エクスポージャー管理はサイバーセキュリティをどう変えるか

従来とは異なる考え方をもたらす5つの戦略的転換

ivanti

エクスポージャー管理という概念は、**サイバーセキュリティを変革するひとつの力として浮上しています。**

リスクを単独でとらえることが多い従来の手法とは異なり、エクスポージャー管理では、脅威をより広範な事業目標の枠組みの中に位置づけ、状況に照らし合わせて理解することが奨励されています。こうした転換は単なる視点の変更にとどまりません。企業がセキュリティにどのように取り組むかという根本的な考えを再構築することなのです。

現在、組織が直面している脅威は、その数と複雑さを増すばかりです。組織によるサイバーリスクの考え方も、それに見合った成長が求められています。セキュリティは、もはや IT 部門内でサイロ化することができず、ビジネスのあらゆる役職において、リスクの特定・軽減・管理の責任が共有されなければなりません。こうした協調的アプローチは、組織の回復力を高めると同時に、イノベーションを促進し、競争上の優位性を高める役割を果たします。

エクスポージャー管理は継続的に存在感を増し、サイバーセキュリティの分野を変革し、ビジネスレベルでのサイバーセキュリティの捉え方を根本的に変える可能性を秘めています。Ivanti が考える以下の 5 つの予測は、その可能性だけでなく、そこから発生する成果についても関わるものです。

エクスポージャー管理の5つの戦略的転換

01

組織はサイバーセキュリティリスクを包括的に捉える方向にシフトするでしょう。

02

「攻撃対象領域」の概念が大幅に広がるでしょう。

03

サイバーセキュリティリスクは、主観的評価から客観的評価へと移行するでしょう。

04

サイバーセキュリティ戦略が事業投資の指針となるでしょう。

05

経営幹部は、情報に基づいたサイバーセキュリティ管理を優先するようになるでしょう。

01

組織は**サイバーセキュリティリスク**を包括的に捉える方向にシフトするでしょう。

現在、リスク管理は、すべてではないにせよ、その大部分をIT部門が担っています。ITチームがサイロ化されているため、中核事業へのITの関与と、組織レベルでの ITの取り扱いとが適切に調和していないのです。

さらに、ポイントプロダクト、つまり特定のセキュリティ脅威発生時に対処するために設計されたソリューションを中心に展開されることも多く、サイバーリスクを全体的に捉えるのではなく、サイロ化された専門分野でのフィードバックループを生み出しているのです。ポイントプロダクトは適切な相互統合ができないことが多いため、その連携にギャップが生じると、結果としてセキュリティの適用範囲にギャップが生じることになります。

このような欠陥のある方式から脱却するには、リスクデータを統合し、サイバーセキュリティリスクを包括的かつ状況に適合した見方で捉えるようにすべきです。総合的なリスク管理に向けて、実践的なステップをいくつかご紹介しましょう。

データの収集と統合

組織全体で使用されているすべてのサイバーセキュリティツールとプラットフォームの包括的なインベントリを作成し、それらのツールからリスクデータを集約するための集中型プラットフォームを導入します。

コンテクスチュアルなリスク評価

組織のより広範な状況を考慮したリスク評価の枠組みを構築してリスクの潜在的な影響を評価し、それに応じて優先順位を設定します。

統合型リスク管理

統合型リスク管理プラットフォームでリスク状況を一元的に把握し、リアルタイムのモニタリングと自動化されたワークフローで対応と修復を合理化します。

戦略的アライメント

事業計画にサイバーセキュリティを盛り込み、組織によるリスク対策を明確かつ簡潔に示す経営幹部へのレポートを作成する

このアプローチに従うことで、組織はサイバーセキュリティ・リスクをより包括的かつ状況に応じて捉えることができ、中核的な事業目標に統合して、全体的な回復力と競争力を高めることができます。

組織の攻撃対象領域は静的なものではなく、急速に変化しています。これまで攻撃対象領域を定義していた伝統的なパラメータ（ソフトウェアおよびハードウェア）では、現代のセキュリティ戦略の数多くの重要事項を捉えることができなくなっています。

現代のビジネスの原動力となっているテクノロジーがさらに相互の繋がりを強めるにつれて、企業の攻撃対象領域もそれにともなって拡大しています。クラウド環境、サードパーティベンダー、増え続ける人的要因といった新しい要素は独自の脆弱性をもたらしており、組織はこれらを無視できなくなっています。

これらは、攻撃対象領域の一部とされる多くの要因のうちのいくつかです。

ソフトウェアとハードウェアのさらに先に

攻撃対象領域が従来の IT 資産以外にも広がっていることを認識します。考慮すべき事項として、クラウド環境、IoT デバイス、サードパーティベンダー、サプライチェーンパートナー、人的要因、その他の重要な領域が含まれます。

サードパーティリスク

サードパーティリスク管理（TPRM）ツールからデータを収集・分析し、ベンダーやパートナーのセキュリティ態勢を評価します。サードパーティとの関係を定期的に評価し、それらが組織のセキュリティ基準やコンプライアンス要件を満たしていることを確認します。

クラウドセキュリティ

クラウドセキュリティ態勢管理（CSPM）ツールのデータを統合し、クラウドサービスに関連するリスクを監視・管理します。クラウド環境のコンプライアンスとセキュリティのベストプラクティスを継続的に評価します。

人的要因

人間の行動に関連するリスクを理解して軽減するために、セキュリティ意識向上トレーニングプログラムやフィッシング・シミュレーション・ツールのデータを含めます。人為的なセキュリティ・インシデントの可能性を低減するために、継続的なセキュリティ意識向上トレーニングの文化を培います。

IoT デバイス

IoT セキュリティソリューションのデータを取り入れて、接続デバイス特有の脆弱性に対処します。IoT デバイスを安全に保護し、潜在的なリスクを軽減するために、堅牢な監視と管理を実施します。

デジタルリスク保護

デジタルリスク保護システムからのデータを統合し、ソーシャルメディア、ダークウェブ、その他のオンラインプラットフォームを含むデジタルチャネル全体のリスクを監視し、ブランドのなりすましやデータ漏えいなどの脅威の特定と対応を支援します。

攻撃対象領域を拡大してこれらの追加領域を含めることで、組織はサイバーセキュリティリスクをより包括的かつ状況に捉えじて把握し、全体的にレジリエンスを高めることができます。

03

サイバーセキュリティリスクは、主観的評価から**客観的評価**へとシフトします。

現在のセキュリティ運用チームが使用しているメトリクスは、普遍的に受け入れられる標準を備えておらず、戦略的なプランニングに効果的に反映されていません。セキュリティのフレームワークや標準はある程度の指針にはなるものの、多くの場合、それをどのように行うかよりも、何を行うべきかに重点が置かれています。

エクスポージャー管理は、意思決定データをより厳密に測定することにつながり、また、経営陣に提出されるアウトプットを合理化します。つまり、組織を望ましいセキュリティ態勢に導くための実用的で客観的な情報なのです。

その実現のためのステップをご紹介しましょう。

資産価値の分析

資産に関連するリスクを効果的に管理するには、まず各資産の価値を理解することから始めましょう。その分析には、一般的な市場動向ではなく、内部データ、リスク選好度、独自の脆弱性など、組織に特有の情報を使用します。

リスクの確率を測定する

次に、リスクの発生頻度と重大性を評価し、組織に関連するシナリオを作成することで、様々なリスク事象の発生確率と潜在的影響を理解することができます。

リスクのインパクトによる分類

資産は、バリュー・アット・リスク（VaR）やコンディショナル・バリュー・アット・リスク（CVaR）のような定量的手法を使用して、リスク・プロファイルに基づいて分類されなければなりません。

継続的に進化する機械学習で、組織が意思決定を行う際に正確かつリアルタイムのリスク評価ができるようになり、この移行が促進されます。

04

現在、サイバーセキュリティは主に技術的な専門家によって管理されていますが、彼らは自身のニーズを経営幹部に効果的に伝えることによく苦労しています。同時に経営幹部は、サイバーセキュリティの重要性と、それを軽視するリスクを十分に認識していながらも、経営幹部とIT/セキュリティ・チーム間の知識のギャップを埋める能力を必ずしも持ち合わせていません。

こうした壁があるために、いかなる組織でも「優れた」「合理的な」サイバーセキュリティ予算や戦略を定義することが難しくなっています。その結果、十分な情報に基づいた判断ではなく、恐怖心や業界のトレンドに基づいて決断が下されることがきわめて多く。こうしたアプローチは、優先順位のズレ、非効率的なリソース配分、説明責任の欠如をもたらしています。以上を総合すると、自らを守るために正しい手順を踏んでいると信じる組織でさえ、それが失敗に終わる可能性があるのです。

このような課題に対処するためには、組織はサイバーセキュリティに対する戦略的アプローチを導入し、業務上の優先事項とパフォーマンスデータを統合しなければなりません。その方法は：

データドリブンな意思決定

パフォーマンスデータを継続的に収集・分析し、最も有意義な結果をもたらす活動は何か、十分な投資対効果をもたらさない活動は何かを判断します。

パフォーマンスのメトリクス

サイバーセキュリティに関するイニシアチブの有効性を測定する主要業績評価指標（KPI）を開発し、追跡。これによって「適正」かつ「合理的」なサイバーセキュリティ予算がより明確になります。

包括的な管理

より広範な経営幹部が、包括的な意思決定とフィードバックループを監督しなければなりません。これにより、セキュリティ対策がビジネス目標に沿ったものとなり、組織の投資規模を適正化することができます。

パフォーマンスのメトリクス

サイバーセキュリティに関するイニシアチブの有効性を測定する主要業績評価指標（KPI）を開発し、追跡。これによって「適正」かつ「合理的」なサイバーセキュリティ予算がより明確になります。

セキュリティを中心に据えた文化を培う

セキュリティをコストセンターとしてではなく、付加価値として統合します。こうした文化の転換は、より賢明な投資とより良い結果をもたらすはずです。

これらの戦略を実施することで、組織はサイバーセキュリティ投資についてより多くの情報に基づいた意思決定ができるようになります。サイバーセキュリティ投資がビジネス目標と合ったものになり、好結果が生まれます。

05

経営幹部は、**情報に基づいたサイバーセキュリティ管理**を優先するようになるでしょう。

わかりやすいメトリクスが共有されていなければ、意思決定を任された経営幹部にサイバーセキュリティのリスクを適切に説明することはできません。結果を客観的に測定することができなくとも、実質的に組織のセキュリティ戦略を考える責任は経営幹部にあります。

現在、客観性があり、なおかつデータドリブンな意思決定に直結する信頼できるプロセスは存在しません。そのため、サイバーセキュリティをビジネス戦略に盛り込むことは、不可能ではないにしても困難になっています。組織のリスク選好度をしっかりと評価することが妨げられたり、阻まれたりしているのです。

経営幹部はエクスポージャー管理を行うことによって、情報に基づき、一貫性があり、説明可能なサイバーセキュリティリスク管理の意思決定を行うコアコンピテンシーを習得できるようになります。リーダーは、強固なデータと高度な分析を備えることで、リスクをビジネス用語で表せるようになり、組織全体のコミュニケーションと連携が促進されます。

これを実現するには、ベンダーの新しい能力だけでなく、企業文化の変化や意思決定プロセスを見直そうという意欲が必要となります。それには何が必要か、そのために必要なアプローチとは

リスク選好度のフレームワークを確立する

組織のリスク許容度を定義し、ビジネス目標に適合させる このフレームワークは意思決定の指針となって一貫性を実現します。

高度な分析を導入する

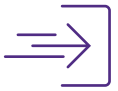
データドリブンな洞察によって、トレンドの特定、脅威の予測、セキュリティ管理の有効性の測定を行い、リスクの全体像を把握します。

リスクをビジネス用語で伝える

技術的リスクをビジネスへの影響に変換して利害関係者の参加を促し、共通のリスク言語とわかりやすい指標を用いて情報に基づいた意思決定を推進する

部門横断的な連携を促進する

定期的な会議やワークショップを開催して一貫性のある取り組みを実現してサイロを解体し、セキュリティチーム、IT チーム、ビジネスチーム間の連携を促進



定期的な見直しと適応

情報に基づいた意思決定を継続的なプロセスにする 進化する脅威の状況に適応するため、リスク、管理、想定事項を定期的に見直す

エクスポージャー管理がより堅牢になるにつれて、この変化はサイバーセキュリティ市場全体に大きな影響を及ぼします。

サイバーセキュリティにおいて経営幹部が積極的な役割を担うことで、トップダウンによる戦略的支援が強化され、新たな脅威が出現したときにセキュリティチームが迅速かつ徹底的に対応できるようになります。より良いリソース配分に加えて組織トップレベルの透明性が向上することで、リスク管理の優先度は高くなりメリットを受けるようになります。

サイバーセキュリティは戦略的イネーブラーとなり、新たなレベルの連携と賛同を得て、幅広いビジネス目標をサポートすることができます。セキュリティに対する取り組みが組織全体に浸透し、その結果として文化的な変化が生まれ、従業員一人ひとりの習慣や意識といった細かなレベルでのセキュリティ態勢がさらに強化されます。セキュリティを幅広く浸透させることで、組織は脅威に対して、情報に精通したセキュリティ意識の高いユーザー層からのリアルタイムのフィードバックに基づいて動的な対応ができるようになります。

最後に、エクスポージャー管理は主観的なものから客観的なものへと移行しています。定量的データの利用が増えれば、現在の定性的な判断への依存が減り、測定可能なリスク要因に基づくデータドリブンな意思決定が可能になります。最大のリスクがどこにあるのかを明確かつ実証的に理解することで、組織はより効果的に対処することができ、最も重大な脆弱性への対策を優先できるようになります。

これらは、実践分野としてのサイバーセキュリティ、また戦略的なビジネス目標としてのサイバーセキュリティを全面的に変革することに繋がります。エクスポージャー管理はこうした移行を今後もさらに後押しするはずです。

ivanti

詳細は Ivanti（ivanti.com/ja）
にお問い合わせください。