CompTIA

EXECUTIVE SUMMARY

Building a Culture of Cybersecurity:
サイバーセキュリティ文化を醸成する

企業エグゼクティブ（経営層）や役員メンバーのためのガイド

World Economic Form によると、ビジネスリーダーたちは 2018 年の最大の懸念事項としてサイバー攻撃をあげていました。多くの組織にとって重大なマインドセットの転換が必要となっています。セキュリティはもはや技術的な解決策がある問題ではなく、ビジネス上の重要な懸念事項として扱われるべきなのです。

しかし、このことを認識している企業のリーダーでさえ、彼ら組織のサイバーセキュリティ戦略をどう進めるべきか把握していないケースもあります。多くは、問題の技術的側面を十分に理解するためのトレーニングを受けておらず、さらにサイバーセキュリティプロフェッショナルは、役員メンバーが最終的に執行しなければならいビジネス上の問題への対処経験を持たないことがあります。

CompTIA Cybersecurity Advisory Board は、役員やエグゼクティブにとって最重要となるビジネスの側面からみたサイバーセキュリティの脅威、問題、懸念に焦点を当てたホワイトペーパーを作成しました。このホワイトペーパーは、ビジネスリーダーがサイバーセキュリティに対する組織のアプローチを評価・改善するための 6 つの指針を明確化しています。

指標 1 ：サイバーセキュリティをビジネス戦略に組み込む

シニアエグゼクティブと役員メンバーは、サイバーセキュリティの取り組みの定量化に直接関与し、サイバーセキュリティのコスト・回収に対する新たなアプローチを促進する必要があります。

- サイバーセキュリティを ROI 計画と捉えてください。サイバーセキュリティは、企業の戦略プランと関連して取り組まれるべきで、そこには成長機会と並行してリスクが伴います。数ある基本的なサイバーセキュリティテストは、ごくわずかな費用で実施できるものでありながらも、貴重な収益をもたらすことを理解する必要があります。リソースが限られている場合は、より深刻かつ大きな脅威からの保護に重点的に取り組むことがベストと言えます。

- 企業データの「重要資産」を特定しましょう。また、他のメンバーの「重要資産」に対する共通認識 ― 「重要資産」が何であるか、それがミッションクリティカルであり、ビジネスにとって競争上の強みをもたらすものであるといった認識 ― を確実にしましょう。「重要資産」を特定したら、それをどう保護するかより明確に取り組むことができます。

- 企業経営者は、サイバーレジリアンスを幅広いビジネス戦略に組み込むべきです。取締役やシニアエグゼクティブは、シナリオモデリング、ROI 分析、競合分析、新興テクノロジーの再検討といった新しい機会を評価するためにすでに使用しているツールに、サイバーセキュリティリスクを組み込む必要があります。

- こうした考えは、企業文化の変化を必要とします。NIST のフレームワークは、エグゼクティブが、技術仕様ではなく、事業目標の観点からサイバーセキュリティを検討する上で役立つものです。NIST は、９ページに渡る概要を提供しており、より強固なサイバーセキュリティのための段階的なパスをつくるガイドとなります。

指標２：企業構造は、サイバーセキュリティ文化を強化すべき

明確なサイバーセキュリティ対策の欠如は、組織の目標にコミットしていないことと同じです。

- 役員メンバーは、サイバーセキュリティの問題に特化し報告するメンバー１名を選任しましょう。役員全体が関与し、情報提供が実施されるべきではありますが、少なくとも１名は、差し迫った問題をビジネス用語で説明するためのテクニカル知識を持っていることが重要です。これにより、サイバーセキュリティが主に IT 部門で管理されるというサイロ化を防ぐことができます。

- 明確なサイバーセキュリティの「チェーンオブコマンド（指令系統）」を描きましょう。すべての組織に合致する答えはありません。重要なのは、役員にはじまり、サイバー脅威からビジネスの保護を任務とする人物まで、あなたの組織はサイバーセキュリティのアカウンタビリティ（責任義務）に配慮しているという点なのです。

- 人材の配置と報酬は、サイバーセキュリティの重要性が反映されるべきポイントです。CIO や他のサイバーセキュリティプロフェッショナルがどのように評価され、報酬を得ているか調べてみてください。残念ながら頻繁に、「対応のスピード」と「コストの最小化」は、彼らのパフォーマンス評価において過小評価されていることがあるのです。

- サイバーセキュリティ協議会などで企業リーダーたちを集めましょう。チーフリスクオフィサー、CPO、CISO、ビジネスユニットリーダー、さらには外部コンサルタントや、主要ベンダーを含む部門間のサイバーセキュリティ協議会をつくりましょう。これにより、組織全体がサイバーセキュリティの問題を理解し評価することが可能となります。

指標３：従業員が最大のリスク

従業員は、誤ってデータを危険にさらしたり、ライバル企業のために情報を盗んだり、データや機密情報を売ったりする可能性があります。企業データへのアクセスを制御することで、致命的な損害となる前にこうした行動を捉える確率を向上させることができます。

- サイバーセキュリティプロフェッショナルは、通常のトレーニング以上のものを受ける必要があります。彼らのトレーニングに投資することは、組織に対する報酬であり、最新の脅威に遅れを取らないため必要不可欠といえます。

- 大半の従業員には、トレーニングは短期間に、頻繁かつ現実のシナリオに基づくことがポイントとされます。効果的なサイバーセキュリティトレーニングは、小規模でわかりやすいセッションで提供され、試験や補強学習で補完されること。すべてのレベルの従業員を参加させることで、セキュリティ文化を作るよう設計されることが重要です。

- 経営の上層部や役員メンバーは、データへのアクセス権を持つものの十分なトレーニングを受けていない場合があります。日々のサイバーセキュリティ対策トレーニングは、トップレベルの管理者であってもリスクやビヘイビアをより効果的に判断する上で役立つものです。

- ユーザーのエラーを排除することは不可能であることから、データへのアクセスを制限する必要性が

あります。何人のユーザーがどのレベルのデータ、特に「重要資産」にアクセスしたか、といった組織全体における正確なデータの把握が重要となります。

指標 4：検出、検出、検出

データ違反/侵害を検出するまでの時間が長くなればなるほど、その代償は高くつきます。

- 内部監視。ビジネスリーダーの職務では、それぞれのセキュリティ問題を積極的に検出することは難しくても、検出を優先する取り組み、サイバーセキュリティを促進する取り組み（インセンティブ）を強化することが可能です。

- 第 3 者の監査。関連するシニアレベルの委員会では、実施された報告書を正式な形で評価する必要があります。さらに、フィードバックループを作ることで、こうした調査からの洞察を、既存のプロセス、ポリシー、マニュアルに直ちに組み込むことが可能となります。

- 検出を向上させるツール。EDR、SIEM、その他テクノロジーはすべて、適切なトレーニングを受け、経験豊富なサイバーセキュリティプロフェッショナルによる定期的な分析を必要とします。シニア管理者層は、セキュリティチームがデータを適切にレビューし、十分に対応できるよう必要なリソースを確保する必要があります。

指標 5：データ保護：必要なものを収集し、必要なものだけを共有する

組織には、データ保護のため柔軟かつ適応性のあるアプローチが必要です。

- ビジネスクリティカルなデータのみを収集しましょう。データの収集がなければ、そもそも盗まれることがないのです。あなたの組織に、データの収集、保管、保護、分析に必要となるリソースの明確なプランおよび、現実的な見積もりがあることを確かにしましょう。

- ベンダーとサプライチェーンの脆弱性。すでに協業しているベンダーについては、彼らがアクセスできるデータが何であるか、どのようにアクセスしているか把握しましょう。新しいサプライヤーと契約を結ぶ前に、サプライヤーが提示した基準を満たしていること、契約にあるセキュリティ対策が取られていることを確実にするため外部監査を実施しましょう。このような監査は、少なくとも年に一度実施されるのが理想とされます。

- 法的環境の変更は、規制対応を困難にします。従って、あなたの企業がある（法的）管轄区域でのサイバーセキュリティに関する法的要件や規制要件を理解するエグゼクティブを一人置くことが堅実といえます。また、この人物は、こうした要件が、組織のサイバーセキュリティ戦略にどのように反映されるべきか判断する手助けを行います。

指標 6：強固な危機管理プランを立てる（そして試験する！）

正式なインシデント対応チームが設置されていないとしたら、これこそがサイバーセキュリティ戦略の重要な構成要素となります。

- 内部の危機管理戦略を作成する。最も可能性の高いサイバーセキュリティ脅威に優先順位をつけ、シナリオに応じて最も堅固かつ詳細なプランを作成しましょう。また、脅威の種類に応じて、法務、通信、マーケティング、人事部門など組織全体に渡る主要部門を明記する必要があります。

- エグゼクティブや役員メンバーは、訓練やシミュレーションに直接的に関与しなければなりません。ビジネスリーダーらは、組織のサイバーセキュリティプロフェッショナルと協力して、潜在的なサイバーセキュリティインシデントに関する通知の手段や、関与の仕方を話し合う必要があります。

- 外部のエンゲージメントとアウトリーチ(支援)を計画する - Equifaxの情報漏えいから学べること。レスポンスの早い段階において、法律顧問やPRチームとどのように関わるか、予め検討しておく必要があります。法務チームへの連絡が遅れると、コンプライアンスの不履行や、訴訟の可能性が発生します。さらに、対応の遅い/薄弱な公式声明は、企業の評判を傷つけることとなります。

まとめ

企業文化を変え、サイバーセキュリティを真に包括するには、解決策のあるテクノロジー問題として扱うのではなく、幅広いリスク管理プロセスの一環として考える必要があります。問題を起こしてしまった個人を非難するのではなく、まず企業の構造に目を向けてください。従業員は、問題が起きた際、それを隠すように教育されていますか、またはそれを調査し解決するよう教育されていますか？あなたのサイバーセキュリティ部門は、課題に取り組むために必要なリソースを持ちますか、あるいは枯渇した予算で実施するよう指示されていますか？最も成功したサイバーセキュリティのアプローチは、必ずしも高価であるものではありませんが、持続性、注意、優先順位付けを必要とします。これらは、ビジネスリーダーらのみが組織にもたらすことができる特性なのです。

「Building a Culture of Cybersecurity：サイバーセキュリティ文化を醸成する」は、
https://www.comptia.org/insight-tools より閲覧いただけます。