に実施していることに関して、IT部門は心地よく思わないでしょう。



多くの従業員は、利用可能なアカウント防御があることを知らず、利便性のためセキュリティを疎かにしてしまいがちです。例えば、41%は二段階認証に知識がなく、27%は聞いたことはあっても概念について理解していません。自発的に二段階認証を適用している割合は、半数以下（48%）にとどまりました。

地域や年齢の違いも、従業員の習慣に影響を与える要因のようです。欧米の従業員は、二段階認証が何であるのかを最も認識していて（38%が認識。全体の平均では32%）、また、自身のアカウントに適用している割合が高いことが分かりました（55%）。年代別に見ると、ミレニアル世代が最も高く46%。その後にジェネレーションX世代31%、ベビーブーマー世代21%となりました。同様に、ミレニアル世代は、自発的に二段階認証を適用している割合が最も高く（63%）、ジェネレーションX世代51%、ベビーブーマー世代34%と続きます。

オンラインでの個人情報の提供が増加

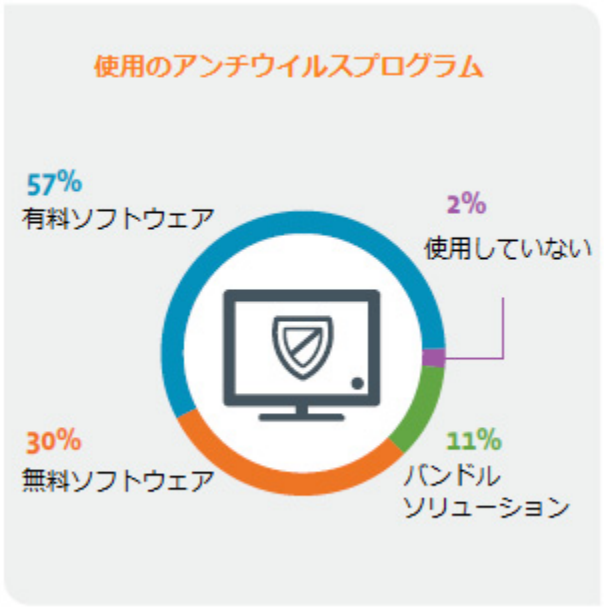
オンライン上のコンテンツやサービス、プロモーションと引き換えに、消費者は少なくともメールアドレスの提供が条件として求められるケースが増えています。一般に、従業員は、様々なオンラインアカウントに自身のメールアドレス、氏名、生年月日などを提供することにさほど抵抗を感じません。ですが、特定の情報に関しては、チャネルにより提供を判断または拒否しているようです。クレジットカード情報をソーシャルメディアアカウントに提供することにためらいを感じないとするのは、ごくわずかの従業員でした（8%）。しかし、その提供先がEコマースサービスや、エンターテイメント系アカウントになると、ハードルが下がるようです。それぞれ41%、35%の従業員は、カード情報の提供を行うと回答しました。比較的少数（37%）の従業員は、ソーシャルメディアに住所を提供していますが、4分の3近く（71%）は、Eコマースサービスのサイトに住所を提供しているといいます。

米国のソーシャルセキュリティ番号は、すべてにおいて機密性の高い情報という認識があります。ソーシャルメディアまたはEコマースサイトに番号を提供する場合があると回答したのは、従業員のわずか6%でした。また、運転免許証や身分証明となる番号にも同様の認識が見られます。それら情報を、ソーシャルメディアのアカウントに提供する場合があると回答したのは7.5%。エンターテイメント系サービスへの提供は7.5%。Eコマースサイトのプロフィールへの提供は7%でした。

従業員とIT部門に共通する、ハードウェア保護の負担

従業員デバイスの保護は、本人およびIT部門で共有される負担です。当然のことながら、一部の従業員には、他者よりも厳しい保護体制が適用されていることもあります。

プラス面としては、ほぼすべての従業員が何らかのアンチウイルスプログラムを使用していること。使用していない割合は2%であったことです。大半（57%）が有料のソフトウェアを使い、30%が無料のオンラインソフトウェアを使用。11%は、デバイスとバンドルされているアンチウイルスソリューションに依存しています。



オペレーティングシステムに関しても同様に良好な結果となりました。ほとんどの従業員は、自身のデバイスを最新の状態に維持するため、積極的な取り組みを行っていると報告しています。これは、「アップデートが利用できます」というプロンプトを無視したり、自動再起動のリマインダを無視するといった、多忙な従業員の典型的な行動に反する結果です。回答者の多くは、自身でオペレーティングシステムのアップデートを行うよう努めているといいます。

年齢別にみると、ミレニアル世代は、仕事で使用するコンピュータのオペレーティングシステムアップデートの管理に関してIT部門に依存する傾向が低いことがわかっています。割合としてはわずか29%でした。この割合は、ジェネレーションX世代では43%、ベビーブーマー世代では46%でした。ミレニアル世代は、アップデートのプロンプトが上がってから1週間以内に実施する傾向の高いことも分かっています。（22.5% vs. 16%ジェネレーションX世代 vs. 10% ベビーブーマー世代）

十分注意せず扱われているUSBメモリ

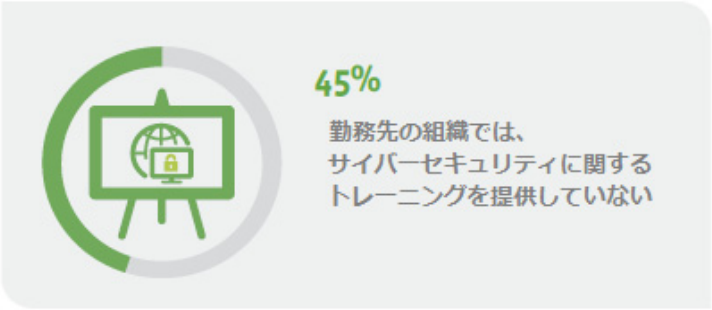
無料かつ商業向けのファイル共有アプリが普及しているにもかかわらず、多くの従業員（58%）が、デバイス間のファイル転送にUSBベースのストレージデバイスに依存しています。これは、認識のないUSBメモリを使用してしまう傾向が検証されていることから、多くのセキュリティリスクを意味しています。

従業員の3分の1以上（35%）は、ファイルのコピーまたは転送のためにUSBメモリを借りた経験を持ちます。また、公共の場に落ちているUSBメモリがあると仮定した際、22%はそれを拾うだろうと回答しています。この回答をしたグループのうち、84%が、自身のデバイスに接続する行為に至る可能性があるとしています。

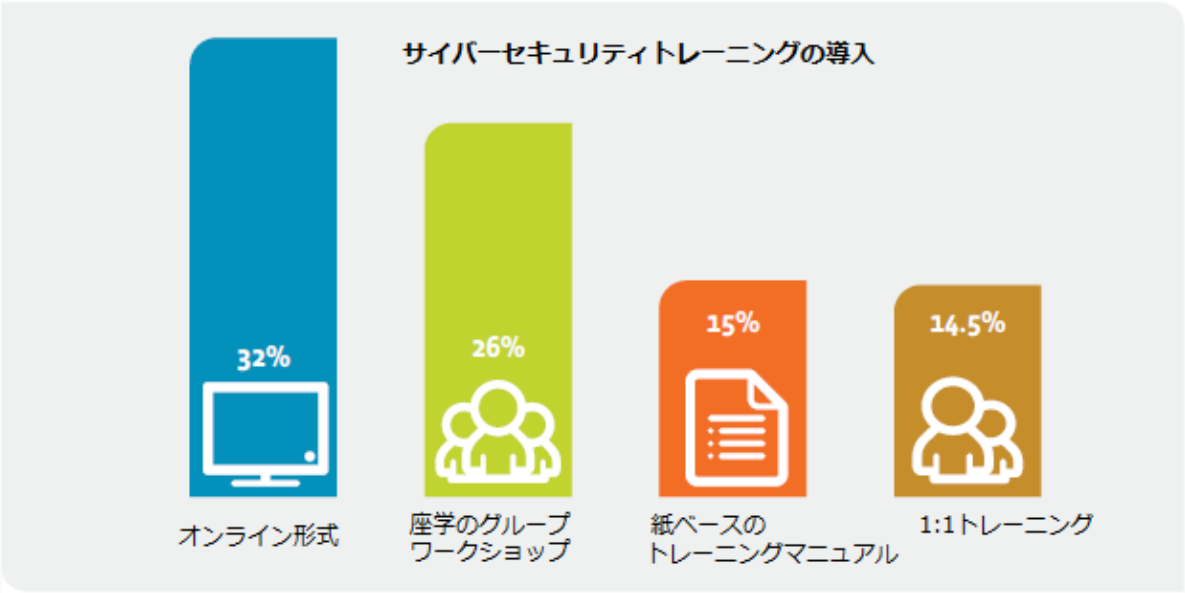
ミレニアル世代は、日頃よりUSBメモリを使用する傾向が最も高いだけではなく（ミレニアム世代 74% vs. 55% ジェネレーションX世代 vs. 47% ベビーブーマー世代）、認識のないメモリスティックを信用してしまう傾向にあります。ミレニアル世代の40%は、公共の場に落ちているUSBメモリを拾う可能性が高いことが分かりました。世代別で見ると、ジェネレーションX世代で20%、ベビーブーマー世代で9%でした。また、米国内では、西部地域の従業員が、落ちているUSBメモリを拾ってしまう可能性が最も高い事が分かりました（63%）。

サイバーセキュリティのトレーニング & 教育

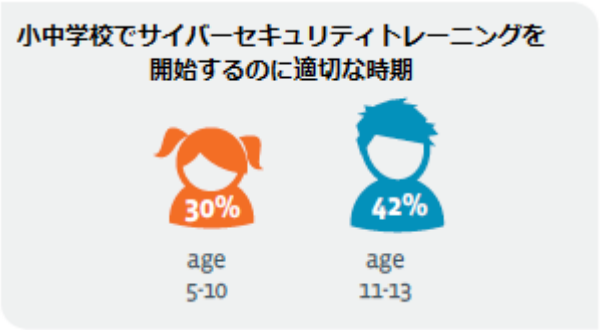
多くの従業員は、サイバーリスクに対処するために必要なトレーニングを受けていないのが現実です。従業員の45%は、勤務先の組織ではサイバーセキュリティに関連した教育を提供しておらず、エンドユーザーが取るべきベストプラクティスについても言及されていないと報告しています。ITセキュリティを、新人研修やプロフェッショナルの育成プログラムに組み込んでいない組織は、従業員に提供されるデバイスの数や、多くの従業員やスタッフに処理される機密データを考慮した際、非常に脆弱であることが分かるでしょう。



サイバーセキュリティトレーニングを実施している組織では、その多くがオンラインおよび対面の座学的な学習形式の組み合わせを導入しています。



大人にもサイバーセキュリティ教育の欠如の広がりが見られることから、子供には小中学生といった早い段階で必要なスキルを鍛えるべきではないかという意見があります。ほぼ3分の1の従業員は、学生のためのサイバーセキュリティトレーニングは、5歳から10歳の間に始められるべきだと感じています。42%は、11歳から13歳の間に始められるべきだとしています。また、3%以下の回答者が、サイバーセキュリティは、小中学生のカリキュラムに組まれるには不適切なトピックであると感じています。



結論

この10年間で、サイバーセキュリティは、主に政府や企業のITマネージャに監視されていたニッチな領域から、トップ記事、消費者の注目を集める大きな問題となりました。しかし、認知の上昇にもかかわらず、多くの従業員のサイバーセキュリティへの理解・行動は、デバイスや個人情報の保護の点において、それぞれ低水準といえます。

このような状況は、ITのある概念から成るものかもしれません。従業員は、アンチウイルスソフトウェア、ファイアウォール保護、その他ITプロトコルがインストールされていることから、オンラインで何を行おうと安全である、または、何か起きたとしてもテクノロジーで守られていると思っているのかもれません。すべてのデータ侵害やID盗難のインシデントがニュースの見出しになるわけではない、といった考えも個人の脆弱性を過小評価してしまう原因でしょう。

同時に、消費者向けテクノロジーのエコシステムが活性化していることから、デバイス使用の線引きが非常にあいまいになっています。従業員は、様々な個人および企業ツールを使用しますが、仕事用デバイスは仕事目的だけに使用されるとは限られません。こうした混合が生じていることから、組織に責任が問われることになります。組織は、従業員が「良好な」サイバーセキュリティプラクティスを理解していること、また、それを実施できるスキルを備えていることを確実にしなければなりません。

従業員は、サイバーセキュリティトレーニングを通じて取り組むべき課題が多くあります。人事、IT、実行機能すべてにおけるビジネスリーダーは、脅威、ソフトウェア、デバイスの状況は変化を続けることから、従業員・スタッフの教育により積極的なアプローチを取らなければなりません。優秀なトレーニングプログラムは、サイバーセキュリティの知識や意識を提供するだけではなく、エンドユーザーの行動を形作り、情報に基づいた安全な選択を行うことを教えます。

様々な点において、エンドユーザーはこれまで以上にテクノロジーに精通していますが、必ずしも安全面にも反映されているとは限りません。IT環境は複雑化が進み、対策が不十分であれば代償も高くつきます。エンドユーザーは、テクノロジーの精通と安全性の両方を確保することが必須です。

調査方法：
この調査は、Blackstone Groupにより、Instantly Inc.のオンラインパネルを使用し実施されました。パネルには、仕事上でコンピュータを使用する米国のフルタイム従業員1,200名が参加しました。調査結果は米国のワークフォース全体を示すよう、年齢、性別、企業サイズにクォータ法（割当法）が使用されています。

ソース：
データ侵害に関する報告書、Identity Theft Resource Center 2015/9
http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf
ITセキュリティ動向調査、CompTIA 2015/3
https://www.comptia.org/resources/trends-in-information-security-study（英語）
http://www.comptia.jp/cont_library.html （日本語）
2014インターネットクライムリポート、連邦捜査局 2015/5
https://www.fbi.gov/news/news_blog/2014-ic3-annual-report
アメリカ成人の半数がハッキング被害に、CNN Money 2014/5
http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/