ivanti

2023 注目点 - 経営陣のセキュリティ

Ivanti の新しい調査が示す、経営幹部が直面する真のリスク

Ivanti のサイバーセキュリティステータスレポートシリーズの一部

経営陣のサイバーセキュリティ脅威を遮断する

通常、組織は経営陣のサポートが優れたサイバーセキュリティを妨げるとは考えていません。当社が初めて発表する「Press Reset」レポートでは、経営陣によるコンセンサスがセキュリティの障壁になっていると考えている幹部およびセキュリティ担当者は、全体のわずか21%にとどまりました。これは、もっとも大きな阻害要因である技術スタックの複雑さ (37%) より16ポイントも低い数字です。

しかし、経営陣は、セキュリティチームが以前に認識していたよりも、安全とはいえないセキュリティ行動を実践する可能性が高くなっています。

経営陣が、顧客や企業の機密情報への不正アクセスを意図的に取得したことがあると回答する確率は、実に5倍にものぼります。

経営陣のる3人に1人以上が、フィッシングリンクをクリックした経験があり、これは他の一般従業員一の4倍です。

また、経営陣が会社のパスワードを社外の人物と共有している確率は4倍にのぼります。

最も標的にされやすい従業員グループである経営幹部が、組織の義務に賛同すると言いながら、セキュリティプロトコルを頻繁に無視する場合、彼らをいったいどのように保護すればよいのでしょうか。

ivanti

このレポートは次の点を浮き彫りにします。

経営陣が表明している優先事項 (例: セキュリティ方針を支持すること) と経営陣の業務上の行動との間 にかなりのギャップがあること。

いかにエグゼクティブのセキュリティ習慣が、一般従業員よりも、サイバー攻撃や侵害に対してきわめて高いリスク をもたらしているか。

経営陣と、経営陣のセキュリティを確保するチームとの間にある不信感 により、経営陣は社内のサポートに依頼するのではなく、社外の IT サポートを頼る可能性があること。

組織のセキュリティを確保するための実践的な方法 を、舞台裏でひっそりと実行します。その間に、チームと一緒に、セキュリティプログラムに対する経営陣の真の賛同を得るために必要な相互信頼を回復することができます。

ivanti

セキュリティのリーダーは、高い能力を持ち、高いアクセス権を持つ人物が、固有のセキュリティ上の脅威となることをすでに知っています。むしろ、Ivanti の最新の調査は、問題の規模を強調し、経営陣のセキュリティの例外が組織的なリスクの大きさにつながることを示唆しています。

経営幹部の人数は限られているため、彼らがもたらす潜在的な脅威を過小評価し、幹部に対しては厳格なサイバーセキュリティ対策を免除したくなるかもしれません。

しかしながら、最近の研究では、そのような考えがまったくの間違いであることが明らかになっています。経営幹部の職場での行動は他とははっきりと違っており、彼らは他とは比べようもないアクセス権と影響力を享受しています。

「この研究は、彼らの習慣および行動に注目し、これらを修正する必要があることを明確に示しています」

ジュリアーノ・リグオーリ
Kenovy社CEO

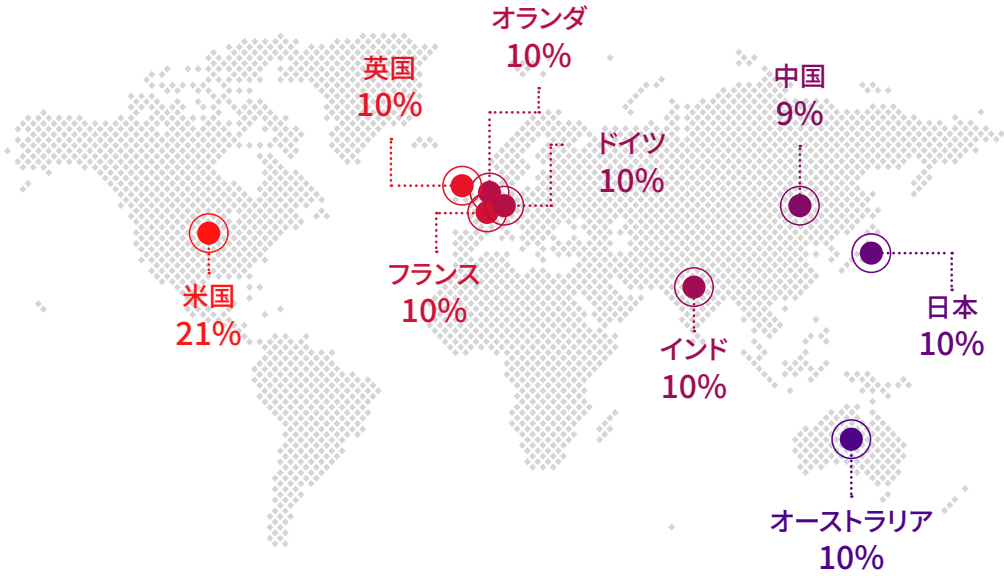
目次

ivanti

調査方法

Ivanti は、2022 年第 4 四半期に 6,500 人以上の役員、サイバーセキュリティ専門家、一般従業員を対象に、今日の脅威を理解し、未知の将来の脅威に対して組織がどのように備えているかを明らかにするために調査を実施しました。

本レポートでは、経営幹部に焦点を当て、経営幹部がセキュリティ上の危険要因なる態度と行動について考察します。



一般従業員
5,202人

セキュリティ担当者
902人

経営幹部
454人

01

経営陣の行動のギャップ:

経営陣がセキュリティについての見解と、経営陣の行動の傾向との違い

ivanti

現在の問題

経営陣の言動には大きなギャップがあります。

経営幹部はサイバーセキュリティに対して強気であり、ほぼ全員が組織のセキュリティ指令を支持していると述べています。
しかし、Ivanti の調査によると、リーダーの言動の間には大きな矛盾があります。これを行動のギャップと呼んでいます。

行動のギャップ：経営幹部の信念と行動の相反状態

	経営陣たちの発言：	経営陣たちの行動：
セキュリティカルチャー	経営陣の96%は、経営幹部は組織のサイバーセキュリティの義務に対し少なくとも一定のレベルで協力的であるか、または投資を行ってきていると回答しています。	**CxOの49%は、過去1年間に1つ以上の**セキュリティ対策を無視するよう要求したことがあります。
トレーニング	78%が、自分の組織がサイバーセキュリティのトレーニングを必須業務として提供していると答えています。	**77%が、誕生日やペットの名前といった**覚えやすい文字列をパスワードとして使っています。覚えやすい文字列をパスワードとして使っています。 また、経営幹部は、友人、家族や外部のフリーランサーなど、権限を持たないユーザーと仕事用デバイスを共有する確率が3倍も高くなっています。
フィッシング	経営幹部の88%は、マルウェアやフィッシングといった脅威を認識し報告する用意ができていると回答しています。	フィッシングの標的となった者の35%はリンクをクリックしたことを認めています — なかには金銭を送ってしまったケースもあります。

適切な手続きを踏む時間がないのか、例外意識（「ルールが私に適用されるはずがない」）があるのか、あるいは他の要因によるものなのか、経営陣は単純に、他の従業員とは異なる行動（読んで字のごとく、よりリスクの高い行動）をとる傾向があります。

24%

業務用アプリケーションで、オンボーディング中に発行された元のパスワードを変更していないと回答している経営幹部

14%

元のパスワードを変更していない現場の一般従業員

重要な理由

無害な回避策どころか、経営陣の行動は深刻な脅威

経験豊富なセキュリティ専門家の多くは、経営陣のリスクの高い行動が存在することを知っていますが、他の戦略的優先事項を優先して経営陣のサイバー衛生への対応を後回しにしがちです。

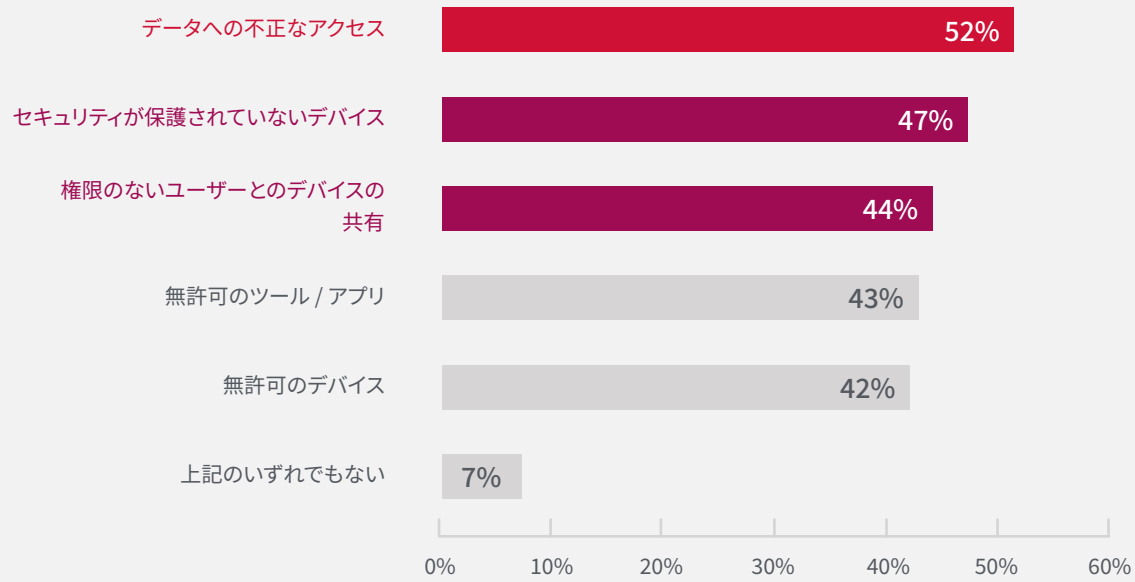
セキュリテ担当者は、限られた時間とリソースを、最も可能性の高い危険なリスクから組織を守るために使う必要があります。では、なぜセキュリティチームは、プログラムに賛同し、そのための予算まで確保したと言うリーダーを守るために、さらに時間を費やさなければならないのか、という論理になります。

Ivanti の調査によると、経営陣のセキュリティは問題であるだけでなく、ほとんどの組織を悩ませるシステム的な問題でもあります。

実際、セキュリティの専門家が自社の組織に高いセキュリティリスクをもたらす要因として挙げたものとまったく同じ項目が、経営陣が自認する習慣と直接対応しています。

Q: 質問：これらのうち、あなたの組織に高いセキュリティリスクをもたらすものはどれですか？

注：回答者がセキュリテの専門家 to 担当者であった場合は、複数のオプションを選択した可能性があります。



経営幹部の3人に1人

が、許可されていないファイルやデータにアクセスしたことがあると認めています。

経営幹部は他の一般従業員に比べ3倍の確率で

仕事用デバイスを家族や友人と共有しています。

経営陣のセキュリティ行動には権限が関与

残念なことに、セキュリティチームと経営幹部の間の不平等なが問題を悪化させています。

限られた作業処理能力、疲労、燃え尽き症候群のため、セキュリティ

セキュリティ担当者は、ベストプラクティスのセキュリティポリシーを導入しようとしても、その保護しようとしている対象の最前線のユーザーから公然と苦情を受けたり、シャドー IT という回避策を取られたりした経験が何度あるでしょうか。

不透明な雇用市場の中で、セキュリティチームが、予算や雇用を承認する権利を握った経営陣に、より良いサイバー衛生とセキュリティの実践を強制することをどのように期待できるでしょうか。

専門家はしばしば経営陣からの圧力に屈してしまいます。

セキュリティチームが経営幹部の行動に影響を与えるのが困難な理由

燃え尽き症候群

CISOは過剰な負担を負っており、燃え尽き症候群にかかっています。CISOの60%が、過去12か月間で燃え尽き症候群を経験したと回答しており、61%はCISO/CSOに過剰な期待が寄せられていると述べています。[1]

カルチャー

上司 (または上司の上司) がプロトコルに反するお願いやワークアラウンドを求めた場合、セキュリティ担当者が彼らの要求を退けることに抵抗があるのは当然です。

強力な「セキュリティファースト」のカルチャーがなければ、従業員やセキュリティの専門家は、権限を持つ層の安全とはいえない要求に単に従うようになる可能性があります。

「今回だけ」イズム

「今回だけ」または「あなたのためにだけ」という言い訳には、大きな魅力があります。

このときセキュリティの専門家は、CEOに対しルールを強制することを気まずく感じている可能性があるかもしれません。特に、過去に例外が認められている場合はその可能性が高いでしょう。

「今回だけ」ということはほとんどなく、経営陣が回避策を講じたり、後戻りしにくい前例を作ったりするリスクが高まります。

02

組織にとってきわめて大きい経営陣のリスク:

経営陣のセキュリティにおける悪習慣がサイバーセキュリティに与える影響

ivanti

現在の問題

リスクの高い経営陣の行動が重大な結果をもたらす

人数は少ないものの、経営陣は非常に高度な自動アクセス機能を持ち、セキュリティ行動にも懸案が見られます。このような経営陣は、一般従業員よりもはるかに大きなセキュリティリスクを組織にもたらします。

保護されていない、第一級幹部のコネクション

経営陣の45%

が、少なくとも月に1度は家族や友人に仕事用デバイスを使用させています。

これは、他のすべての一般従業員の3倍にものぼる数字です!

経営陣のほぼ5人に1人

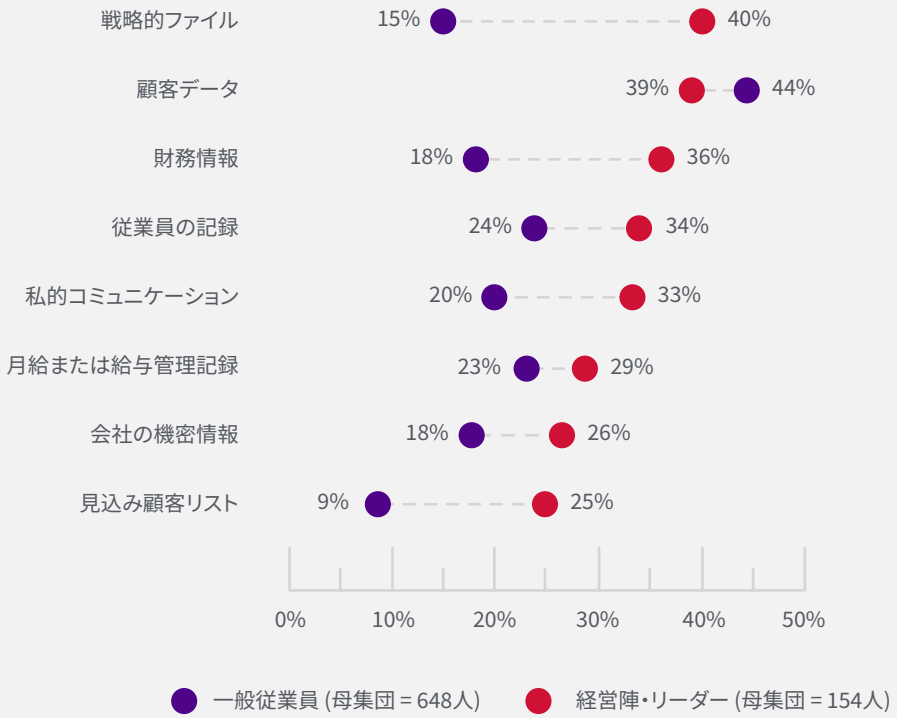
が、自分の仕事用パスワードを社外の人物と共有したことがあります。

このような経営幹部は、セキュリティの訓練を受けておらず、組織の安全を守ることにも投資していません。ファイルやネットワークに深くアクセスできる組織のデバイスを使っているにもかかわらずです。

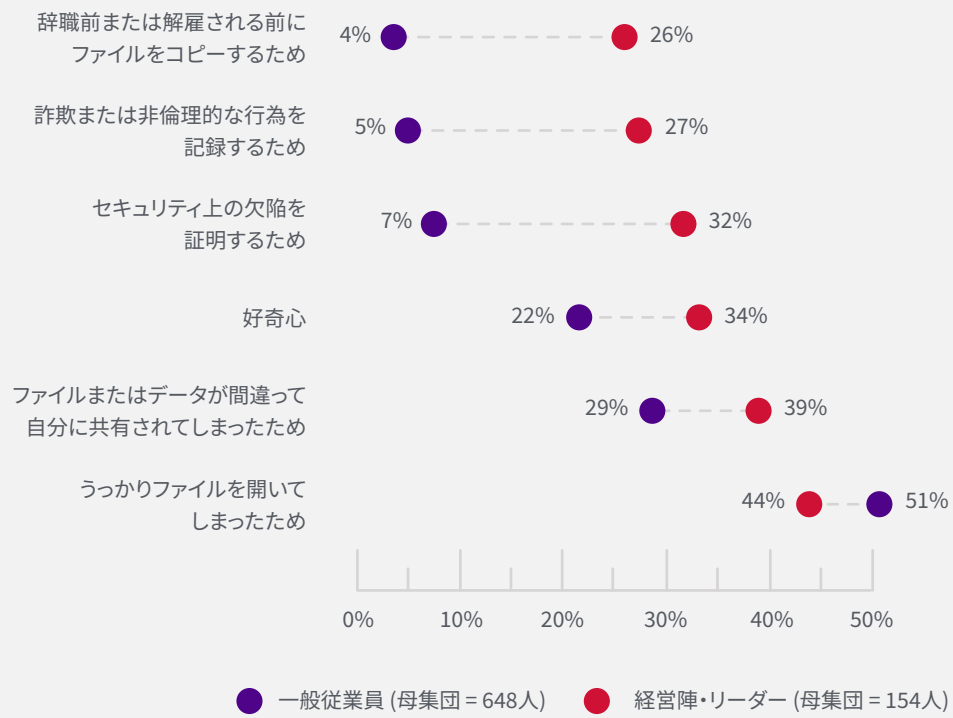
経営陣の不正アクセス

経営陣の 3 人に 1 人 (34%) が業務で許可されていない情報にアクセスしたことがあると認めています。また、3 人に 2 人近くが、それらのファイルやデータにアクセスしたときに編集できたと答えています。

質問: どんなファイルにアクセスしましたか？



質問: 許可されていない情報にアクセスしたのは何故ですか？



注：各グラフでは、すべての回答者は自分のロールに必要がないファイルにアクセスしたことがあることを事前に確認しています。

重要な理由

経営陣のセキュリティの例外を認めると、リスクが高まる

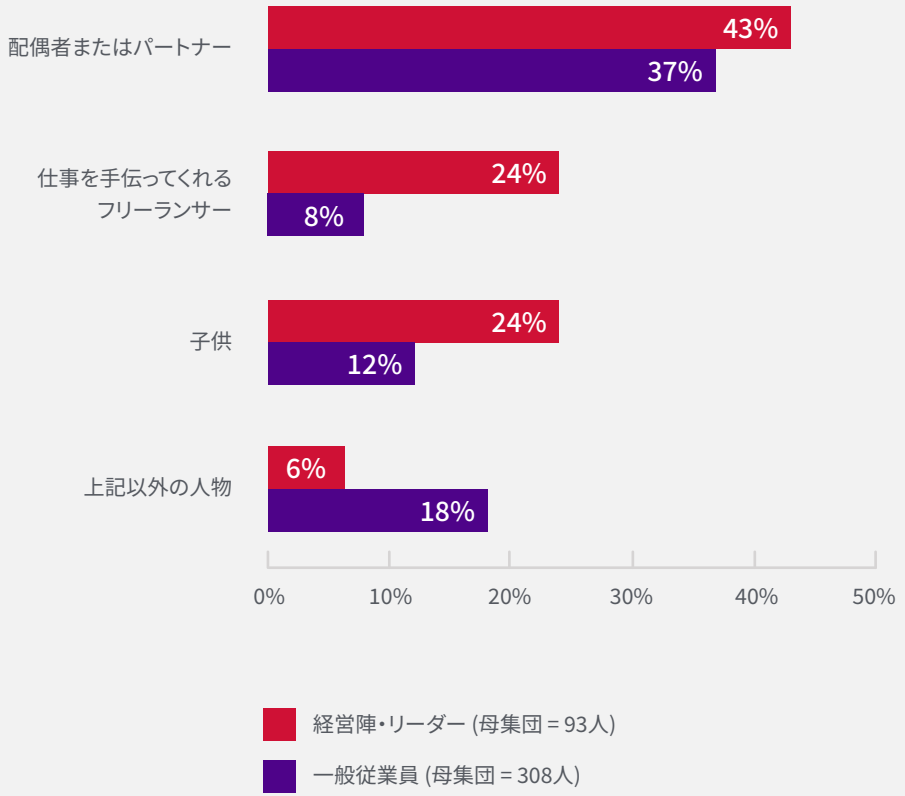
多くの経営陣は、時間や手間を省くために、重要な手順を省略します。しかし、Ivanti の調査によれば、そのリスクはこれまで理解されていた以上に浸透的だということがわかりました。

経営陣は、自分たちの時間が貴重であり、限られていると、合理的に考えています。たとえば、家族や同僚、第三者の技術サポートと、パスワードやデバイスを共有することは、リスクの少ない時間の節約になると考えられている可能性があります。

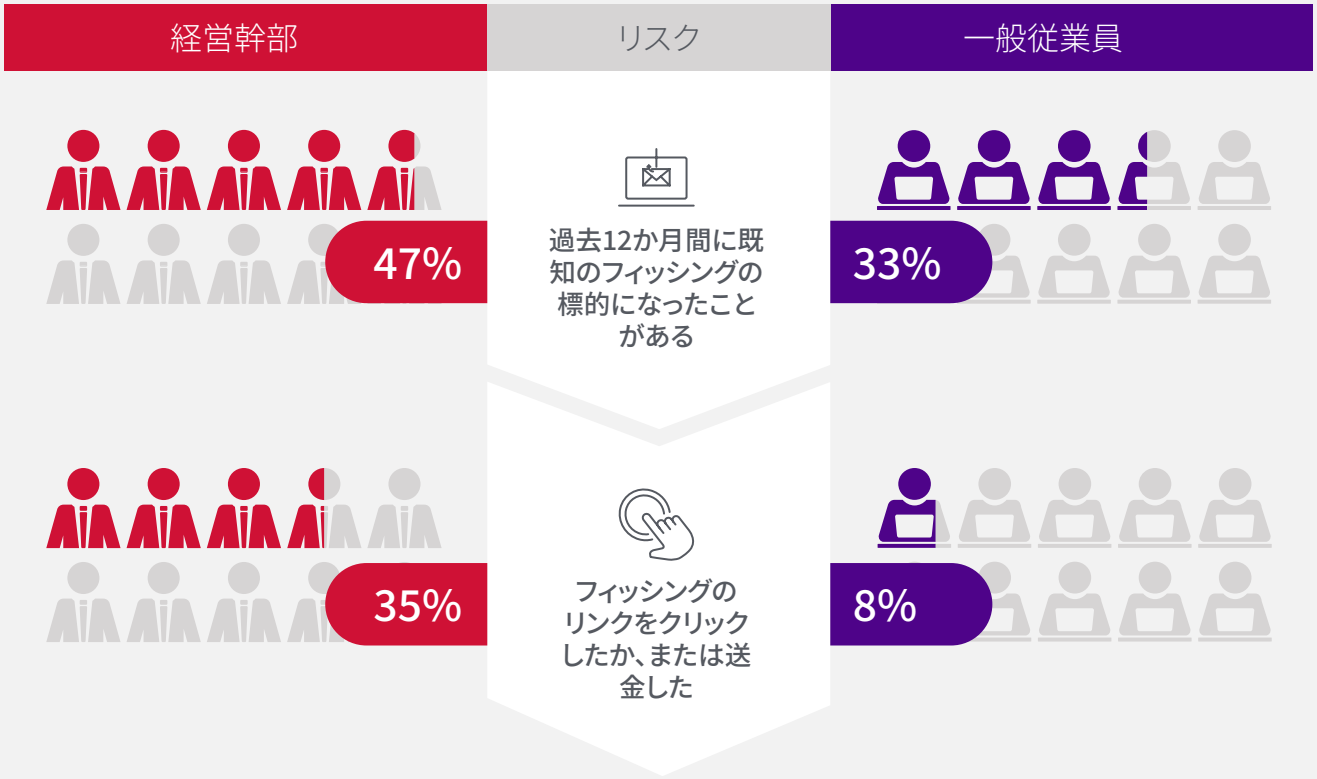
27%

少なくとも月に1度は友人や家族に自分の仕事用デバイスを使わせると答えた経営幹部 — その他の一般従業員では、同様の回答をした者は全体のわずか6%です。

質問: 自分のパスワードを誰と共有したことがありますか?



経営幹部は一般従業員よりも高いフィッシングのリスクにさらされています



このような高い割合は、ホエールのためにカスタマイズされたスピアフィッシング攻撃の増加によるものかもしれません。攻撃者がクジラを標的にするのは、そのアクセス権と特権のため、時間と労力を多く費しても価値があるからです。

脅威アクターは、金銭的な動機に基づくランサムウェアの犯罪集団であっても、高度持続的脅威 (APT) であっても、貴重なデータソースやネットワーク資産に高いアクセス権で接続している一方で、サイバー衛生の習慣に対する警戒心が低いため、上級経営幹部を明確に標的にしています。

結局のところ、1 人のホエールがより価値のある資産への特別なアクセスを許可しているのに、なぜ平均的な従業員のアクセス許可のために広い網を張るのでしょうか。

「組織が昨年フィッシングにあった可能性は 100% あります。これは、脅威アクターがネットワークへの最初の足がかりを得るための第一の方法です。

私たちは、人々が『よく分かっている』と思い込んだり、フィッシングが過度に明白であると思い込んだりしないようにする必要があります」

ダニエル・スパイサー (Daniel Spicer)
Ivantiセキュリティ最高責任者

実世界への影響

経営陣の交代は理想的なフィッシングの条件を提供する

2015 年、マテルは世間を騒がせたスピアフィッシングの被害に遭い、中国に拠点を置くサイバー犯罪者に 300 万ドルを奪われました。

Infosec[2] がその後に行った事例研究よると、マテルが新しい CEO を採用するという決定を下したことで、悪用されやすいシナリオができたということがわかりました。

2015 年 1 月、マテルは、ブライアン・ストックトン氏の後任として新しい CEO のクリストファー・シンクレア氏を任命しました。新しい CEO の登場は、企業ヒエラルキーにおける新たな権力闘争を引き起こすであろう、上層部の変化を意味していました。

「言い換えれば、サイバー犯罪者はマテルの社内政治や人間関係まで考慮してホエールフィッシングメールを計画したのです」

Infosec の事例研究[2]

03

セキュリティの摩擦:

経営陣とセキュリティ部門との緊張関係を探る

ivanti

現在の問題

経営陣のセキュリティ体験がサイバー衛生を悪化させる

Ivanti の調査によると、経営陣は平均的な従業員よりも 2.5 倍セキュリティ部門に接触する可能性が高くなっています。このこと自体は良い兆候ですが、経営陣はセキュリティ部門とのやりとりを否定的だと考えている可能性が大幅に高くなっています。

経営陣：

2倍

過去のセキュリティとのやりとりを気まずく感じた確率

4倍

承認されていない外部の技術サポートを使用している確率

33%

フィッシングのリンクをクリックしてしまった場合など、セキュリティのミスを安心してレポートできないと感じている確率 (経営幹部10人につき1人以上がこう答えています!)

2倍

経営幹部がそうしたやりとりに気まずさを感じた確率

5倍

経営幹部が業務用のパスワードを社外の人間と共有する確率

エラーを報告することに気後れしてしまう経営陣と、経営陣を守ろうとするセキュリティチームとの間のコミュニケーションの障壁をどのようにして低くすることができるのでしょうか。

注：これらの統計は、経営幹部レベルの従業員をその他すべての一般従業員と比較しています。

データ侵害が経営幹部の最大の懸念事項であることには疑いの余地がありません。堅牢な保護を実現するには、経営幹部はリアルタイムの脅威を検出するAIの優れた能力を今すぐ最大限に活用し、組織資産を強化する必要があります。

ロナルド・ヴァン・ルーン
Intelligent World社CEO、主席アナリスト

重要な理由

組織は強固なサイバーセキュリティプログラムを必要としている

経営陣の回避策が深刻なセキュリティの脆弱性を生み出していますが、その根底には、経営陣の例外主義を容認し、間違いを報告する可能性を低くする企業文化があります。

セキュリティチームは、非難や見下しではなく、誠実で友好的なサポートから、経営陣との信頼と同意を再構築することを優先しなければなりません。

最高経営幹部

組織内でのサイバーセキュリティの戦略的役割を理解し、その取り組みを目に見える形で支持することによって、セキュリティカルチャーをサポート

セキュリティチーム

間違いを犯した人を（罰したり恥をかかせるのではなく）教育することを目的をオープンなコミュニケーションの場を設ける事で、セキュリティカルチャーをサポート

ivanti

経営陣のセキュリティリスクの軽減は解雇時にはさらに急務となる

Ivanti 調査によると、資格情報のデプロビジョニングは全体的に問題であり、セキュリティ専門家は、デプロビジョニングのガイダンスが 3 分の 1 の割合で無視されていると述べました。これは関連するリスクを考えると、衝撃の告白です。

また、調査対象となった経営陣の 26% が、前職で使用可能なパスワード 幽霊資格情報をまだ持っていると答えています。

幽霊資格情報がもたらすリスクは、従業員がデータを持ち出したり、以前の雇用主に恨みを抱いたりする可能性が高い、解雇の時期にさらに高くなります。

Forrester のアナリスト、Jeff Pollard 氏は、次のようにこの結論を支持しています。「解雇や失業はインサイダーリスクの予測因子であり、セキュリティイベントが発生する確率が高くなることがわかっています。このようなことが起きていることを、私たちは長年にわたって見てきました。」[3]

「昔は (内部犯行を成功させるのは) 困難でしかったが、今は簡単です。以前は、ブリーフケースに入れられるものしか持ち出せませんでした。今はテラバイト規模の情報を持ち出すことができます。」

Pete Nicoletti 氏
Check Point Software
北米・中南米担当フィールド CISO [3]

04

解決するための行動:

組織における経営幹部の行動のギャップを解消する

ivanti

解決するための行動

問題に妥協なく光を当てる

Ivanti の調査は、私たちの多くが以前から知っていたことを裏付ける結果となりました。経営陣は、組織のセキュリティの立場にとって独特かつ重大な脅威となります。今、データを手にしたところで、問題に対処する時が来ました。

1. 監査を実施し、
   現在の経営陣の行動ギャップを評価します。
2. 最も簡単で影響の少ないリスクを最初に修正し
   不必要な場合は経営陣との直接的な衝突を避けます。
3. ゲーム化された卓上演習
   により、経営陣は基本的なサイバー衛生と、将来の情報漏えいが各部門に与える影響との間に点を結ぶことを余儀なくされます。
4. 「ホワイトグローブ」セキュリティプログラムを実装します。
   リーダーレベルの従業員よりも一般従業員の人数の方がはるかに多い場合でも、このより小さい利害関係者のコミュニティにきめ細かい注意を払うことで、限られたリソースの投資に対する大きなリターンが得られます。

「経営陣に挑戦し、全員が責任を負うプロセスを構築できるような文化を築く必要があります。簡単なことのようですが、これは真実です。」

AJ Nash 氏
ZeroFox インテリジェンス担当部長兼特別フェロー

20%

グローバルなデータ侵害のうち、内部関係者の攻撃に関連している可能性はこれくらいあります。[3]

ご存じでしたか？

経営幹部は、他のナレッジワーカーと比較して、辞職または解雇される前にファイルをコピーする可能性が6.5倍となっています。

1 監査を実施する

組織内の役員と従業員の行動について最新の情報を得るには、監査を検討します。ここでの目的は、処罰や辱めを与えることではなく、役職に関係なく、すべての従業員にセキュリティガバナンスポリシーが適用されるようにすることです。

内部監査

セキュリティチームと経営幹部(重役レベル以上) との過去12か月間のやり取りをしっかりチェックしましょう。経営幹部とセキュリティチームの両方において、ミスコミュニケーションやリスクが高い行動のパターンを探してください。

たとえば、通話の録音やアーカイブ化されているチケットメッセージをランダムに抽出してサンプルを取得してください。これらを確認し、双方の口調や言葉の選択に関連するヒントを見つけてください。

やり取りにおいて：

- 愚かな間違いをめぐって気まずい雰囲気が生じましたか？
- 見落としてしまったことに起因する恐怖が煽られませんでしたか？
- どちらかの側が阻害されたり、挫折感を味合わされたりしましたか？

外部監査

経営幹部のリスク評価のために、外部監査人を雇うことも検討してください。

企業が経営幹部の特権を変更したり、トップマネージメントに対して強力な管理を課したりすることを検討している場合は、外部からの視点を得ることが常に得策です。

外部から来た監査人は、経営幹部のリスク評価を公平に監督し、必要に応じて経営幹部や取締役会に悪いニュースを伝えることができます。

現実世界への影響

社内ポリシーが 10 万ドルのフィッシング詐欺から学校を救う[4]

フロリダ州のチャータースクールの校長である Jan McGee 博士は、億万長者のイーロン・マスク氏かその代理人と思われる人物と数カ月にわたってやりとりした後、学校の口座から 10 万ドルの小切手を振り出しました。

McGee 博士の権限では、理事会の承認がなければ、小切手として振り出せる学校資金は 5 万ドルまででした。幸運なことに、同校のビジネスマネージャーである Brent Appy 氏が、その詐欺行為者が小切手を決済する前に、その小切手を取り消すことに成功しました。

「私はとても賢い女性です。高い教育を受けています。私は詐欺にひっかかってしまいました。

グルーミングというのは、誰かと話して、その人を信じて、これは本当に本物なんだと信用させることなのです。」事件後に公開された教育委員会で、マギー博士はこのように語りました。

ジャン・マギー博士
フロリダ州チャータースクールの元校長

ivanti

2 最も簡単で、最も邪魔にならない経営陣のリスクを最初に修正します。

監査が完了し、セキュリティの脆弱性についての認識が深まったなら、次は行動計画を策定します。そして、過度に邪魔にならないようにします。

経営陣の行動ギャップの監査に基づき、組織で最も一般的な違反やリスクを特定し、まずその改善を優先します。

最も簡単な項目の例として、次のようなものがあります。

データ機密性と分類ポリシーの確立と更新: データ機密性と分類ポリシーの確立と更新: 誰が、どのような状況で、どれくらいの期間、何にアクセスすることを許可されるのか。なぜ特定の権限が許可されていないのか。何が許可され、何が許可されないのか、そしてその理由を全員にとって透明で明白にします。

社内コミュニケーション戦略を更新し 全従業員の入社時に許容可能な使用ポリシー (AUP) とデータの機密性に関するポリシーを導入し、定期的に注意喚起を行います。組織のイントラネット上にある単一の「公式」ポリシー文書では、社内のステークホルダー全員を教育することはできません。特に多忙な経営陣の教育は簡単にはできません。

標準的なアクセス承認および実行手順を文書化し、導入 することで、アクセス制御ポリシーがすべての従業員に適用され、すべての活動が完全に文書化され、検証可能であることを保証します。(監査でアクセスやネットワーク活動を確認できなかったのであれば、今こそ確認できるように改善するときです)

経営陣の現在のデジタル従業員体験 (DEX) を考慮します。 経営陣の通常のワークフローを妨げるような、懲罰的あるいは抑制的なセキュリティ対策は、不信感に拍車をかけることになります。代わりに、舞台裏で静かに動作し、過剰な質問や頻繁なロックアウトに対する苦情のチケットを増やすことなく、経営陣にセキュリティを提供するセキュリティツールを選択します。

3 経営陣の卓上演習をゲーム化します。

非技術系リーダーを対象としたゲーム化されたセキュリティトレーニングセッションは、参加者自身が部門レベルのセキュリティ侵害の影響を発見し、セキュリティ担当者が正しい方向性を示すことができるため、経営層の賛同を得ることができます。

まずは「フィッシング詐欺を見抜く」ことから始めましょう。

次の幹部会では、「フィッシング詐欺を見抜く」というシンプルなテーマから始めましょう。ここでは、チームにフィッシング詐欺メッセージのサンプルを見せ、どれが本当のメッセージでどれがフィッシング詐欺かをグループに尋ねてください。

実際のサイバー攻撃を題材にしたシンプルでインタラクティブなこのゲームには、スライドが2枚、所要時間は3分もかかりません。

経営幹部向けのゲーム化したセキュリティトレーニングのヒント

時間は短く

半日や一日のワークショップではなく、人が主導する、対面またはリモートのもっと短いセッションをもっと頻繁に行ってみてください。定期的な幹部会の開始時5分間を使って、簡単なセキュリティゲームまたはセッションを行いましょう!

偶然の要素を追加する

セッションで使う脅威やシナリオはランダムで選びましょう。20面のさいころを振って、番号付きリストからリスクを選択するという単純な方法も可能ですし、または特定の組織、地域または業界に対する極めて現実的なリスクに重みを置くジェネレーターのような、複雑な手段も取れることでしょう。

クリエイティブになる

攻撃をブロックするクリエイティブな解決策や、シナリオで示されたリスクを活用する方法を考え出すよう、経営陣を促しましょう。アイデアが非現実的、非実用的または不正確である理由を説明することでセッションを行き詰らせないでください。

同じチームで連携する

現従業員や元従業員をリスクや脅威として決して名指ししないでください!たとえ演習で「ふり」をするだけの場合も同様です。経営幹部とセキュリティチームのメンバーの両方が同じ側に立って作業できるようにすることで、全員がグループとして成功または失敗することになります。

演じてみる

さまざまなシナリオ、素材、小道具、ツール、またはおもちゃのブロックさえも備えた既成のセキュリティトレーニングボックスをセットアップして、ユニークでクリエイティブな参加の機会を含めつつ、トレーニングの演習をスピーディに行いましょう。[5]

ボードゲームを応用する

「シューツ・アンド・ラダーズ」や「ライフ」といった子供用すごろくの中古ボードゲームを購入し、簡単応用造できるセキュリティゲームを一箱にまとめましょう。

アワードを贈呈する

最も優秀な参加者やクリエイティブな参加者に、会社の記念品を贈呈しましょう!

複雑な専門用語を使うのを避ける

セキュリティの専門用語や頭字語は避けてください。また、経営幹部の現在のセキュリティに関する慣習について、遠回しに言及することも避けてください。

実際のケーススタディを使って点と点を結びます。

また、セキュリティリーダーは、同様の業界、経営陣の役割、リスクプロファイルにおけるインシデント事例を通じて、悪意のある攻撃が個人の生活やキャリアにどのような影響を与えるかを強調すべきです。良い反応と悪い反応の両方を見つけることを忘れずに。

事例：Levitas Capital社

事件の概要：

2020年、Levitas Capital社の創立者はなりすましのZoomリンクをクリックし、組織のネットワークにマルウェアをインストールしてしまいました。これを仕組んだ攻撃者らは、この策略が発覚する前に80万どるを盗みました。

何が悪かったのか：

短く説明してください 金融送金を承認する通常のチャネルが機能しなくなりました。攻撃者らは会社のEメールシステムを掌握し、サードパーティ管理者に対してファンドの共同創立者に2度なりすましました。

その後に起きたこと：

Levitas社の一番の大口顧客は信頼を失って離れていき、このヘッジファンドは事件の2か月後に閉鎖されました。同ファンドの2人の創立者、マイケル・ブルックスとマイケル・フェーガンの社会における地位や名声は失墜しました。

「発見されるべき危険信号は実にたくさんありました」

マイケル・フェーガン
Levitas Capital社 共同創立者

4 経営陣向けの「ホワイトグローブセキュリティサービス」の導入を検討します。

上級経営幹部は知名度やアクセス機会が高いため、セキュリティチームはそのような幹部に個別に注意を向ける必要があります。いわゆる「ホワイトグローブセキュリティサービス」です。

経営陣は、セキュリティ部門とのやり取りが気まずいと回答する傾向が 2 倍も高く、外部の技術サポートを求める傾向が 4 倍も高いことを考えると、このようなプログラムの目標は、信頼関係を構築し、セキュリティ上のエラーや疑問を報告する際の障壁を低くすることです。

「ホワイトグローブ」セキュリティプログラムを作成する際には、次の点を考慮します。

上級経営幹部向けに連絡窓口を一本化する。
これは最上位のセキュリティリーダーではありません。これは、コミュニケーションを統合し、標準化しながら、信頼を築くのに役立ちます。

自動化によるデプロビジョニングポリシーの実施
ゾンビ資格情報を回避するための手動オフボーディングチェックを含む）。

カスタムアクセス権限や個人パスワードマネージャーのセットアップを含む、経営陣クラスの従業員に対するオンボーディングを再考する。
リーダー自身は、適切な設定のための段階的な指示に従う時間がないかもしれませんが、組織としては、経営陣がこれらの基本的な保護対策を設定せずに業務を遂行することを認められる余裕はありません。

経営陣が読み飛ばせるような一般的なプレゼンテーションではない、1 対 1 のパーソナルセキュリティトレーニング
を開発する。これまでの卓上演習を利用し、新任幹部の部署や役割に類似した事件に焦点を当てたケーススタディを選ぶ。

どのような措置を講じたとしても、チームの焦点は、ポジティブなセキュリティ文化を浸透させること（懲罰的なものではない）、および説得力のある教育と協力的な洞察を通じて経営陣のコンプライアンスを向上させることです。

このレポートが引用したケーススタディが証明しているように、ヒューマンエラーは起ります。それはどの組織でも起こるでしょう。それは避けられないし、完全に避けることは不可能です。

しかし、経営陣の真の賛同を得た組織だけが、システムと信頼を回復し、侵害を乗り越えて前進することができます。

Ivanti のサイバーセキュリティに関する調査・報告シリーズをご覧ください!

参考文献

1. Proofpoint. (2022, May). 2022 Voice of the CISO: Global Insights Into CISO Challenges, Expectations and Priorities. From Proofpoint: https://go.proofpoint.com/en-voice-of-the-ciso-2022.html

2. Yip, K. N. (2016, May 21). Whaling Case Study: Mattel's $3 Million Phishing Adventure. From Infosec: https://resources.infosecinstitute.com/topic/whaling-case-study/

3. Pratt, M. K. (2023, February 28). Economic pressures are increasing cybersecurity risks; a recession would amp them up more. From CSO Online: https://www.csoonline.com/article/3689008/economic-pressures-are-increasing-cybersecurity-risks-a-recession-would-amp-them-up-more.html

4. Metz, C. (2023, March 29). Florida principal resigns after sending $100K to scammer posing as Elon Musk. From CBS News Miami: https://www.cbsnews.com/miami/news/florida-principal-resigns-after-sending-100k-to-scammer-posing-as-elon-musk/

5. Garzón, G., & Garzón, F. (2020, June 30). Cybersecurity Incident Response: Tabletop Exercises Using the Lego Serious Play Method. From ISACA: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/cybersecurity-incident-response

6. SecureWorld News Team. (2020, November 23). Hedge Fund Closes Down After Cyber Attack. From SecureWorld: https://www.secureworld.io/industry-news/hedge-fund-closes-after-bec-cyber-attac

2023 注目点 - 経営陣のセキュリティ

Ivanti の新しい調査が示す、経営幹部が直面する真のリスク

Ivanti のサイバーセキュリティステータスレポートシリーズの一部

Ivanti.com/ja
03-6432-4180
contact@ivanti.co.jp